German Federal Ministry of Justice and Consumer Protection
State Administration for Industry and Commerce of the People´s Republic of China
National Consumer Secretariat, Ministry of Justice of the Federal Republic of Brazil
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH (eds.)

Consumer Data Protection in Brazil, China and Germany

A Comparative Study

Board of Editors
Rainer Metz
Jörg Binding
Pan Haifeng

Coordinating Editor
Florian Huber

Göttingen University Press

Consumer Data Protection in Brazil, China and Germany

Published by Göttingen University Press 2016

Consumer Data Protection in Brazil, China and Germany

A Comparative Study

Edited by

German Federal Ministry of Justice and Consumer Protection

State Administration for Industry and Commerce of the People´s Republic of China

National Consumer Secretariat, Ministry of Justice of the Federal Republic of Brazil

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Board of Editors: Rainer Metz, Jörg Binding, Pan Haifeng

Coordinating Editor: Florian Huber

Göttingen University Press
2016

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de

Set and layout: Franziska Pannach
Cover design: Jutta Pabst
Cover picture: Maksim Kabakou/shutterstock.com

http://univerlag.uni-goettingen.de
ISBN: 978-3-86395-236-5

Table of Contents

Chapter 1
Study Structure

A. Project Summary

The rapid development of new information and communication technologies has changed people's everyday life and consumption patterns significantly. The worldwide spread of those technologies provides many innovations for consumers, including new communication channels as well as access to a wide range of goods and services by e-commerce and online payment. The use of these innovations offers consumers many advantages and benefits, but it can also bear risks, such as the indiscriminate collection, storage and cross-border flow of personal data, illegal spying on Internet activities, dissemination of personal information, and abuse of user passwords. The said risks can lead to personal and economic damages and impairments. Therefore, a more effective protection of consumer

data through an international cooperation involving developed and developing countries with emerging markets is necessary.

There are already initiatives of cooperation, such as the harmonization of consumer data protection in the European Union (EU), the European Economic Area (EEA) and the Council of Europe. Examples of the said initiatives in the EU in terms of legislation are the Data Protection Directive and the proposed General Data Protection Regulation of the EU. Another example is the International Conference of the Commissioner for Data Protection. Although these initiatives represent an advance, consumer and data protection policies remain limited regionally and fail to involve key players of emerging economies efficiently. More recent developments demonstrate that awareness in emerging countries, such as China and Brazil, is growing regarding the importance of adequate consumer protection. Some recent examples are the enactment of the revised regulations on consumer protection in China or the Internet Civil Rights Framework in Brazil.

Against this background, the German Federal Ministry of Food, Agriculture and Consumer Protection commissioned the German Agency for International Cooperation (GIZ: Deutsche Gesellschaft für Internationale Zusammenarbeit) in 2013 to implement the project *"Consumer Data Protection in Emerging Economies"*. In 2014, due to the reassignment of consumer protection to the German Federal Ministry of Justice and Consumer Protection (BMJV: Bundesministerium der Justiz und für Verbraucherschutz), the project continued in cooperation with this ministry. Currently, the project has three main partners: the Chinese State Administration for Industry and Commerce (SAIC), the Brazilian Ministry of Justice (Ministro da Justiça) with its National Consumer Secretariat (MoJ for its initials in English) and the BMJV.

The objective of this project is to improve the conditions of cooperation between Germany, China and Brazil in the field of consumer data protection. The implementation of the project is based on the principle of an equal partnership between the countries participating. Accordingly, key actions of the project are planned under the responsibility of a Steering Committee, composed of the representatives of the participating countries and the non-governmental organization (NGO) Consumers International (CI). The Organization for Economic Cooperation and Development with its Committee on Consumer Policy (OECD-CCP) and the Global Privacy Enforcement Network (GPEN) have also been involved in the activities of the project. Additionally, consumer organizations, trade associations and academic experts are participating in the project's initiatives and activities.

The project seeks to engage at a high level with governments in the three countries through initiating an international dialogue to form a basis for close political and technical cooperation, to conduct a comparative research study, to analyze the current situation of consumer data protection and privacy in the three countries, and to use the results of the study to develop an international e-learning

platform to improve human capacity on those issues. In order to achieve the objective mentioned, this project uses a methodology which consists of political and professional dialogue (e.g. conferences, study tours, workshops, experts meetings) and training strategies (including training events, elaboration of training material and concepts of e-learning tools).

Firstly, the national regulators and governmental authorities concerned shall increase their awareness of comparative experiences and best practices using data protection regulations in order to include possible law reforms in their own national agendas. The international context of consumer data protection is also discussed with the government organizations, consumer organizations and other international actors participating. Conferences and workshops allow a direct exchange between members of state institutions, consumer organizations, experts from academia and the private sector.

Secondly, the comparative study on legal and practical aspects of consumer data protection in the three countries participating in the project will allow governmental institutions and NGOs to be informed of the current state of consumer data protection in Germany as well as in Brazil and China, two of the BRICS countries (Brazil, Russia, India, China and South Africa). The technical basis of the comparative study is established in reports by a group of international experts on consumer and data protection issues.

Thirdly, the findings of the comparative study will be included in an e-learning platform for training activities on consumer data protection, complementing and sharing knowledge for the development of future research and advocacy ideas. The development of this e-learning platform will be based on the reports and comparative academic training events in China and Brazil which are carried out for staff members from consumer organizations or state institutions in those countries. The e-learning tool will be designed as a multimedia online platform with a modular structure, which allows its users an easy adaptation to their country's specific context through the integration of different language versions of various modules. In addition, it offers a flexible use for different stakeholders, e.g. governmental institutions and consumer organizations. The e-learning tool will be elaborated during the second semester of 2015 and the beginning of 2016.

B. Research Activities

The work on the present comparative research study began in 2013. In October 2013, a German delegation on consumer privacy issues visited China to familiarize themselves with the status quo of consumer data protection. It held talks with the Ministry of Industry and Information Technology (MIIT), SAIC, the China Consumers' Association (CCA) and several companies. The delegation completed and presented a report to the GIZ with comprehensive recommendations. The next

step was the appointment of the organization CI in 2014. Consumers International supports the project, mainly in cooperation with Brazil, in the preparation of technical studies and the development of the e-learning platform. In addition, a group of international experts was established in 2014. The purpose of the said group is to discuss current national and international developments in the political and legal context of consumer data protection. This group is composed of Prof. Dr. Gerald Spindler, professor at the Faculty of Law of the Georg August University of Göttingen, Germany, Prof. Dr. Zhou Hanhua, Assistant Director of the Institute of Law of the Chinese Academy of Social Science (CASS), Prof. Dr. Danilo Doneda, consultant to the National Secretary for Consumers of the Brazilian Ministry of Justice, and Amanda Long, Antonino Serra Cambaceres and Joana Varon Ferraz of CI.

The first meeting of the Steering Committee, a kick-off conference and the first expert workshop on the creation of a comparative technical study between the countries (part of the project) were carried out in Berlin in November 2014. The meeting of the Steering Committee was attended by governmental representatives of the partner countries, international experts of CI and staff of the GIZ. The workshop was conducted by country experts of the project countries and the outline of the study was reviewed by the Steering Committee. The kick-off conference on cooperation with emerging economies in the field of consumer data protection was attended by high-level governmental representatives, including the German Minister of Justice and Consumer Protection, the German Federal Commissioner for Data Protection and Freedom of Information, the designated European Data Protection Officer and representatives of international organizations, such as the OECD and GPEN. Subsequently, the second expert meeting was held in Germany in April 2015 to discuss the status quo of consumer data protection from a comparative law perspective. Additional activities were planned to encourage the international cooperation and political dialogue on consumer data protection during 2015 and 2016.

C. General Overview of the Study

The study deals with the current state of consumer data protection law in the partner countries and practical developments in this field. Its results shall serve as a conceptual basis for any future cooperation among the partner countries and constitute a useful tool for actors engaged in international efforts to regulate data collection, usage, security, and consumer protection.

Chapter 2 of the report covers the main legal issues of consumer privacy and data protection of the partner countries. Among the topics analyzed from a comparative point of view are the following: an overview of the scope of legislation addressing consumer data protection (including the subject of the legislation, the

general legal framework for consumer data protection, and sectorial laws and regulations concerning telecommunications, banks, media-related and specific acts for e-commerce); the territorial and international applicability of data protection acts; central definitions and concepts of the notion of consumer and data; the general guiding principles established in laws and regulations; the concepts of collecting, storing and processing consumer data and the approaches to consumers' consent; basic rules on publicity and transparency; data security, data control, data portability and the right to access, modify and delete collected data; the roles and responsibilities of intermediaries; access to user data by third parties, provisions on data retention; regulations concerning the transfer of data on an international scale, transfer to third countries and requirements for data transfer outside the country; the enforcement of consumer data protection (through civil, criminal and administrative law); and, finally, the current role of self-regulation and co-regulation.

Chapter 2 also analyzes and discusses the international standards in the field, among them the United Nations Guidelines for Consumer Protection, the Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, elaborated by the OECD, the Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy of the GPEN, the Convention for the Protection of Individuals with regard to automatic processing of personal data, adopted by the Council of Europe, or the Framework for Information Privacy Protection developed by the Asia Pacific Economic Cooperation's (APEC) Electronic Commerce Steering Group (ECSG).

Chapter 3 seeks to explain current issues and case law concerning consumer data protection from a practical perspective. Firstly, it concentrates on the problem of consumer profiling and case law related to that phenomenon, as well as the databases which currently exist to report consumer rights violations in Brazil. Secondly, it deals with current issues of consumer data protection before Chinese tribunals. The relevant case law regarding civil claims will be analyzed within four topics: illegal collection and use of personal information for economic or other reasons; disclosure and illegal release of consumers' personal information; advertisements without the prior consent of consumers and clients; and the boundaries of legal protection of the right to privacy. Criminal justice case law addresses illegally acquired personal information, selling and illegally providing citizens' personal information to third persons, the use of different criminal means to acquire citizens' personal information illegally, and the qualification of certain "grave circumstances" of criminal acts. Finally, current developments regarding the administrative enforcement of consumer data protection laws and regulations by governmental authorities in China are illustrated.

Thirdly, regarding practical experiences from Germany and Europe, the study focuses on credit scoring and related databases, data protection in social networks, cloud computing, "big data," the existence of rating platforms on the Internet,

profiling, unsolicited e-mails (spam), the role of online search engines and the right to be forgotten in the jurisprudence of the European Court of Justice, as well as its judgment on data retention.
Finally, the chapter addresses the current challenges of new technologies for consumer data protection.

In Chapter 4, the main topics contained in every country report are summarized and compared. A summary and comparison of the main topics found in each country report are offered here.

The whole study, which includes the developments in consumer data protection up to August 2015[1], shall serve as a tool for further cooperation between Brazil, China and Germany and facilitate discussions for the improvement of consumer data protection policies and regulations through its dissemination and implementation within and outside of the said countries. The results of the technical study also serve as a basis for the e-learning tool being designed currently, for future training events for consumer organizations and policy makers, and for consumer education in general.

[1] After the agreed submission deadline for the country reports of this study elaborated between 2014 and 2015 on the developments in the field of consumer data protection, the Permanent Representatives Committee of the Council of the European Union confirmed on 18 December 2015 the revised compromise texts of the "General Data Protection Regulation" and the "Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data", agreed with the European Parliament as part of the European data protection reform. The agreement had been reached between the Council of the EU, the Parliament and the European Commission on the 15 December 2015. On 17 December 2015, the European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee endorsed the texts agreed in the trilogies. They are expected to be submitted in early 2016 for adoption by the Council and, subsequently, by the Parliament. The regulation and the directive are likely to enter into force in spring 2018.

Chapter 2
Country Studies on Consumer Data Protection (Brazil, China, Germany) and International Initiatives

A. Consumer Data Protection in Brazil
(Prof. Dr. Danilo Doneda)

I. Introduction

Brazil, with over 202 million inhabitants, has the fifth largest population in the world.[2] It has the largest national economy in Latin America, the world's seventh largest economy at market exchange rates (with a nominal GDP of US$ 2.24 tril-

[2] See Brazilian Institute for Geography and Statistics, <ftp://ftp.ibge.gov.br/Estimativas_de_Populacao/Estimativas_2014/estimativa_dou_2014.pdf> (last accessed June 26, 2015).

lion and a GDP per capita of US$ 11,067 in 2014) and the seventh largest economy in purchasing power parity. There were over 271 million registered mobile phones subscriptions in Brazil in 2013, which represents around 135 % of Brazil's population.[3] By 2013, an estimated 51.6 % of Brazilians had access to Internet. Finally, e-commerce is estimated to have grown 26 % between 2013 and 2014, with an economic volume of US$ 13.4 billion.[4]

II. Overview and scope of legislation addressing consumer data protection

1. Character of legislation

The legal framework of consumer and data protection is composed of the Federal Constitution of October 5, 1988, and several laws, among them the Civil Code (Law No. 10.406 of 2002),[5] the Consumer Defense Code (CDC; Law No. 8.078 of 1990),[6] the Credit Information Law (Law No. 12.414 of 2011), the Access to Information Law (Law No. 12.527 of 2011), and the Civil Rights Framework for the Internet (Law No. 12.965 of 2014).[7] These acts can be described collectively as the Data Privacy Regulations.

In general terms, the constitution protects the rights to privacy, including secrecy of the following: correspondence, bank operations, telegraphic communications, telephone communications, and data communications. The Civil Code allows individuals to seek injunctions before any relevant court to impede or cease any privacy violation. The CDC, as the main consumer law, constitutes the legal regime of regulations concerning consumer protection issues. However, despite some sector laws governing the telecommunications and Internet branch, there is no general data protection law enacted in Brazil as of today. Therefore, the legal framework for the protection of data is formed by the general principles of protection to privacy and intimacy contained in the Brazilian Federal Constitution and national laws. Those general principles and provisions on data protection and privacy can be derived from the constitution, the Brazilian Civil Code, and laws and regulations that address particular types of public and private relationships, different sectors (e.g. financial institutions, health industry, telecommunications),

---

[3] <http://www.factfish.com/statistic-country/brazil/mobile+cellular+subscriptions> (last accessed June 26, 2015).

[4] <http://info.digitalriver.com/rs/digitalriver/images/DigitalRiverCountrySpotlightBrazilValueBrief.pdf> (last accessed June 26, 2015).

[5] Law No. 10.406 of January 10, 2002 (Civil Code; *Código Civil*), <http://www.wipo.int/wipolex/en/details.jsp?id=9615> (last accessed June 26, 2015).

[6] Law No. 8.078 of September 11, 1990 (CDC; *Código de Defesa do Consumidor*), <http://www.procon.sp.gov.br/texto.asp?id=745> (last accessed August 7, 2015).

[7] Law No. 12.965 of April 23, 2014 (*Marco Civil da Internet* – Civil Rights Framework for the Internet; also called the Internet Act), <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> (last accessed June 26, 2015).

and the treatment and access to documents and information handled by governmental entities and bodies.

With regard to the constitutional level, the Federal Constitution of Brazil provides, on the one hand, for the protection of the right to freedom of expression[8] and the rights to privacy, private life and intimacy, honor, and the image of persons, protects the confidentiality of correspondence and telegraphic, data and telephone communication, and ensures people's access to information from governmental institutions.[9] The latter are enforced through the writ of *habeas data*, which was introduced into the constitution in 1988 and regulated by Law No. 9.507 of 1997 (*Habeas Data* Law), and has, since then, influenced the concepts of the right to privacy and data protection in other Latin American countries. Brazil, thus, responded to social demands after the end of the military dictatorship to grant access to the information gathered by governmental bodies.[10] This historical circumstance, rather than the need for a data protection statute among individuals, was the main reason for the creation of a constitutional and legal framework regarding data protection. This constitutional remedy is available for individuals to grant access to information related to the individual, which is registered on governmental or public databases, to correct or update data or to proceed with annotations or clarifications on public databases concerning pending litigation.[11] Any database including the following information is considered a public database and, therefore, subject to *habeas data* (*Habeas Data* Law): information that is or may be transmitted to third parties, and information that is not exclusively used by the governmental agency or legal entity that generated or managed that information.[12] However, the *habeas data* writ, considered as a costly and slow remedy as it must

---

[8] See Federal Constitution, Article 5, IV: "[…] the expression of thought is free, and anonymity is forbidden."

[9] See Federal Constitution, Article 5: "All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms […]:
X – the privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured; […]
XII – the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts; […]
LXXII – habeas data shall be granted:
a) to ensure the knowledge of information related to the person of the petitioner, contained in records or data banks of government agencies or of agencies of a public character;
b) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative."

[10] *Doneda/Schertel Mendes*, Protection in Brazil: New Developments and Current Challenges, in: *Gutwirth/Leenes/De Hart* (Eds.), Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges, 2014, p. 5.

[11] See Federal Constitution, Article 5, LXXII: "*habeas data* shall be granted: a) to ensure the knowledge of information related to the person of the petitioner."

[12] See Law No. 9507 of 1997, Article 1, sole paragraph.

be presented by a lawyer after the plaintiff`s unsuccessful request for the data from the defendant, was neither understood as a modern data protection tool nor did it develop into such.[13] Instead, other instruments were developed in Brazilian law to address the increase of electronic data processing, e.g. the Credit Information Law and the Access to Information Law.

On the other hand, the Federal Constitution refers directly to consumer protection, both in Article 5, XXXII,[14] which considers consumer protection as a fundamental right, and Article 170 V,[15] which establishes consumer protection as a principle of the national economic order, as well in Article 48 of its Temporary Provisions, creating an obligation to enact a CDC.[16] That code provides for a multifaceted framework to address consumer protection issues and balance the information and power asymmetries between consumers and business enterprises.[17] It entails a variety of principle-based norms, which are broad enough to offer solutions to new conflicts related to information technology.[18]

Later, the Credit Information Law (Law No. 12.414 of 2011) was enacted to regulate the use of credit databases, allowing data controllers to register the so-called "positive" credit information, i.e. information about the consumer's general financial situation, and not only restricted to unpaid debts, which was the only credit data that the CDC allowed to be registered.[19]

Finally, the Internet Civil Rights Framework (Law No. 12.965 of 2014) deals specifically with issues affecting the collection, maintenance, treatment, and use of personal data on the Internet. It contains several provisions concerning the pro-

---

[13] *Doneda/Schertel Mendes*, Protection in Brazil: New Developments and Current Challenges, in: *Gutwirth/Leenes/De Hart* (Eds.), Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges, 2014, p. 6.

[14] See Federal Constitution, Article 5, XXXII: "the State shall provide, as set forth by law, for the defense of consumers."

[15] See Federal Constitution, Article 170, V: "The economic order, founded on the appreciation of the value of human work and on free enterprise, is intended to ensure everyone a life with dignity, in accordance with the dictates of social justice, with due regard for the following principles: […] V. consumer protection."

[16] See Temporary Constitutional Provisions Act, Article 48: "The National Congress, within one hundred and twenty days of the promulgation of this Constitution, shall draw up a consumer defense code;" <http://www.v-brazil.com/government/laws/ADCT.html> (last accessed June 26, 2015).

[17] *Doneda/Schertel Mendes*, Protection in Brazil: New Developments and Current Challenges, in: *Gutwirth/Leenes/De Hart* (Eds.), Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges, 2014, p. 6; *Lima Marques/Herman Benjamin/Miragem*, Comentários ao Código de Defesa do Consumidor, Revista dos Tribunais, 2006.

[18] *Doneda/Schertel Mendes*, Protection in Brazil: New Developments and Current Challenges, in: *Gutwirth/Leenes/De Hart* (Eds.), Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges, 2014, p. 6.

[19] For more details, see *Doneda/Schertel Mendes*, Protection in Brazil: New Developments and Current Challenges, in: *Gutwirth/Leenes/De Hart* (Eds.), Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges, 2014, pp. 8-10.

tection of privacy and data protection. Its first draft was the result of a consultative process through the Internet, which resulted in a principle-orientated statute, and whose main aim is to assure the existence of a set of rights for Internet users. During the legislative process, the parliament decided to include more specific rules on data protection and privacy. The result was a text with a rather impressive length of provisions on privacy. However, it must be born in mind that it cannot be considered a general data protection law, as it only applies to Internet-related issues without including general provisions and principles regarding data protection.

2. General legal framework for consumer data protection

As explained before, Brazil does not currently have a general law or legal framework concerning data protection. Several laws (CDC, Credit Information Law, Access to Information Law, and the Internet Civil Rights Framework) regulate relevant issues of consumer data protection, but are limited with regard to its scope of applicability. Therefore, one has to draw on general principles of data protection derived from constitutional provisions concerning privacy and data protection.

3. Telecommunication

Telecommunication issues are regulated by the General Telecommunications Act (Law No. 9.472 of 1997), which regulates the exploitation of telecommunication services. It establishes a series of rights for telecommunication services users, among them the right to confidentiality of their communications.[20] In the regulatory field, the Brazilian Telecommunications Agency (ANATEL) included provisions about privacy in the General Consumer Rights Regulation (Resolution 632/2014).[21] It must be stressed that telecommunication services are also subject to consumer law and the applicable consumer privacy provisions when provided to a consumer.

[20] See Article 3, V. "Users of telecommunication services have the right to: […] the inviolability and secret of their communications, except in the cases and conditions provided by the Constitution or the Law."

[21] See Article 3, VII. "The consumer of the services related to this regulation have the right, notwithstanding the legislation and the regulation specific to each of these services, to: […] the privacy in the billing documentation and in relation to the use of their personal data by the provider of the service."

4. Banks

The CDC protects personal data, specifically those contained in databases held by banks and credit agencies.[22] The confidentiality of financial data is also mentioned in the Complementary Law No. 105 of 2001.[23] According to this law, every financial institution must assure the confidentiality of its transactions and services, which include the personal data involved.[24]

5. Media-related acts

What can be described as media regulation in Brazilian law is, as of today, basically a set of rules governing the concession of licenses to operate communication services. There are discussions regarding the applicability of these rules to Internet-based services (such as rules governing accessibility to the content of streaming services). Nevertheless, there are no specific rules of media regulation concerning privacy and data protection.

6. Specific acts for e-commerce

The National Plan on Consumption and Citizenship (*Plano Nacional de Consumo e Ciudadania* – Plandec) was proposed by Decree No. 7.963 of 2013,[25] with the objective of promoting consumer protection in Brazil through the integration and coordination of policies, programs and actions.[26] Among the main goals of Decree No. 7.963 is the protection and promotion of privacy, confidentiality and

[22] Article 43 of the Consumer Protection Act reads as follows: "The consumer, without prejudice to the provisions of the article 86, shall have free access to any of his own data informed in reference files, index cards, records, personal and consumer data, as well as their respective sources.
Paragraph 1. – Consumers' data and reference files shall be objective, clear, true and comprehensively written, not bearing any negative information concerning a period of time of more than five years.
Paragraph 2. – If not requested, the consumer shall be communicated in written form about the inclusion of his name in any reference file, index card, register, personal and consumer data.
Paragraph 3. – Whenever finding any inaccuracy in his data and records, the consumer shall be entitled to require the prompt correction, and the person in charge of such records shall communicate the alteration, within five weekdays, to any possible addressee of the incorrect information.
Paragraph 4. – Consumers' databases, reference files, credit protection services and others related, shall be understood as public entities.
Paragraph 5. – Once extinguished the time for collecting consumers' debts, the respective Credit Protection Services shall no longer provide any information that might prevent or make it difficult to consumers a new access to credit operations before suppliers."

[23] <http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp105.htm> (last accessed August 7, 2015).

[24] See Article 1. "The financial institutions shall keep the confidentiality of their active and passive transactions and services rendered."

[25] <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7963.htm> (last accessed June 26, 2015).

[26] See Article 1 of Decree No. 7.963 of 2013.

security of personal data. It was enacted together with the Decree No. 7.962,[27] which specifically provides for new rules for e-commerce in order to enhance the quality of information concerning products, services and suppliers.[28]

III. Applicability of data protection acts

The Civil Code applies to private relationships involving individuals and legal entities. As data protection acts in Brazil are of a sectoral character regulating specific issues (e.g. consumer protection, telecommunication, Internet), they are only applicable in the relevant sector. A more general data protection provision, such as the aforementioned *habeas data* writ, applies only with regard to access to personal information before public bodies.

Consumer law can be applied to enforce consumer privacy in the case of any relationship involving a consumer and a supplier,[29] while the Credit Information Law applies merely to database-related issues concerning financial data. According to the CDC, any transaction between a consumer and a supplier, where at least one major part of the transaction took part in Brazil, falls under its jurisdiction. Therefore, consumer law applies whenever a product or service was bought or provided in Brazil. However, enforcement might prove difficult when suppliers operate beyond Brazilian borders.

With regard to the use of data collected on the Internet, Internet connection and application providers must comply with Brazilian laws in the following cases: if collection, storage or treatment of personal data occurs in Brazil, if at least one of the terminals involved in the communication is located in Brazil, or if the providers offer services to Brazilians or have, directly or through a company pertaining to their group, an establishment in Brazil.[30] The Brazilian Internet Civil Rights Framework applies to Internet users in general, Internet connection providers (which promote the transmission of data packages between terminals over the Internet) on the assignment or authentication of an IP address, and Internet application providers (which provide a set of features that can be accessed by a terminal connected to the Internet).[31] The Act establishes that any treatment of personal data that is processed in Brazil, even partially and merely collected by means of a terminal located inside the territory, must comply with Brazilian legislation. Article 11 reads as follows:

---

[27] <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm> (last accessed June 26, 2015).

[28] See Article 1 of Decree No. 7.962 of 2013.

[29] See CDC, Articles 2 and 3.

[30] See Law No. 12965 of 2014 (Brazilian Internet Civil Rights Framework), Article 11, paragraph 1.

[31] See Law No. 12965 of 2014 (Brazilian Internet Civil Rights Framework), Article 5.

> *In any operation of collection, storage, retention and treating of personal data or communications data by connection providers and Internet applications providers where, at least, one of these acts takes place in the national territory, the Brazilian law must be mandatorily respected, including in regard the rights to privacy, to protection of personal data, and to secrecy of private communications and of logs.*
>
> *§1°. The established in Art. 11 applies to the data collected in the national territory and to the content of the communications in which at least one of the terminals is placed in Brazil.*
>
> *§2°. The established in Art. 11 applies even if the activities are carried out by a legal entity placed abroad, provided that it offers services to the Brazilian public or at least one member of the same economic group is established in Brazil.*

Foreign companies are subjected to this rule whenever they provide services to Brazilian citizens. This means that even if a company does not particularly focus and approach Brazilian users, but admits them as customers, the provisions of the Internet Civil Rights Framework shall apply. The same applies if the company has a subsidiary in Brazil. In this context, it is worth mentioning that, during the last decade, Brazilian courts have debated jurisdiction issues related to foreign Internet companies with small operations in Brazil, but whose services are mainly provided by their foreign operations. In such cases, Brazilian jurisprudence tended to hold Brazilian subsidiaries liable for Internet services, even if those services were not provided by them in a technical sense.

This approach of multiple statutes aimed at regulating personal data can make it legally more and more complex when the number of new statutes concerning consumer data protection continues to grow.

IV. Definitions of consumer and data

The CDC uses a broad concept of a consumer, which allows its application in a variety of cases, even beyond the strict contractual relation between consumer and trader. The consumer can be either a natural person or a legal entity. The Consumers' Code contains four definitions of who can be considered a consumer. Firstly, according to the standard definition, a consumer is any physical person or corporate entity who acquires or uses a product or service as a final user.[32] Secondly, a consumer is also a group of persons who participate in consumer relations.[33] Thirdly, a consumer is anyone who has suffered damages caused by a

[32] Article 2. – "Consumer is any individual or body corporate who acquires or uses any product or service as an end user."

[33] Article 2. Sole Paragraph. – "Any group of persons, even if unidentifiable, whose activities might intervene in the consumer relations, shall be understood as consumer."

commercial activity.[34] Fourthly, any person who is exposed to a commercial practice, such as advertising or databases, is also considered a consumer.[35] In any of these cases, the CDC applies. Thus, a citizen does not need to prove any contractual relation to exercise their rights to correction and disclosure of their personal information, e.g. illegally contained in a database. It also means that consumer damage claims can be directed not only against the person or enterprise with which they have a contract, but also against the party responsible for the database. That is why the data protection norms of the CDC have had a much broader application than the strict relation between consumers and traders, promoting a modernization that extended beyond consumer relations. It is important to observe that financial institutions must also comply with the CDC. This understanding was confirmed by the Federal Supreme Court in its Informative Acts 452, 430, 425, and 417, and in its ruling of the Unconstitutionality Claim ADI 2.591/DF of 6 July 2006. Therefore, the definition of a consumer under the CDC covers any individual or legal entity that utilizes, as a final consumer, banking, financial and credit services.

The CDC does not only define a consumer as the final intended party that purchases goods or contracts services (Article 2 of the CDC). In regard to the supplier, product and service, Article 3 of the CDC defines them as follows: The supplier is any individual or legal entity, public or private, domestic or foreign, as well as depersonalized entities engaged in the activities of production, assembly, creation, construction, transformation, import, export, distribution, or commercialization of products or service. The product is any movable or immovable good, material or immaterial, while the service is considered as any activity supplied in the consumer market, upon remuneration, including banking, financial, credit, and insurance activities, except those that are supplied under labor agreements.

There is no general legal definition of "personal data" established in a particular statute in Brazil. However, based on decisions of the Brazilian courts, it is argued that any data which can be used to identify an individual (for example, the name, ID and taxpayer number of the individual) should be considered personal data for the purposes of the Data Privacy Regulations. In general, "personal data" should be considered to include any particular information related to an individual, including name, age, sex, profession, or address, as well as any personal communication exchanged without any intent to go public, such as personal e-mails and messaging.

It is argued that the Constitution makes a distinction between the concepts of communication and other uses of personal data, as article 5, XII, of the constitu-

[34] Article 17. – "For the effects of this Section, all the victims of the event are equivalent to consumers."

[35] Article 29. – "For the purposes of this Chapter and following, every individual, identifiable or not, that is exposed to the practices provided for herein shall be understood as a consumer."

tion recognizes the right to the "communications data secrecy," which only applies to communication data and not to any data that are occasionally stored. Therefore, it is argued that the constitution only grants protection to communications data and not to any data in general. Consequently, any attempt to protect personal data as a constitutional right presupposes that the personal data in question are related to the intimate and private life of an individual.

The only definition of personal data in Brazilian legislation can be found in the Access to Information Law (Law No. 12.527 of 2011), which refers to any information pertaining to the natural person, whether identified or identifiable.[36] This definition of personal data only relates to the natural person, not to legal entities. However, in private law, privacy is also considered as one of the so-called rights to personhood. In this sense, it can also apply to legal entities. Article 52 of the Brazilian Civil Code, for example, mentions that the rights of the personhood apply, "to the necessary extent," to legal entities.

In general terms, Brazilian laws do not establish different kinds of personal data, e.g. by establishing distinctions with regard to legal concepts such as "sensitive data." The only reference to "sensitive information" can be found in the Credit Information Law, which forbids the recording of such information. According to its Article 3, "[r]ecord must not be made of [...] sensitive information, being considered as such those information related to the social and ethnicity origin of an individual, his health, genetic information, sexual orientation, and political, religious and philosophical beliefs." Moreover, professional secrecy laws, as in the case of ministers and physicians, also protect some of these values.

V. General guiding principles

Despite the lack of a comprehensive data protection law, general data protection principles can be identified in essentially all specific acts of relevant sector legislation. The principle of access is probably the one with the most robust formulation in Brazilian Law, as it is clearly based on the Brazilian Constitution – more precisely, the *Habeas Data* writ, as already mentioned. There is no law establishing general data quality obligations. However, both the CDC and the Credit Information Law impose that data must be: objective, clear, truthful, and easily understandable (Article 43 of CPC and Article 3, para. 2 of the Consumer Information Law). In the CDC, some privacy principles are contained in Article 43.[37] According to this, the consumer's right to access to data is granted. Consumers' files must be objective, clear, truthful, easily understood, and cannot contain the same negative information (regarding unpaid duties) for more than five years. In respect to

[36] See Article 4, IV – personal information: information pertaining to the natural person, whether identified or identifiable.

[37] *Gambogi Carvalho*, O consumidor e o direito à autodeterminação informacional, in: Revista de Direito do Consumidor, n. 46, abril-junho 2003, pp. 77-119.

this negative information, the consumer must be explicitly informed that such data was recorded. Moreover, a right to rectification of inaccurate or incomplete data is granted (Article 43 CPC). Credit information protection is addressed more extensively under the Credit Information Law (Law No. 12.414 of 2011). Finally, Article 7 of the Internet Civil Rights Framework contains the rights and guarantees of Internet users:

- "inviolability of intimacy and private life, safeguarding the right for protection and compensation for material or moral damages resulting from their breach;
- inviolability and secrecy of the flow of user's communications through the Internet, except by court order, as provided by law;
- inviolability and secrecy of user's stored private communications, except upon a court order;
- non-suspension of the Internet connection, except if due to a debt resulting directly from its use;
- maintenance of the quality of Internet connection contracted before the provider;
- clear and full information entailed in the agreements of services, setting forth the details concerning the protection to connection records and records of access to Internet applications, as well as on traffic management practices that may affect the quality of the service provided;
- non-disclosure to third parties of users' personal data, including connection records and records of access to Internet applications, unless with express, free and informed consent or in accordance with the cases provided by law;
- clear and complete information on the collection, use, storage, processing and protection of users' personal data, which may only be used if it:
  a) justifies its collection;
  b) is not prohibited by law; and
  c) is specified in the agreements of services or in the terms of use of the Internet application.
- the expressed consent for the collection, use, storage and processing of personal data, which shall be specified in a separate contractual clause;
- the definitive elimination of the personal data provided to a certain Internet application, at the request of the users, at the end of the relationship between the parties, except in the cases of mandatory log retention, as set forth in this Law;
- the publicity and clarity of any terms of use of the Internet connection providers and Internet applications providers;

- accessibility, considering the physical, motor, perceptive, sensorial, intellectual and mental abilities of the user, as prescribed by law; and
- application of consumer protection rules in the consumer interactions that take place in the Internet."

VI. Collecting, storing and processing consumer data

The Data Privacy Regulations apply to the collection, storage, treatment, and use of any personal data. However, the concepts of collecting, storing and processing personal data are not explicitly defined in Brazilian Law.

VII. Approaches to consent

There is no general approach to consent for the treatment of personal data in Brazilian Law. Some references can be found in sector legislative acts, such as the CDC, the Credit Information law and the Internet Civil Rights Framework. The Credit Information Law establishes that prior consent is necessary for the collection of so-called "positive financial data," i.e. data regarding regular financial operations by an individual. In the Internet Civil Rights Framework, consent is needed for processing personal data. It corroborates the general privacy principles provided in the CDC, i.e. the collection and use of personal data is subject to the data subject's prior and express consent. It also determines that the terms and conditions of any Internet application or website regarding the collection, use, storage, and treatment of personal data must be highlighted in a manner easily identifiable by the respective user in the applicable agreement and terms of use. According to Article 7 of the Internet Civil Rights Framework, the users' rights include "the guarantee that personal data, including connection logs and access to Internet applications records will not be shared with third parties, except upon the user's express free and informed consent or as provided by law." Consent is here presented as the instrument the individual can use to decide whether their personal data will (or will not) be disclosed or transmitted to third parties. The connection logs and Internet applications records mentioned here will be further dealt with later. The consent must be free, i.e. it must correspond to the actual will of the citizen, not being forced by any means, and informed, i.e. the citizen must have received enough information in order to know the context and the consequences of their choice; both requirements are very important criteria that must inspire industry to be clear and precise when informing and asking for citizens' consent.

In the case of data collection on the Internet, the expressed consent for the collection, use, storage, and processing of personal data shall be specified in a separate contractual clause. Therefore, the provisions regarding collection and use of personal data must be highlighted in the applicable agreement/terms of use. To ensure compliance, a website can have hyperlinks which guide Internet users to its

privacy policies and regulations, either on its homepage or on the data collection page. Access to the website is then made subject to the acknowledgement by the user of the privacy policy and their express consent to the terms of the privacy policy regarding collection, use, storage, and treatment of personal data.

Minors under 16 years old are not able to give consent and must be represented by their legal guardian. Minors between 16 and 18 years old can give consent with the assistance of their legal guardian. In relation to consent obtained through the Internet, it is normal to ask users to confirm that they are over 18 years old and, therefore, have the legal capacity to accept terms of use and other conditions.

Explicit consent is required for the collection, treatment, storage, and use of consumer's personal data or personal data collected on the Internet. An Internet user's silence cannot be considered as implied consent in Brazil.[38]

VIII. Publicity and transparency

Several provisions in Brazil's consumer legislation contain references to the principles of publicity and transparency. The access to education and information about the adequate level of consumption of products and services, and the right to adequate and clear information about products and services are defined as basic consumer rights in the CDC.[39] The Code also makes it compulsory to inform the consumer that a database with their data has been created.[40] Case law has established that the consumer must be informed about the creation of the database; however, their consent or authorization for the creation is not necessary.[41] The Credit Information Law establishes transparency rules, which are only applicable to financial consumer data.[42] There is currently no regulation regarding notification of data breaches in Brazil. Any incident involving data breaches can be addressed by means of civil liability in the case of damages inflicted on the data owner.

[38] See Law No. 12965 of 2014 (Brazilian Internet Civil Rights Framework), Article 7, VII.

[39] See Article 6. The following are basic consumer rights: "[…] II - education and information about the adequate level of consumption for products and services, ensuring freedom of choice and equality in hiring processes; III - adequate and clear information about different products and services, with correct specifications for quantity, characteristics, composition, quality and price, as well as any risks involved."

[40] See Article 43, § 2° "The opening of a file or record of personal and consumption data shall be communicated in written form to the consumer, in case it has not been requested by him."

[41] See CDC, Article 43.

[42] See, among the most relevant ones, those contained in Article. 5: The rights of the data owner are: II - to access, free of charge, information about him in databases, including his credit history.

IX. Data security

There is no specific legal requirement concerning security of personal data. In view of applicable general principles, data processors in Brazil are required to take reasonable technical, physical and organizational measures to protect the security of personal data, due to general liability rules and good faith standards. However, there are no specific regulations, requirements, restrictions, or details on how security should be implemented and guaranteed. The Internet Civil Rights Framework establishes provisions regarding the security of personal data. For the storage and processing of personal data, security and confidentiality measures and procedures must be informed in a clear manner by the party responsible for the provision of the services.[43]

Case law establishes the obligation of service providers and networks to establish and maintain access records (e.g. IP addresses and logins), in order to be able to identify users who might commit crimes or acts of infringement. If such records are not kept for a reasonable period of time, the service provider or network may be held jointly liable for an act of infringement.[44] The data security standards must be informed to the Internet user and comply with standards (yet to be defined in a regulation) which will be produced by the Federal Government.

X. Data control, data portability and the right to access, modify and delete collected data

As already mentioned, the right to access personal data is a right of the data owner, enforceable by means of the *Habeas Data* Writ. The CDC contains provisions regarding access to data in its Article 43. It determines that whenever a database with consumer information is created, the consumer must be informed; and all data stored about them must be accessible. Consumers are entitled to have access to any personal or commercial information that concerns them. Allowing access to personal data stored in consumer databases is mandatory, even when the consumer has agreed previously to its collection. Databases with consumer information must be objective, clear and created in a language that is easy to understand. Negative credit information must not be stored for more than five years. A consumer is entitled to request the updating or correction of any inaccurate personal information stored in any database, regardless of their previous authoriza-

[43] See Article 10. "The retention and the making available of connection logs and access to Internet applications logs to which this law refers to, as well as, of personal data and of the content of private communications, must comply with the protection of privacy, of the private life, of the honor and of the image of the parties that are directly or indirectly involved. […] §4. The security and confidentiality measures and procedures shall be informed in a clear manner by the responsible for the provision of the services, and meet the standards set in regulation, in compliance with rights of confidentiality of business secrets."

[44] See Law No. 12965 of 2014 (Brazilian Internet Civil Rights Framework), Article 2, paragraph 2, III.

tion for the collection of the relevant data. Any request for correction or updating must be addressed within five business days. In addition, consumers are entitled to request the exclusion of their personal data from databases, unless the relevant database is a credit protection database. Internet users can request the deletion of their personal data from the database of Internet applications at the end of their relationship with the provider. This right does not apply in relation to the mandatory retention provisions. In addition, the Credit Information Law establishes a set of provisions regarding free access to consumer's financial data. There are currently no specific provisions on data portability. The Internet Civil Rights Framework establishes the right for the user to access all data. Decree No. 7.962 of 2013 aims at regulating online consumer services and highlights the need for transparency of information regarding products, services and suppliers and their methods of operation, including data processing. In addition, Article 7 of the Internet Civil Rights Framework requires the definitive elimination of the personal data provided to a certain Internet application, at the request of the users and at the end of the relationship between the parties, except in the cases of mandatory log retention.

As a general principle, consumers can object to the processing of their data, but this might prevent them using the service. The CDC and the Internet Civil Rights Framework determine that consumers must have the option to delete and change data of the databases which contain their personal and consumer data.[45]

XI. Roles and responsibilities of intermediaries

There is no equivalent of the distinction between the concepts of data controller and data processor in Brazilian Law. However, the Internet Civil Rights Framework distinguishes between Internet connection[46] providers and Internet application[47] providers. It exempts Internet connection providers from civil liability for contents generated by third parties.[48]

Liability of Internet application providers for damages generated by third party content arises only in cases in which, after a specific court order has been issued,

[45] The provisions about user's data in the Internet Civil Rights Framework stress the transparency and clearness of the contractual clauses about user's data. The debate about their proportionality has not yet been well established, even if it could be evoked by the reading of the good faith clause in the consumer law.

[46] See Article 5, V - Internet connection: designation of a terminal for delivery and reception of data packets through Internet, by means of election or authentication of an IP address.

[47] See Article 5, VII – Internet application: a set of features that can be accessed by a terminal connected to the Internet.

[48] See Article 18. The provider of connection to Internet shall not be liable for civil damages resulting from content generated by third parties.

no steps are taken to make the third party's content unavailable.[49] Article 21 establishes an exception with regard to Internet applications with a sexual content.[50]

XII. Access to user data by third parties

There are no specific provisions concerning the possibility of a third party processing personal data on behalf of the entity that collected the data. Therefore, sharing personal data with third parties for commercial reasons can be interpreted as not being permissible under consumer law. It is argued that this processing must be authorized by the data subject.[51] Nonetheless, it cannot be ignored that it does happen in practice due to the lack of clear rules and judicial precedent concerning a general application of the purpose principle.

XIII. Provisions on data retention

Debate about data retention duties have increased in Brazil in the last five years. The National Telecommunication Agency (ANATEL), in its resolution 614, determines in Article 53 that telecommunication enterprises must retain the logs (metadata) of telephones for one year.[52] The CDC determines that data concerning unpaid financial duties of the consumer can be retained for up to five years.[53] Data retention duties were also introduced by the Internet Civil Rights Framework. The possibility of data retention performed by Internet providers, which is one of the main reasons of the very existence of the Act and led to controversial discussions during the drafting process, was first proposed as a counterpart to another bill that proposed mandatory data retention within a legal framework based upon criminal sanctions. The Act establishes a mandatory minimal retention of one year and six months respectively for logs of access to Internet connection providers[54] and commercial Internet applications,[55] i.e. Internet connection pro-

[49] See Article 19. In order to ensure freedom of expression and prevent censorship, the provider of Internet applications can only be subject to civil liability for damages resulting from content generated by third parties if, after an specific court order, it does not take any steps to, within the framework of their service and within the time stated in the order, make unavailable the content that was identified as being unlawful, unless otherwise provided by law.

[50] See Article 21. The Internet application provider that makes third party generated content available shall be held liable for the breach of privacy arising from the disclosure of images, videos and other materials containing nudity or sexual activities of a private nature, without the authorisation of the participants, when, after receipt of notice by the participant or his/hers legal representative, refrains from removing, in a diligent manner, within its own technical limitations, such content.

[51] *Ejnisman/Cinci Silva*, Data Protection in Brazil: Overview, < http://us.practicallaw.com/4-520-1732#a994883> (last accessed 25 June 2015).

[52] See Resolution 614 of Anatel: ≤http://www.anatel.gov.br/legislacao/resolucoes/2013/465-resolucao-614L (last accessed 7 August 2015)

[53] See CDC, Article 43, paragraph 1.

[54] see Article 5, V: "Internet connection: the enabling of a terminal for sending and receiving data packets over the Internet, by assigning or by authenticating an IP address; VI: connection log: a

viders must store connection registrations (that is, information regarding the date, time, duration, beginning and end of the connection, the IP address used for sending and receiving data packages) confidentially for one year,[56] while Internet application providers must store registrations of access to Internet applications (date, time, duration, beginning and end of an application, and the IP address) for six months.[57] However, on request from the police authorities, administrative authorities or the Ministry of Public Prosecution, the six month and one year terms can be extended (no judicial order is needed for the extension but the request for a judicial order must be filed within 60 days; furthermore, there is no maximum time limit for data retention). The log must be kept by the company which collects it. In order to comply technically with this obligation, the company must not use a contractor or third party as a "data processor."[58] The Internet Civil Rights Framework strictly demands the separation of Internet connection logs (kept by ISPs) from "Internet application" logs, making it a key tool of its privacy framework.

These provisions concerning data retention of Internet application logs constitute an extreme measure, as they not only drastically increase the volume of personal data being kept as a result of regular Internet navigation, but they also make it impossible to run several kinds of privacy-friendly services, which are not meant to preserve records of their normal use. Keeping more data means not only increased costs for Internet enterprises, but also negative consequences for Internet users, such as the risks of data misuse, unauthorized access and accidental disclosure. Even though the records mentioned do not directly contain personal information, it is clear that they will be only be useful in cases when they can be related to an identifiable individual. Therefore, for the purposes proposed, they must be considered as equivalent to personal data. This kind of mandatory log was a last-minute addition to the Bill that was not fully discussed as other provisions were. Practically no equivalent can be found in other legislation (in fact, data retention

set of information regarding the date and time that the Internet connection begins and ends, its duration and the IP address used by the terminal to send and receive data packets."

[55] See Article 5, VII: "Internet applications: a set of functionalities that can be accessed through a terminal connected to the Internet."

[56] See Subsection I: Keeping of connection records. Article 13. "In the provision of Internet connection, the entity responsible for the management of the autonomous system must maintain the connection records, under confidentiality, in a controlled and safe environment, for the term of 1 (one) year, in accordance with regulations."

[57] See Subsection III: Keeping of records of access to the Internet applications. Article 15. "The Internet application provider that is duly incorporated as a legal entity and carry out their activities in an organized, professional and with economic purposes must keep the application access logs, under confidentiality, in a controlled and safe environment, for 6 months, as detailed in regulations."

[58] See Article 13. § 1: "The responsibility for retaining connection logs cannot be transferred to third parties."

usually refers to ISP logs and not logs from Internet sites). It is doubtful if the provisions are in line with the principles of proportionality and economy.

XIV. Transfer of data on an international scale, transfer to third countries and requirements for data transfer outside the country

Currently there is no legal provision in Brazil regulating transborder flow of personal data. There are no restrictions on the transfer of data outside Brazil. However, foreign companies storing Brazilians' private data have to comply with Brazilian laws. Data transfer agreements are not usually adopted. There is also no standard form or precedents for these agreements.

It is worthwhile mentioning that Brazil was one of the founders in the 1970s of the Intergovernmental Bureau for Informatics (IBI), a group of developing countries whose task was to establish rules for the transborder flow of data. Law No. 7.232 of 1984 envisaged in its Article 7, X, that the National Council for Computers and Automation (CONIN) should discuss and decide how policies regarding information and the transborder flow of data should be dealt with. However, none of these efforts and discussions led to a regulation on the transborder flow of data. In the meantime, some critical issues have been addressed by specific industry standards and self-regulations, such as the SWIFT (Society for Worldwide Interbank Financial Telecommunication) system for the financial market or the SITA (Société Internationale de Télécommunications Aéronautique) for aeronautics.

The transmission of consumer information to foreign bodies has occurred beyond the boundaries of coordination and regulation, e.g. in the case of passenger flight lists handed over to U.S. authorities. Consequently, decisions regarding data transfer currently occur on a case-to-case basis without adequate and detailed regulation.

XV. Enforcement

The administrative departments that can address issues related to consumer privacy are part of the National System of Consumer Protection (SNDC), a pool of state and municipal public bodies that can apply consumer protection legislation in order to protect consumer's data. There exist currently 786 public bodies, which are known by the name Procon, which stands for Procuradoria de Proteção e Defesa do Consumidor (Ombudsman for Consumer Protection and Defense). Although it is a state institution, municipal governments can also establish a Procon. The first Procon office was created in the state of São Paulo in 1970 even before the Consumer Defense Code was promulgated. Other Brazilian states took it as an example and opened offices. Today, all Brazilian state capitals have at least one Procon office responsible for guiding consumers in their complaints, giving information about their rights and verifying the consumption relations.

The federal government body in charge of consumer protection (non-exclusively) is the National Secretariat of Consumer of the Ministry of Justice. The SNDC is also integrated by other public bodies that have the power to enforce consumer law: the Federal Public Minister at the federal level, Public Ministers in each of the 27 Brazilian States, and the Offices of the Public Defendant. There is no hierarchy among these public bodies, as each one of them is part of an autonomous federative body (the union, the state or the municipality). Therefore, they are all autonomous in their application of consumer law to protect consumers' privacy.

The National Consumer Defense Policy is coordinated by the Consumer and Protection Defense Department (DPDC), which is subordinated to the Secretariat of Economic Law of the Ministry of Justice. In 2012, consumers could use approximately 1.3 million service stations throughout the country. Among the institutions responsible for consumer rights are the aforementioned Procon offices and their similar bodies in states and municipalities, the Health and Agricultural Surveillance, the National Institute of Metrology Standardization and Industrial Quality (Inmetro) and the Institute of Weights and Measures (IPEM), special Courts (apart from regular justice services), the Public Prosecution Offices linked to the Office of the Public Interest Attorney, specialized police stations, civil entities for consumer protection, the Brazilian Tourism Board (Embratur), and the Private Insurance Superintendence (SUSEP).

There are several ways consumers can protect themselves against violations of their right to privacy and data protection. Firstly, if the violation is related to a consumer relationship, consumers can lodge a complaint before the governmental supervisory authorities, which can impose fines and determine that certain activities which infringe on consumer rights must be omitted (Article 56 of the CDC). Secondly, NGOs, the Public Prosecution and some government agencies can claim judicial remedies (i.e. class actions) against every party responsible for a consumer rights violation. The Consumer DC expressly authorizes consumers to adopt class action lawsuits and public lawsuits (Law No. 7.347 of 1985) to defend the interests and rights of the consumers as a collectivity (Article 81 *et seq.*). They may lodge, in their own name and in the interests of the victims or their successors, a class action for indemnification of the damages that were individually suffered in accordance with the law. Thirdly, under constitutional and consumer law provisions, consumers have the right to initiate individual judicial procedures against those responsible for consumer rights violations.[59]

[59] *Costa*, A Brief Analysis of Data Protection Law in Brazil, June 2012, presented to the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD), p. 8.

1. Civil law

The principles of civil liability are contained in the general clause of the Civil Code, in conjunction of Articles 186 and 927.[60] The notion of moral damages is the basis for the reparation of illicit acts (violation of the right to privacy and data protection). In fact, privacy is one of the rights of the personhood in the Brazilian Civil Code.[61] These general rules concerning civil liability, however, do not apply when other provisions concerning consumer protection, e.g. the CDC, are more specific on the matter. Under the Civil Code, for example, burden of proof would fall on the data owner, while under the CDC, it generally falls on the data controller, making it a more favorable regime for the consumer. Contrary to civil law, which requires proof of fault, under consumer law, the plain existence of damage effectively caused to the consumer will suffice. This means that the supplier (e.g. producer, distributor, dealer) can be held accountable for any damage caused to the consumer irrespective of the supplier's degree of fault, as the consumer presumably lacks the conditions for defense due to economical or technical disadvantages. Accordingly, strict sense liability intends to place the consumer and the supplier on a same level. The CDC, therefore, establishes mechanisms for the effective judicial protection of the consumer in order to facilitate their defense, such as the "reversal of the burden of proof," "strict sense liability," and "indemnification of patrimonial and moral damages," among others.

The Internet Civil Rights Framework introduces specific penalties for Internet connection and application providers if they violate data privacy obligations. Any or all of the following penalties can be applied, regardless of further civil, criminal and administrative penalties: a warning, a fine of up to 10 % of the gross revenues of the economic group in Brazil, or temporary or permanent suspension of activities. Article 12 reads as follows:

> *Art. 12. Without prejudice to any other civil, criminal or administrative sanctions, the infringement of the rules set forth in the Articles 10 and 11 above are subject, in a case basis, to the following sanctions applied individually or cumulatively:*
>
> *I – a warning, which shall establish a deadline for the adoption of corrective measures;*
>
> *II – fine of up to 10% (ten percent) of the gross income of the economic group in Brazil in the last fiscal year, taxes excluded, considering the economic condition of the infractor,*

[60] Article 186. "Anyone that, for voluntary action or omission, negligence or imprudence, violate and cause damage to another person, even if exclusively moral, commits an illicit act." Article 927. "Anyone that, by means of an illicit act, causes damage to another persona is obliged to repair it."

[61] Article 21. "The private life of the natural person is inviolable and the judge, after requirement of the interested part, can take the necessary measures to avoid or finish acts that are contrary to this rule."

the principle of proportionality between the gravity of the breach and the size of the penalty;

III – the temporary suspension of the activities that entail the events set forth in Article 11; or

IV – prohibition to execute the activities that entail the activities set forth in Article 11.

Sole paragraph. In case of a foreign company, the subsidiary, branch, office or establishment located in the Country will be held jointly liable for the payment of the fine set forth in Art. 11.

With regard to the establishment of special courts, Article 19, Para. 3 of the Internet Civil Rights Framework determines that compensation disputes for damages arising from content made available on the Internet related to the honor, reputation or personality rights, as well as the removal of related contents by Internet application providers, can be presented to special small claims courts.[62]

2. Criminal law

The CDC criminalizes some conduct directed against the consumer and their right to adequate information.[63] However, in practice, this conduct is rarely, if ever, sanctioned by courts.

3. Administrative law

There is no data protection authority in Brazil, since no data protection law is enacted. Nevertheless, consumer protection authorities are entitled to act in defense of the consumers if the latter's personal data is misused or if their rights to privacy are violated, according to the general measures defined in the Consumer Defense Code. The administrative structure which is also in charge of enforcing consumer law in Brazil is entitled to deal with consumer privacy issues. However, it does not have a specialized infrastructure, nor does it currently receive specific technical training and capacity-building support in privacy and data protection issues.

There are no specific legal provisions, standards or case law relating to the penalties and amounts payable for data privacy violations by Brazilian companies. Therefore, the competent court or judge has to determine the penalties and amounts payable by examining the particular circumstances of the case.

[62] Article 19, Para. 4 of the Internet Civil Rights Framework.

[63] See Article 72. "Preventing or hindering access by the consumer to information on himself in records, data banks, cards or an registers: Penalty: Six months to one year's imprisonment or fine." Article 73. "Failure to immediately correct information on consumers in records, data banks, cards or registers, which the person knows or ought to know is inaccurate: Penalty - one to six months' imprisonment or fine."

Finally, Art. 24 of the Internet Civil Rights Framework sets out the guidelines for the performance of the Federal Government, states, Federal District and municipalities in the development of the Internet in Brazil, among them:

- establishment of mechanisms of governance that are multi-stakeholder, transparent, cooperative and democratic, with the participation of the government, the business sector, the civil society and the academia;
- promotion of the rationalization of management, expansion and use of the Internet, with the participation of Brazilian Internet Steering Committee (CGI.Br);
- promotion of rationalization and technological interoperability of e-Government services, within different branches and levels of the federation, to allow the exchange of information and speed of procedures;
- promotion of interoperability between different systems and terminals, including among the different federal levels and different sectors of society;
- preferred adoption of open and free technologies, standards and formats;
- advertising and dissemination of public data and information in an open and structured manner;
- optimization of network infrastructures and promoting the implementation of storage, management and dissemination of data centers in the country, promoting the technical quality, innovation and the dissemination of Internet applications, without impairment to the openness, neutrality and participatory nature;
- development of initiatives and training programs for Internet use;
- promotion of culture and citizenship; and
- provide public services for citizens in an integrated, efficient and simple manner and through multi-channel access, including remote access.

XVI. Role of self-regulation and co-regulation

Self-regulatory efforts in Brazil regarding privacy and data protection are rather scarce. The most relevant initiative in this regard was the "E-mail Marketing Self-Regulation Code" (*Código de Autorregulamentação para a Prática de E-mail Marketing,* C@PEM)[64] in 2009. The code was issued as a response to the problem caused by the high volume of junk mail in Brazil, and was promoted by a group of entities and organizations including Internet providers, and commercial, marketing and consumer associations, among others. The companies that are signatories to the code accept that e-mail marketing is only possible when requested by the Internet user or due to a prior commercial relationship between the sender and the user. If

[64] <http://www.capem.org.br/arquivos/codigo.pdf>

a company does not comply, the issue can be brought before an Ethics Committee, which will decide on sanctions. Another measure to be mentioned, although not of a self-regulatory nature, is the possibility of blocking Internet providers in order to fight against spam. It is an effort, coordinated by the Brazilian Internet Steering Committee (www.cgi.br), which was created in 1995, with the purpose of coordinating and integrating all Internet service initiatives in Brazil, as well as promoting technical quality, innovation and the dissemination of the services available. Finally, a data protection draft bill, currently being submitted to a public debate, is trying to introduce the principle of self-regulation as a standard market practice.[65]

B. Consumer Data Protection in China *(Prof. Dr. Zhou Hanhua)*

I. Introduction

In December 2014, China had 649 million Internet users, with an increase of 31.17 million new users in that year. The Internet penetration rate was 47.9%, an increase of 2.1% from 2013. There were 557 million mobile Internet users, with an increase of 56.72 million compared to 2013. Across all Internet users, the proportion of those using mobile phones to access the Internet rose from 81% in 2013 to 85.8% in 2014. Internet users in rural areas made up 27.5% of Internet users in China, reaching 178 million (1.88 million more than in 2013). Among Chinese users, a percentage of 70.8% and 43.2% respectively accessed the Internet via desktop and notebook computers; 85.8% used mobile phones, an increase of 4.8%; 34.8% used tablet computers; and 15.6% used televisions. Finally, there were 20.6 million domain names registered in China, among which the.cn domain names increased by 2.4%, reaching 11.09 million and accounting for 53.8% of all the domain names in China. There were 3.35 million websites in China with an annual growth of 4.6%, and the Internet bandwidth at the international exit was 4,118,663Mbps, an annual growth of 20.9%.

[65] <http://dadospessoais.mj.gov.br/>

II. Overview and scope of legislation addressing consumer data protection

China does not have legislation that specifically addresses the collection, storage, transmission and operation of personal information. There are no regulations comparable to the EU model of personal data protection law, nor has China entered into any treaty with the EU or any agreement similar to the EU-US Safe Harbor framework. There are a few provisions in the laws and regulations, which generally address the protection of personal information by regulating specific industrial sectors (e.g. the telecommunication sector) or referring to certain information of a specific nature (e.g. individual financial credit information, consumer information, population health information and medical records).

1. Character of the legislation

The legal system in China consists of the Constitution, national laws, administrative regulations, local decrees, administrative rules and local rules. In addition, the judicial interpretations issued by the Supreme People's Court and the Supreme People's Procuratorate are also legally binding. China possesses a diversified and multilevel legislative system. Legislative power is exercised by the National People's Congress and its Standing Committee.[66] The State Council enacts administrative regulations in accordance with the Constitution and national law. Administrative regulations deal with matters that require the enactment of administrative regulations for the implementation of a national law, or matters which are subject to the administrative regulation of the State Council under Article 89 of the Constitution. It might be the case that a national law of the National People's Congress and its Standing Committee should regulate a given matter, but, pursuant to an enabling decision issued by the National People's Congress and its Standing Committee, this matter is instead regulated by the State Council through an administrative regulation. If the conditions for enactment of the relevant national law develop or change, the State Council shall submit a timely request to the National People's Congress and its Standing Committee for the enactment of the relevant national law.

In specific situations and given actual need to exercise jurisdiction, the People's Congress of a province, autonomous region or municipality, subordinate to the central government and its Standing Committee, may enact local decrees if they do not contravene any provision of the Constitution, national law or administrative regulations. The same applies for the People's Congress and its Standing

[66] The National People's Congress enacts and amends criminal, civil, and state organic and other basic laws. The Standing Committee enacts and amends laws that are not enacted by the National People's Congress. While the National People's Congress is not in session, the Standing Committee can amend and supplement national law enacted by the National People's Congress, provided that the amendments or supplements do not contravene the laws.

Committee in a major city, which may enact local decrees in accordance with any provision of the Constitution, national law, administrative regulations and local decrees in the province or autonomous region in which the city is located. Such local decrees[67] shall be implemented after being reviewed and approved by the Standing Committee of the People's Congress of the province or autonomous region. In this context, a major city refers to a city where the People's Government of the province or autonomous region is based or a special economic zone is located, or any other major city approved by the State Council. The People's Congress of a province or city where a special economic zone is located and its Standing Committee shall, pursuant to an enabling decision issued by the National People's Congress, enact decrees for implementation within the special economic zone.

The various ministries, commissions, the People's Bank of China (PBOC), the Auditing Agency, and a body directly under the State Council exercising regulatory function, may enact administrative rules in accordance with national law, administrative regulations, as well as decisions and orders of the State Council. The People's Government of a province, an autonomous region, a municipality directly under the central government, or a major city, may enact local rules in accordance with national law, administrative regulations and local decrees of the province, autonomous region, or municipality directly under the central government.[68]

The main regulations concerning consumer data protection can be found in the following legal instruments: the Constitution, the *Consumer Rights Law*, the *Decision of the Standing Committee of the National People's Congress concerning Strengthening Network Information Protection* (*NPC Decision*), the *Decision of the Standing Committee of the National People's Congress on Revising the Consumer Rights Protection Law of the People's Republic of China* (*Consumer Rights Law*), the *Regulation on Personal Information Protection of Telecom and Internet Users* (*MIIT Regulation*), the *Administrative Measures for Online Transactions*, the *Personal Information Security Measures for Mailing and Courier Services*, the *Medical Records Administration Measures of Medical Institutions*, and the *Measures for the Administration of Population Health Information* (*PHI Measures*).[69]

In China, legislation concerning personal information protection has developed in three steps. Initially, instead of using concepts of privacy or personal information, Chinese legislation adopted the notion of *"Yin Si"* (literally, "private

[67] A local decree deals with matters that require the enactment of a local decree in order to implement a national law or administrative regulation, or that are of a local nature and require the enactment of a local decree.

[68] A local rule deals with matters that require the enactment of local rules in order to implement a national law, administrative regulation or local decree, or matters within the scope of the local jurisdiction.

[69] See *Xiao Dong*, Data Protection in China: Overview, <http://uk.practicallaw.com/4-519-9017?q=*&qp=&qo=&qe=> (last accessed June 25, 2015).

affair"), which was much used in folk and historical traditions. The *Decision of the NPC Standing Committee on Cases Not to be Tried Publicly*, issued in response to an inquiry of the Supreme People's Court concerning the question of which cases could be tried in a nonpublic manner, specified that a people's court shall not try a case publicly when it involves state secrets, the private affairs (*Yin Si*) of parties concerned or persons under 18 years of age. This Decision set out a fundamental principle for nonpublic trial, the content and provisions of which were later adopted in a procedural law.[70]

The Supreme People's Court also attempted to define the scope of *Yin Si*-related cases and *Yin Si* indirectly.[71] Relevant provisions of this period had two characteristics: (i) the general adoption of the concept of *Yin Si* reflected the powerful impact of cultural tradition, and (ii) the law's main intention was to protect the procedural right of parties to nonpublic trials.

In the wake of China's political and economic opening and following law reforms in the 1980s and early 1990s, the concept of 'privacy' replaced *Yin Si* and became widely used by legislative, executive and judicial authorities.[72] By the end of January 2015, the concept of privacy had been used in 26 national laws[73] and 16 administrative regulations.[74] During this period, the shift of the legal concepts towards privacy led to the following changes:

---

[70] In the late 1970s, Article 111 of the *Criminal Procedure Law* and Article 7 of the *Law on the Organization of the People's Courts* (1979) continued to use this concept.

[71] Pursuant to the *Preliminary Opinions of the Supreme People's Court on Public Trial in accordance with Law*, "cases related to *Yin Si* usually refer to those connected with sexual intercourse or insulting women".

[72] The *Civil Procedure Law* of 1982 adopted the concept of privacy for the first time; in 1989, the *Regulations on the Organization of the People's Mediation Committees* became the first administrative regulation adopting the concept of privacy; in 1996, the revised *Criminal Procedure Law* replaced *Yin Si* with "privacy".

[73] Respectively, they include: the Espionage Act (2014), the Administrative Procedural Law (revised in 2014), the Law on the Prevention and Treatment of Infectious Diseases (revised in 2013), the Decision of the Standing Committee of the National People's Congress concerning Strengthening Network Information Protection (2012), the Law on Penalties for the Violation of Public Security Administration (revised in 2012), the Law on the Protection of Minors (revised in 2012), the Mental Health Law (2012), the Law on Lawyers (revised in 2012), the Civil Procedure Law (revised in 2012), the Criminal Procedure Law (revised in 2012), the Law on Civil Mediation (2010), the Law on the Laws Applicable to Foreign-Related Civil Relations (2010), the Tort Liability Law (2009), the Law on Administrative Penalties (revised in 2009), the Law on Administrative Review (revised in 2009), the Law on Mediation and Arbitration of Disputes over Contracted Rural Lands (2009), the Law on Mediation and Arbitration of Labor Disputes (2007), the Anti-Money Laundering Law (2006), the Law on the Organization of the People's Courts (revised in 2006), the Law on Banking Regulation and Supervision (revised in 2006), the Notarization Law (2005), the Administrative Licensing Law (2003), the Insurance Law (revised in 2002), the Law on Medical Practitioners (2002), the Law on the Protection of the Rights and Interests of Women (2002), and the Basic Law of the Macao Special Administrative Region (1993).

[74] Respectively, they include: the *Interim Regulations on Enterprise Information Publicity* (2014), the *Administrative Regulations on the Credit Reporting Industry* (2013), the *Regulations on the Compulsory Insurance for Liability for Traffic Accidents of Motor Vehicles* (revised in 2012), *the Implementing Rules of the Law on the*

1) The focus of protection has moved from procedural rights to substantive civil rights (e.g. the *Law on the Protection of Minors*, the *Law on the Protection of the Rights and Interests of Women* and similar laws establish the right to privacy as a substantive right; in a similar vein, *judicial interpretations* of the Supreme People's Court also recognize the right to privacy as a civil right);[75] 2) the approach developed from a simple procedural protection through nonpublic trial to a combination of procedural and civil remedies; and 3) with regard to procedural rights, as previous judicial interpretations are still effective, and the Supreme People's Court has not redefined the scope of "privacy-related cases" yet, the concept – despite its change - stills reflects that of *Yin Si*.[76] However, with regard to the substantive right, laws and regulations adopting the concept of privacy for years have failed to provide a clear definition and description of the scope of such a right, with the consequence that the boundaries of the substantive right to privacy have remained obscure both in legislative theory and in judicial practice. The clarity of its procedural aspects and the obscurity that surrounds its substantive aspects have led to confusion, and legislative bodies have failed to distinguish and use those concepts correctly.[77] For these reasons, in practice, the right to privacy frequently does not offer parties effective protection.

Administration of Tax Levying (revised in 2012), the *Regulation on the Administration of Security and Guarding Service*s (2009), the *Provisions for the Planned Parenthood of Floating Population* (2009), the *Regulations on Nurses* (2008), the *Regulations on the Punishment of Civil Servants of Administrative Organs* (2007), the *Regulations on Open Government Information* (2007), the *Regulation on the Work of Local Chronicles* (2006), the *Regulations on Implementing Customs Administrative Penalties* (2004), the *Regulations on the Management of the Medical Practice of Rural Doctors* (2003), the *Administrative Regulations on the China-based Representative Offices of Foreign Law Firms* (2001), the *Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the People's Republic of China* (1998), the *Regulations on the Settlement of Labor Disputes in Enterprises* (1993), and the *Regulations on the Organization of the People's Mediation Committees* (1989).

[75] Though the *General Principles of the Civil Law* promulgated in 1986 do not provide for the right to privacy, the Supreme People's Court, through several judicial interpretations, particularly the *Answers of the Supreme People's Court on Several Issues Relevant to the Trial of Cases Involving Rights to Reputation* (1993) and the *Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (Trial Implementation)* (1988), actually interprets the right to privacy as one of rights to reputation, granting it the status of a civil right and protecting it accordingly.

[76] For example, the *Several Provisions of the Supreme People's Court on the Strict Implementation of Public Trial System* (1999) clearly states: "a case may be tried in a nonpublic manner if it involves personal privacy, crime committed by persons above 14 but less than 16 years of age, or divorce as approved by the people's court upon application by any party concerned". Here, cases related to personal privacy are lumped together with cases involving other circumstances; therefore, we can conclude that the scope of privacy-related cases is rather narrow, perhaps not including divorce cases.

[77] For example, Article 42 of the *Law on the Protection of the Rights and Interests of Women* provides for the right to privacy and right to reputation, as does the *Tort Liability Law*, while the *General Principles of the Civil Law* provide for the right to reputation and do not mention the right to privacy. Therefore, right to privacy under the *Law on the Protection of the Rights and Interests of Women* and

Towards the end of 1990s, and especially at the beginning of the 21st century, due to the rapid process of informationization and greater awareness of personal rights, the concept of 'personal information' began to appear in local decrees related to informationization[78] and consumer rights protection;[79] it then gradually expanded to national laws.[80] By the end of January 2015, this concept had appeared in nine national laws,[81] five administrative regulations,[82] 12 judicial provisions,[83] and four special rules for personal information protection.[84] Today, the

the *Tort Liability Law* is obscure in meaning, scope, and as regards its difference from the right to reputation, and requires further definition.

[78] Local legislations in respect of ID-card management, credit-reference system building, Internet use and administration and government office automation all have provisions for personal information protection.

[79] Interestingly, the *Consumer Protection Law* of 1993 does not contain any provisions in respect to privacy or personal information, but, since the 21st century, some local decrees on consumer protection (such as Shanghai, Yunnan, Inner Mongolia, Liaoning, Anhui, Fujian, Hunan and Guizhou) have generally added provisions on consumer personal information protection.

[80] At national level, the *Law on Resident Identity Cards* (2003) and the *Passport Law* (2006) are the first to adopt the concept of personal information.

[81] These nine national laws are: the *Passport Law* (2006), *Amendment VII to the Criminal Law* (2006), the *Statistics Law* (revised in 2009), the *Social Insurance Law* (2010), the *Law on Resident Identity Cards* (revised in 2011), the *Criminal Law* (revised in 2012), the *Law on the Administration of Exit and Entry* (2012), the *Tourism Law* (2013), and the *Consumer Protection Law* (revised in 2013).

[82] Specifically, they include the Regulations on Administration of Lotteries (2009), the Regulation on Drug Rehabilitation (2011), the Regulation on the Administration of Recall of Defective Auto Products (2012), the Administrative Regulations on the Credit Reporting Industry (2013), and the Tentative Measures for Social Assistance (2014).

[83] Specifically: *Supplementary Provisions of the Supreme People's Court and the Supreme People's Procuratorate on Implementing the Accusations As Defined in the Criminal Law of the People's Republic of China (IV)* (2009), *Provisions of the Supreme People's Court on Issues Concerning Law Application in Hearing Cases of Tourism-related Dispute* (2010), *Rules on Criminal Procedures of the People's Procuratorate (for Trial Implementation)* (revised in 2012), *Interpretations of the Supreme People's Court on the Application of the Criminal Procedure Law of the People's Republic of China* (2012), *Provisions of the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security, the Ministry of Justice and the Legislative Affairs Commission of the Standing Committee of the National People's Congress on Several Issues Concerning the Implementation of the Criminal Procedure Law* (2012), *Several Opinions of the Supreme People's Court on Promoting the Construction of Three Major Platforms for Judicial Publicity* (2013), *Provisions of the Supreme People's Court on the Online Issuance of Judgment Documents by People's Courts* (2013), *Opinions of the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security and the Ministry of State Security on Legally Handling Cases of Unlawful Producing, Selling and Using 'Pseudo Base Station' Equipment* (2014), *Work Rules for the Publication of Case Information by People's Procuratorate (for Trial Implementation)* (2014), *Provisions of the Supreme People's Court on Several Issues concerning the Application of Law to the Trial of Civil Dispute Cases of Infringement of Personal Rights via Information Networks* (2014), *Provisions on Information Reporting to the People's Procuratorate* (2014), and *Measures of the Supreme People's Procuratorate for Receiving Visitors via Remote Video (for Trial Implementation)* (2014).

[84] They are: *Information security technology - Guideline for personal information protection within information system for public and commercial services* (2012), *Notice of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Legally Punishing Criminal Activities Infringing upon the Personal Information of Citizens* (2013), *Provisions on the Protection of Personal Information of Telecommunication and*

notion of 'personal information', apart from constituting a new concept, has brought about several changes: 1) compared to 'privacy', the boundaries of which seem obscure and which relies mainly on the protection of civil infringement provisions, the concept of 'personal information' is more neutral and goes beyond the scope of conventional civil rights infringement provisions. For example, the improper collection, usage, disclosure, exchange or dissemination of a user's name, address, phone number, occupation, education or other objective personal data can be difficult to qualify as an infringement and imply liability from the perspective of tort law; hence, it will be much easier if the concept of personal information is used. With its wider scope and clearer boundaries, the concept of personal information can expand the boundaries of rights.[85] 2) Personal information protection goes beyond the scope of traditional privacy protection; therefore, in addition to two conventional means, it is also subject to government supervision and administrative protection, and represents a big step forward from *ex post* protection to a multiphase and integral protection. 3) In recent years, judicial interpretations have frequently referred to the concept of personal information, indicating the reality and urgency of personal information protection in practice, as well as the fact that laws and administrative regulations lag behind judicial practice. However, personal information protection in China continues to be dispersed, unsystematic and in need of improvement. For this reason, provisions that deal with consumer personal information protection without ever using the concept of privacy or personal information will also be analyzed in this study.

2. General legal framework for consumer data protection

According to Article 38 of the Constitution, "[t]he personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false accusation or false incrimination directEed against citizens by any means is prohibited". This provision is a direct source of the right to personal information, though it does not refer explicitly to 'privacy protection'; however, through the protection of the

Internet Users (2013), and *Provisions on the Management of Personal Information Security for Postal and Delivery Service Users* (2014).

[85] Pursuant to Article 12 of the *Provisions of the Supreme People's Court on Several Issues concerning the Application of Law to the Trial of Civil Dispute Cases of Infringement of Personal Rights via Information Networks*, network users or network service providers cause damage to others by using the network to disclose any natural person's gene information, medical record, health examination information, criminal record, home address, private activities and other privacies and personal information; the person thus harmed can demand that they be held responsible for such infringements, and the people's court shall uphold such demands. This provision is the first time that an official document distinguishes between privacy and personal information; the latter is limited in scope and equivalent to personal information that falls under tort law and the disclosure of which may have negative effects, while the latter is rather extensive and represents personal information in a neutral sense.

foregoing rights, it protects citizens' privacy indirectly. Similarly, Article 39[86] and Article 40[87] of the Constitution can also be understood as the constitutional basis of the right to personal information.

Moreover, the amended Articles 41, 47, 51 and 24 of the Constitution also offer an indirect protection of personal information, which is also enshrined in Articles 101[88] and 102[89] of the *General Principles of the Civil Law* of 1986, Article 140 of the *Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China*[90] and the *Answers of the Supreme People's Court on Several Issues Relevant to the Trial of Cases Involving Rights to Reputation*, adopted at the 1002th Session of the Judicial Committee of the Supreme People's Court. The *Answers* address some of the typical issues encountered by courts across the country, such as the subject of the infringement of the right to reputation, and the amount and scope of compensation arising from the infringement of the right to reputation.

The *Tort Liability Law* of 2009 established the legal status of the right to privacy for the first time, determining that civil rights and interests refer to personal and property rights, including, *inter alia*, the right to life, right to health, right of name, right of reputation, right of honor, right of portrait, right to privacy, right of self-determination in marriage, guardianship, ownership, usufruct, security interest in property, copyright, patent, right to the exclusive use of trademarks, right of discovery, equity interest and right of inheritance. In addition, the Law requires that "medical institutions and their medical personnel shall ensure the privacy and confidentiality of their patients, and they shall bear tort liability if divulging their patients' privacy or medical records without the patients' consent, causing damage to the patients".

Regarding the protection of vulnerable groups, such as women and children, the *Law on the Protection of the Rights and Interests of Women* (promulgated in 1992 and revised in 2005) stipulates that "Women's rights of personality, including their

---

[86] Article 39: "The residences of citizens of the People's Republic of China are inviolable. Unlawful search of, or intrusion into, a citizen's residence is prohibited."

[87] Article 40: "Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon citizens freedom and privacy of correspondence, except in cases where, to meet the needs of state security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law."

[88] Article 101: "Citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited."

[89] Article 102: "Citizens and legal persons shall enjoy the right of honor. It shall be prohibited to unlawfully divest citizens and legal persons of their honorary titles."

[90] Article 140: "Where anyone breaches the privacy of any other person in writing or orally, fabricates facts to vilify the personality of another person overtly, or damages another person's reputation by insult or slander, which result in certain effects, such an act shall be determined as infringing the citizen's right of reputation."

right of reputation, right of honor, right of privacy and right of portrait, shall be protected by law" and "[b]esmirching women's personal dignity by such means as humiliation and libel is prohibited", while the *Law on the Protection of Minors* requires that society as a whole shall respect the personal dignity of minors and not act in a manner insulting to their personal dignity.

Furthermore, the right to personal information is protected through sectoral laws, such as the *Postal Law*[91] with its *Implementing Rules of the Postal Law*,[92] or the *Law of the People's Republic of China on Resident Identity Cards* (revised in 2011), which strengthens personal information protection, requiring state organs or financial, telecommunications, transportation, education, medical and other units and their staff to keep confidential the personal information as indicated in resident identity cards that they have acquired in the course of performing duties or providing services.

In 2012, the Standing Committee of the National People's Congress issued the *Decision on Strengthening Information Protection on Networks*, requiring the State to protect electronic information able to identify citizens' identity and involving citizens' personal privacy. This *Decision* for the first time defines the meaning and scope of personal information and in a legal sense. The *Decision* also represents the first attempt to set out the substantive scope of personal information protection in a systematic manner.

In 2012, China's Standardization Administration and the General Administration of Quality Supervision, Inspection, and Quarantine (AQSIQ) issued the *In-*

[91] Article 4 of the *Postal Law*: "The freedom and privacy of citizens' correspondence are protected by law. No organization or individual may infringe the freedom and privacy of any citizen's correspondence for any reason, unless the public security organs, national security organs or procuratorial organs examine correspondence in accordance with the procedures specified in relevant laws for the purpose of national security or criminal investigation."
Article 6 of the *Postal Law*: "Postal enterprises and postal staff shall not provide information to any organization or individual about users' dealings with postal services except as otherwise provided for by law."

[92] The *Implementing Rules of the Postal Law* further provide: "In the event that a public security organ, a state security organ, or a procuratorial organ inspects or detains postal materials or freezes remittances or savings deposits out of necessity for state security or the investigation of a criminal offence, it is imperative for the aforesaid organs to issue according to law notifications of the relevant inspection, detention, or freezing to the postal enterprise or the administrative bureau of post and telecommunications concerned at or above the county level, and to create a list of the specific items of postal materials, remittances, or savings deposits; after going through the procedures for inspection, detention or freezing, the postal enterprise shall appoint specially designated persons to be responsible for sorting out the items in question, register them one by one, and then go through the handover procedures; with respect to those postal materials, remittances or savings deposits which need no further inspection, detention or freezing, or which have been proved through investigation to have nothing to do with the case concerned, they shall be returned to the postal enterprise without delay. In the case that in the course of inspection, detention or freezing the postal materials, remittances or savings deposits are lost or damaged, the relevant public security, state security, or procuratorial organ shall be responsible for compensation."

formation Security Technology – Guidelines for Personal Information Protection within Public and Commercial Services Information Systems. The *Guidelines* offer technical guidance and contain the most detailed provisions so far on the standardization of personal information processing by information systems. They cover personal information processed partly or entirely through an information system, offer guidance on personal information protection in different stages of processing, and can be used to direct relevant personal information protection by various organizations other than government departments performing public administration, such as service providers in telecommunications, financial or healthcare areas.

In 2013, the revised Law on the Protection of Consumer Rights and Interests (*Consumer Protection Law)*, instead of constituting the conventional framework of the rights to name, portrait and privacy, included the protection of personal information as a separate fundamental right of consumers and highlighted the provisions for the protection of consumers' personal information. In 2014, the *Provisions of the Supreme People's Court on Several Issues concerning the Application of Law to the Trial of Civil Dispute Cases of Infringement of Personal Rights via Information Networks* defined the boundaries between privacy and personal information, indicating that privacy has a narrower and personal information a broader scope. Finally, in 2015, the *Measures for Punishments against Infringements on Consumer Rights and Interests* defined the boundaries of personal information.

However, despite significant progress in recent years, personal information protection legislation in China is still quite dispersed and obscure in meaning and scope. In particular, a uniform law on personal information protection is lacking, making it difficult in many areas to compare the national legislation with other countries.

3. Telecommunication

In the mid-1990s, the Internet gradually spread across China. In 1998, the State Council Information Commission promulgated the *Interim Administrative Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the People's Republic of China.*[93]

In 1999, the China Information Security Testing and Certification Center was founded to protect state secrets and business secrets on the Internet, to define rights and responsibilities to ensure individual and government network usage, and to protect information by monitoring unauthorized access.

[93] Article 18 specified that "subscribers shall subject themselves to the administration of access units and observe subscription regulations. They are forbidden from entering certain computer systems without permission and illegally changing others' information, distributing malicious information, giving out information in other people's names and violating others' privacy through networks, developing and spreading computer viruses and engaging in other activities in violation of legitimate rights and interests of networks and individuals".

In 2000, the NPC Standing Committee adopted the *Decision on Internet Security Protection*, which contains specific provisions on the infringement of personal privacy through computer networks, and the State Council promulgated the *Administrative Measures for Internet Information Services*, requiring that anyone engaged in the provision of Internet information services shall have in place sound procedures to ensure network and information security, including procedures to ensure website security, a system to manage the security and confidentiality of information, and a system to manage the security of the subscriber's information. In the same year, China issued the *Telecommunications Regulations of the People's Republic* in order to regulate the structure of the telecommunications market, safeguard the legitimate rights and interests of telecommunications subscribers and telecommunications operators, ensure the safety of telecommunications networks and information, and promote the sound development of the telecommunications industry.

In 2006, the Ministry of Industry and Information Technology (MIIT) promulgated the *Measures for the Administration of Internet E-mail Services* with regard to personal information protection in Internet e-mail services. In light of unfair competition among Internet enterprises that often involved users' personal information, in 2011 the MIIT promulgated the *Several Provisions on Regulating the Market Order of Internet Information Services* to provide for comprehensive user information protection for the first time. Finally, the *Provisions on the Protection of Personal Information of Telecommunication and Internet Users*, promulgated by the MIIT in 2012, are among few specific regulations on personal information protection, and refer to activities of collecting and using users' personal information in the course of providing telecommunication services and Internet information services in the People's Republic of China.

4. Banks

When a person applies for a bank account, a credit card or a mortgage loan at a bank, he or she usually has to provide some personal information (e.g. ID number, home address, private phone number, and, if necessary, the assets of the bank account). Leaking such information will cause significant trouble to clients.

As a result, the *Law on Commercial Banks* requires commercial banks to safeguard the lawful rights and interests of depositors against infringements[94] and to adhere to the principles of voluntary deposit, unimpeded withdrawal, payment of interests on deposits and confidentiality for the depositors. Banks cannot refuse to answer inquiries or freeze, deduct or transfer an individual's saving deposits, unless otherwise provided for by law.[95] Several provisions establish detailed rules regarding the confidentiality of financial information.[96]

[94] Article 6 of the Law on Commercial Banks.

[95] Article 29 of the Law on Commercial Banks.

[96] See, for instance, Article 15 of the *Law of the People's Bank of China*: "The Governor, Deputy Governor and other staff members of the People's Bank of China shall safeguard State Secrets ac-

Pursuant to the *Law on Banking Regulation and Supervision* (2003), the staff of the banking regulatory authority shall not reveal the information deemed confidential by the government, or by the banking institutions under the supervision of the banking regulatory authority, or by other parties concerned. The banking regulatory authority under the State Council shall make relevant arrangements for preserving the confidentiality of information in the process of exchanging supervisory information with the banking supervisory authorities in other countries and/or regions.[97]

With regard to personal information protection in connection with electronic payment, in 2005, the PBOC published the Electronic Payment Guidelines (No.1), imposing a duty of notification[98] and restrictions on banks' use of customer information.[99]

In 2013, the China Banking Regulatory Commission (CBRC) issued the *Guidelines on Banking Consumer's Rights Protection*. Pursuant to its Article 12, financial institutions in the banking sector shall respect banking consumers' right to personal financial information security, take effective measures to strengthen the protection of personal financial information, not temper or illegally use banking consumers' financial information, and not provide personal financial information to any third party without the authorization or consent of banking consumers. Article 19 requires financial institutions in the banking sector to establish and improve a mechanism to coordinate and control banking consumer protection. They shall implement internal rules and regulatory requirements for banking consumer pro-

cording to law and be obligated to safeguard the secrets of the banking institutions and parties concerned with their implementation of their functions and responsibilities."

Article 23, Paragraph 2 of the *Administrative Measures for Bank Credit Registration and Inquiry*: "The People's Bank of China shall not disclose relevant information of financial institutions and borrowers willfully."

Pursuant to the *Rules on the Real Name System of Personal Deposit Accounts*, unless otherwise specified by law, financial institutions shall not provide personal deposit account information to any unit or individual, and shall have the right to refuse any unit or individual's demands to inquire about, freeze or transfer an individual's deposit. In addition, some banks also provide for client privacy protection in their internal rules; for instance, *the Rules of Conduct for ICBC Employees* require employees to keep confidential clients' secrets and materials to safeguard clients' lawful rights and interests, and not make any unauthorized disclosure of clients' information unless permitted by law or with the consent of clients.

[97] See Article 11 of the Law on Banking Regulation and Supervision.

[98] Article 11: "When a bank requires a customer to provide the relevant materials and information, it shall inform the customer of the purpose and scope of using the provided information, security protection measures, as well as the consequences if the customer fails to provide or faithfully provides the relevant materials."

[99] Article 27: "A bank shall not exceed the scope permitted by laws and regulations and authorized by customers in terms of using customer data and transaction records, and so on. It shall keep secret customers' data and information as well as transaction records according to law. Unless otherwise specified in national laws and administrative rules, it shall refuse the inquiry of any unit or individual person other than customers."

tection throughout the process of product or service design, development, pricing, agreement formulation, approval, marketing and after-sales management. Finally, they shall ensure that measures for banking consumer protection shall be implemented before a product or service enters the market.

To build a creditworthy society and curb dishonesty, China's government has been dedicated to building a functioning credit system., A very important issue concerning personal information protection arose in this process. The *Administrative Regulations on the Credit-Reporting Industry* of 2012, applicable to credit-reporting agencies, contain some provisions that have become a model for administrative regulations on personal information protection.

5. Media-related acts

Legislation with respect to radio, television and other conventional media includes the *Regulations on Radio and Television Administration* (1997), the *Administrative Regulations on Publication* (2001), the *Regulations on the Administration of Movies* (2001) and the *Regulations on News Coverage by Resident Offices of Foreign News Agencies and Foreign Correspondents* (2008). These provisions provide for privacy protection in a traditional sense.[100] In addition, the *Rules of Conduct for Chinese Journalists* (1994) require journalists to "safeguard citizens' rights under the Constitution, not expose others' privacy, not libel others, obtain news through lawful and proper means, and respect respondents' statements and appropriate requests." In 2005, the State Administration of Radio, Film and Television issued the *Implementing Rules for the Management of Radio, Film and Television News Reporters and Editors* to protect privacy.[101] Article 16 of the *Administrative Regulations on Internet Audiovisual Program*

[100] See for example the *Regulations on the Administration of Publications*, Article 26 (8): "No publication shall contain the following contents: […] those insulting or libeling others, violating the lawful rights and interests of others."
Article 28: "Where the lawful rights or interests of a citizen, a legal person or other organization are infringed upon due to the untruthfulness or unfairness of the contents of a publication, its publishing unit shall make public corrections, eliminate the negative effects, and bear civil liabilities.
Where the lawful rights or interests of a citizen, a legal person or some other organizations are infringed upon due to the untruthfulness or unfairness of the contents of the works published in a newspaper or a periodical, the party concerned shall have the right to require corrections or to make a reply, and the relevant publishing unit shall publish the corrections or reply in the latest issue of its newspaper or periodical; in case of a refusal to publish, the party concerned may bring a lawsuit in a people's court."

[101] For example, requiring them to respect citizens' personal dignity; safeguard citizens' rights of name, portrait, reputation, honor and privacy; not to publicize others' private information or fabricate facts to vilify others; not insult, libel or use other means to damage others' reputation; acquire news through legitimate and rational means, and respect respondents' statements and proper requests; take into account the feelings of victims and their relatives when covering an accident, and refrain from causing psychological harm when interviewing and making audiovisual records, and use a variety of means to publicize the protection of citizens' lawful rights and interests.

Services (2007) stipulates that Internet audiovisual program providers and network operators shall provide audiovisual programs in accordance with laws, administrative regulations and rules, and maintain a program already provided in entirety for 60 days. The contents of audiovisual programs shall not insult or libel others or infringe upon citizens' privacy and other lawful rights and interests. In the age of the Internet, 'personal media' are playing an important role and personal information protection is receiving growing attention from the legislation. The Decision of the *Standing Committee of the National People's Congress concerning Strengthening Network Information Protection* requires network service providers to sign an agreement or confirm the provision of services with users and ask users to provide truthful identity information when handling network, telephone or cell phone access or providing information release service for users. In 2014, the State Council issued the *Notice concerning Empowering the Cyberspace Administration of China to Be Responsible for Internet Information Content Management Work*, authorizing the re-established Cyberspace Administration of China to take responsibility for Internet information content management work nationwide as well as for supervision, management and law enforcement. Pursuant to Article 5 of the *Interim Provisions on the Administration of the Development of Instant Messaging Services*, issued in 2014, instant message service providers shall be responsible for security management. They shall establish and improve various systems, allocate specialized personnel appropriate to their service model, and protect user information and citizens' privacy. They shall also voluntarily accept public oversight and handle violations and unwholesome information reported by the public in a timely manner. The *Administrative Provisions on the Account Names of Internet Users* 2015 requires Internet information providers to protect users' information and citizens' personal privacy.

6. Specific acts for e-commerce

Without a general law on e-commerce, China's legislation is somewhat dispersed. The *Guideline for Personal Information Protection* requires network service providers and other institutions to keep confidential the electronic personal information of citizens gathered in business activities. They may not divulge, alter, damage, sell, or illegally provide others with the information. The *Administrative Measures for Online Trading,* promulgated by the State Administration for Industry and Commerce (SAIC) in 2014, offer systematic provisions on e-commerce, requiring those who engage in online commodity trading to complete business registration procedures in accordance with the law. Participants in online commodity trading shall conduct their business operations through third-party trading platforms and give their name, address, identity, and contact details. The third-party online platform operators shall be legal persons that have registered at and obtained the license of business from the industrial and commercial departments. The third-party online platform operators shall verify and register the business operator status of the legal and natural persons applying to join their platforms to sell goods or services,

set up registration records and verify and update these on a regular basis. When collecting and using consumer or operator information in the course of business operation, online commodity operators and relevant service providers shall follow the principles of legality, rationality and necessity, clearly state the purpose, manner and scope of data collection and use, and obtain the consent of those from whom information is gathered. Without the consent or request of consumers or in the case of consumers' explicit refusal, online commodity operators and relevant service providers shall not send commercial electronic information to consumers. They shall publish their rules concerning data collection and use, and not collect and use information in violation of laws, regulations and mutual agreements. Online commodity operators and service providers shall keep personal information confidential and not disclose, sell or illegally provide to others consumers' personal information or operators' business secrets that they have collected. They shall take technical and other necessary measures to ensure information security and prevent information leakage or loss, and promptly take corrective measures when information leakage or loss occurs or is likely to occur.

Pursuant to Article 10 of the *Guidelines for Standardizing the Standard Terms of Contracts for Online Trading Platforms* promulgated by the SAIC in 2014, online trading platform operators shall not exempt or lessen in their standard contract terms their liability for the security of consumers' personal information and business operators' business secrets that they have gathered. Moreover, the *E-commerce Model Specifications* (2009), the *Specifications for the Service of Online Trading* (2009) and the *Specifications for the Service of Third-party Online Trading Platforms* (2011), promulgated by the Ministry of Commerce (MOFCOM), provide for the protection of users' right to privacy.

III. Applicability of data protection acts

Neither the Decision of the *Standing Committee of the National People's Congress on Internet Security Protection* nor the *Consumer Protection Law* specify the territorial scope of application. The *Provisions on Protection of Personal Information of Telecommunication and Internet Users* promulgated by the MIIT governs the collection and use of users' personal information in the course of providing telecommunications services and Internet information services within the territory of the People's Republic of China. In general, when the person performing the act is located within the territory of China or the act of personal information processing occurs within the territory of China, Chinese law applies. The draft of the *Anti-Terrorism Law* under discussion reiterates this rule, requiring that "those providing telecommunications and Internet services within the territory of China shall keep relevant facilities and domestic user data within China."[102]

[102] Article 15, Paragraph 3 of the *Anti-Terrorism Law*.

IV. Definition of consumer and data

Article 2 of the *Consumer Protection Law* protects the rights and interests of consumers when purchasing or using commodities or receiving services for daily consumption. This refers to the consumption of tangible or intangible products for individual or family life, including basic goods such as clothes, food, shelter and transportation, development-based consumption such as vocational training, as well as entertainment consumption such as culture and travel. The *Consumer Protection Law* also covers the consumption of financial goods and products.[103] In addition, the *Law on Commercial Banks*, the *Law on Banking Regulation and Supervision* and other relevant laws can regulate specific issues in this area. The *Consumer Protection Law* does not specify whether it is applicable to healthcare and education services. This will depend on the circumstances of the case, for example whether the services are intended for "daily consumption". Generally, a consumer is a natural person. However, there is some dispute regarding the possibility of considering legal persons as consumers, as no clear provision exists. Consumer is a concept relative to the seller and producer. As long as the commodities or services are purchased, used or received by persons in market transactions for the needs of individual and family life rather than those of production and operation activities or occupational activities, such persons shall be considered as consumers of "commodities or services for daily consumption", and are subject to the protection of the adjusted *Consumer Protection Law*.

Pursuant to Article 4 of the *Provisions on the Protection of Personal Information of Telecommunication and Internet Users,* personal information refers to the user's name, date of birth, ID number, address, phone number, account name and password, which are collected by telecommunications operators and Internet information providers in the course of providing services that, alone or together with other information, can be used to identify a user's information, time and location of service usage, and so on. This represents the first attempt to define personal information.

Unlike the European Union, China does not have a clear definition of what constitutes sensitive information. However, pursuant to Article 14 of the *Administrative Regulations on the Credit-Reporting Industry,* credit-reporting agencies are prohibited from gathering information on an individual's religious beliefs, genes, fingerprints, blood type, disease and medical history, and any other information prohibited from collection by laws and regulations. Credit-reporting agencies shall not gather information regarding the income, savings, negotiable securities, commercial insurances, real estates and tax payments of an individual, unless the credit-

[103] This conclusion can be derived from Article 27, which requires providers of securities, insurance, banking and other financial services to inform consumers about the place of business, contact details, quantity and quality of goods or services, prices or charges, time limits and ways of performance, security and risk alerts, after-sales services, civil liability, and so on.

reporting agencies have explicitly informed the data subject of the possible adverse consequence of providing such information and have obtained the data subject's written consent. The *Guideline for Personal Information Protection* divides personal information into sensitive personal information and general personal information. Sensitive personal information refers to any information that will result in a negative impact on the data subject if divulged or revised. The contents of sensitive personal information depend on the subject's willingness and business-specific features. For instance, sensitive personal information may include ID number, phone number, ethnic identity, political views, religious beliefs, genes, fingerprints, and so on. General personal information refers to any personal information other than sensitive personal information. Clearly, such a scope of sensitive personal information is much broader than the sensitive information defined in EU legislation and has different meanings.

Pursuant to Article 12 of the *Provisions of the Supreme People's Court on Several Issues concerning the Application of Law to the Trial of Civil Dispute Cases of Infringement of Personal Rights via Information Networks* (2014), network users or network service providers cause damage to others by using the network to disclose any natural person's genetic information, medical record, health examination information, criminal record, home address, private activities and other private and personal information. Finally, the *Measures for Punishments against Infringements on Consumer Rights and Interests* (2015) stipulate in Article 11 that consumers' personal information refers to a consumer's name, gender, occupation, date of birth, ID number, address, contact information, income and property, health, consumption and other information collected by business operators in the course of providing goods or services and that, alone or together with other information, may be used to identify a consumer.

V. General guiding principles

The *Decision of the Standing Committee of the National People's Congress concerning Strengthening Network Information*, which has become a model for later legislation, is the first instrument establishing general guidance for network service providers and other enterprises and institutions on using citizens' electronic personal and privacy information. They shall, when gathering and using electronic personal information of citizens in business activities, adhere to the principles of legality, rationality and necessity, explicitly state the purpose, manner and scope of collecting and using information, and obtain the consent of those from whom information is collected. They shall not collect or use information in violation of laws and regulations or contrary to the agreement between both sides. They shall, when gathering and using the electronic personal information of citizens, publish their rules of collection and use, keep personal information strictly confidential and not divulge, alter, damage, sell, or illegally provide others with the electronic personal information of citizens gathered in business activities. They shall take technical and other neces-

sary measures to ensure information security and prevent the electronic personal information of citizens gathered during their business activities from being leaked, damaged or lost. If this happens, remedial actions shall be taken immediately. They shall strengthen the management of information published by their users, immediately stop transmission of information prohibited by laws or regulations, take measures to eliminate the effects, keep the relevant records, and report to competent authorities.

In a similar way, Article 29, Paragraph 1 of the *Consumer Protection Law* defines basic principles for the protection of consumer personal information. When gathering and using the personal information of consumers, business operators shall follow the principles of legality, rationality and necessity, explicitly state the purpose, manner and scope of information collection and usage, obtain the consent of consumers, and not violate laws, regulations or the mutual agreement. Legality, rationality and necessity mean that personal information is collected in a lawful and fair way, where business operators explicitly state their purposes in advance, and do not gather and use other information irrelevant to transactions. Moreover, 'voluntariness' is an important principle when business operators collect and use personal information, as they must provide prior information with respect to the purpose, manner and scope of data collection, obtaining the prior consent of the consumer. When collecting and using consumers' personal information, they shall not use standard terms and technical means with the aim of compelling consumers to give consent. Pursuant to Article 26 of the *Consumer Protection Law*, business operators shall not use standard terms, notifications, statements, in-store bulletins or any other means to impose transactions, exclude or restrict consumers' rights, lessen or remove business operators' liabilities, aggravate consumers' liabilities, or impose other unfair and irrational provisions on consumers. If standard terms, notifications, statements or in-store bulletins contain such content, they will be void. Business operators will be deemed as not having obtained the consent of consumers and shall bear legal liability if they have collected and used consumers' personal information through coercive means.

Finally, the *Guideline for Personal Information Protection* contains the most comprehensive provisions and specifies eight principles for personal information protection: a) *Explicit purpose*. The processing of personal information shall have a specific, explicit and rational purpose and shall not expand the scope of usage, nor change the purpose without notification of the data subject; b) *Minimal sufficiency*. Only the minimal amount of information relevant to the purposes in question shall be processed; once the purposes are achieved, said information shall be deleted as quickly as possible; c) *Public notification*. Business operators shall inform, provide explanation to and alert the data subjects, and use clear and appropriate means to truthfully inform the data subjects about the purposes of information processing, the scope of personal information collection and usage, measures for personal information protection, and so forth; d) *Personal consent*. Personal infor-

mation shall be processed only after the consent of the data subjects is obtained; e) *Quality assurance*. It shall be ensured that personal information is confidential, complete, usable and updated in the course of processing; f) *Security assurance*. Proper measures and technical means to prevent the possibility and the extent of any damages to personal information so as to ensure the security of personal information and prevent unauthorized searches, disclosure, loss, leaks, damage and tampering; g) *Good faith*. Processing of personal information will take place in good faith, and will stop once the stated purpose has been achieved; h) *Accountability*. Proper measures will be taken to ensure accountability in personal information processing, and record the process for later retracing.

VI. Collecting, storing and processing consumer data

Only the *Guideline for Personal Information Protection* contains specific definitions and legal requirements for the collection, processing, transfer and deletion of personal information. According to the *Guideline*, collection means obtaining and recording personal information. Processing refers to operations related to personal information, such as entering, storing, revising, marking, comparing, digging and masking personal information. Transfer means any act of providing personal information to others, such as publishing it, disclosing it to a targeted population, or entrusting others to process it by copying it to another information system. Deletion means rendering personal information unusable in the information system. There are several requirements for the collection,[104] the processing,[105] the transfer[106] and the deletion[107] of personal information.

---

[104] The requirements are the following: 1) There must be a specific, clear and lawful purpose; 2) prior to collection, accessible means to expressly notify and alert the data subjects must be used; subjects must be informed of: a) the purpose of personal information processing; b) the manner and means of information collection, the content to be collected, and the length of time the information collected will be retained; c) the scope of information use, including the scope of disclosure or provision to other organizations or institutions; d) measures for personal information protection; e) the name, address, contact details and other relevant information of the data administrator; f) the risks that may arise if the data subject provides personal information; g) the consequences that may arise if the data subject opts not to provide personal information; h) where the data subject can make a complaint; i) in order to transfer or entrust personal information to other organizations or institutions, the data subject shall be expressly informed, this information including but not being limited to: the purpose of such transfer and trust, the specific content and scope of use of the information to be transferred and entrusted, and the name, address and contact details of the recipient; 3) obtain the consent of the data subject prior to processing personal information, including implicit consent or express consent. When general personal information is collected, implicit consent may be deemed as having been given, and personal information will no longer be collected or be deleted if the data subject explicitly objects; when personal sensitive information is collected, express consent from the data subject is required; 4) collect the minimum amount of information that is adequate to achieve the stated purposes; 5) use the stated means and manner to collect information from the data subject directly, and not use hidden means or an indirect manner to collect information; 6) when data collection is an ongoing process, allow the data subject to set up, adjust or shut down the function

VII. Approaches to consent

Several legal instruments exist that regulate the requirement of the users' consent in cases of data collection and processing. According to the *NPC Decision* and *MIIT Regulation*, consent is required for the collection and use of an individual's personal information, but there are no detailed requirements regarding the specific form and content of the consent, nor concerning whether consent can be implied or inferred.[108]

Pursuant to the *Decision of the Standing Committee of the National People's Congress concerning Strengthening Network Information Protection,* no organization or individual shall send electronic commercial information to a consumer's home phone, mo-

of personal information collection; 7) not to directly collect personal sensitive information from persons under 16 years of age or others with no or limited capacity for civil conduct; if such collection is indeed necessary, express consent from their legal guardians must be obtained.

[105] The requirements are the following: 1) not do process personal information beyond the stated purpose or scope; 2) use the stated means and manners; 3) ensure that the personal information processed shall not be obtained by any individual, organization or institution irrelevant to the stated purpose; 4) not to disclose personal information processed to other individuals, organizations or institutions without express consent of the data subject; 5) ensure stable operation of the information system, and the integrity, accessibility and currency of personal information throughout the process; 6) when the data subject finds and requests correction of any error in his or her personal information, the data administrator shall check, verify, revise or supplement relevant information without prejudice to data integrity, 7) record details of personal information. Upon inquiry from the data subject, the information administrator shall notify the subject whether they possess his or her information, the content and status of such information and the like truthfully and free of charge, unless the cost or frequency of notification is beyond a reasonable scope.

[106] The requirements are the following: 1) Do not transfer personal information beyond the stated purpose or scope. 2) Prior to the transfer of personal information to other organizations and institutions, assess whether they can process personal information as required by this technical *Guideline*, and define their responsibility of personal information protection in the contract. 3) Ensure that personal information under transfer shall not be obtained by any individual, organization or institution other than the intended recipient. 4) Ensure the integrity, accessibility and currency of personal information before and after transfer. 5) Without the express consent of the data subject, or explicit provision or the approval of the competent authorities, the data administrator shall not transfer personal information to foreign recipients, including individuals outside China and organizations registered overseas.

[107] The requirements are the following: 1) Delete personal information in a timely manner upon reasonable request from the data subject. Take proper storage and masking measures if such deletion may affect the investigation of the enforcement authorities; 2) when the stated purposes are achieved, promptly delete personal information; if further processing is necessary, delete the content that can be used to identify a specific person; if personal sensitive information requires further processing, express consent from the data subject is required; 3) delete personal information promptly upon expiration of the stated time limit; implement relevant provisions if they prescribe such a time limit; 4) delete personal information when the data administrator is bankrupt or dissolved and unable to accomplish the stated purposes. Take proper storage and masking measures if such deletion may affect the investigation of the enforcement authorities.

[108] *Xiao Dong*, Data Protection in China: Overview, <http://uk.practicallaw.com/4-519-9017?q=*&qp=&qo=&qe=> (last accessed June 25, 2015).

bile phone or e-mail inbox without the consumer's consent or request or following a consumer's explicit refusal. The *Measures for Punishments against Infringements on Consumer Rights and Interests* contain a similar provision (Paragraph 3, Article 11). The *Guideline for Personal Information Protection* distinguishes between two forms of consent: the implicit consent of the data subject without any explicit objection, and the express consent when the data subject explicitly authorizes and agrees, with relevant evidence available. Even though these provisions distinguish between implicit and explicit consent and may have some legal significance, they remain overly general and fail to clarify the conditions, scope of application and relationship between these two forms of consent. Therefore these issues are in need of further clarification. However, other legislation also fails to make such distinctions. In practice there is thus still considerable ambiguity as to the requirements and conditions of consent. Finally, it should be mentioned that personal information can be processed by public security authorities without consent in accordance with procedures prescribed by law, to secure national security or an ongoing criminal investigation.[109]

The *Several Provisions on Regulating the Market Order of Internet Information Services* of 2011 establishes that, without the users' consent, Internet information service providers shall not gather users' personal information that is related to or may be used to establish the identity of users – alone or combined with other information –, and shall not provide the users' personal information to others, unless otherwise specified in laws and administrative regulations. When Internet information service providers collect personal information with the consent of users, they shall explicitly notify users of the manner, content and purpose of such information collection and use, not gather information unless necessary for service provision, and not employ of users' personal information for purposes other than provision of services.

The *Administrative Regulations on the Credit-Reporting Industry* of 2012, applicable to credit-reporting agencies, contain some provisions that have become a model for administrative regulations on personal information protection. According to the *Regulations*, information providers shall inform the data subject prior to providing negative personal information to credit-reporting agencies. Credit-reporting agencies can store negative consumer information for up to five years, starting from the date of termination of the misconduct, and then they must delete any of the negative information. The data subject may provide an explanation of the negative information prior to its removal and the credit-reporting agencies should keep a record of such explanations. The data subject can make inquiries to credit-reporting agencies concerning their own information. Each individual is entitled to receive their credit report free of charge twice per year. Any inquiry concerning consumer information directed towards the credit-reporting agencies must obtain

[109] *Xiao Dong*, Data Protection in China: Overview, <http://uk.practicallaw.com/4-519-9017?q=*&qp=&qo=&qe=> (last accessed June 25, 2015).

the written consent of the data subject and the purpose of data usage agreed upon by information user and data subject, unless otherwise stipulated by law. If a credit-reporting agency, data provider, or information user obtains the data subject's authorization or consent using a standard contract, the contract should contain sufficient indications to draw the data subject's attention and consent. The information user should use the consumer data only for the purpose that has been agreed by the data subject and not for any other purpose. The information user should not provide data to any third party without the data subject's consent.

VIII. Publicity and transparency

The *Decision of the Standing Committee of the National People's Congress concerning Strengthening Network Information Protection* and subsequent relevant legislation require "explicitly stating the purpose, manners and scope of information collection and usage". With regard to the notification of data leaks, the amended *Consumer Protection Law* adds a paragraph to Article 56, which specifies that business operators, when incurring in a violation of personal information protection, shall be included in the credit blacklist accessible to the public in addition to the imposition of penalties. Pursuant to Paragraph 2 of Article 56, the administrative departments for industry and commerce shall establish credit files on the basis of their respective duties, register violations of business operations in a timely fashion, and inform the public in accordance with this Law and other relevant regulations. Similarly, Article 108 of the *Tourism Law* stipulates that if tourism operators violate the provisions of this Law, the tourism authorities or other relevant institutions shall record such violations in their credit records and make them public. Paragraph 2 of Article 68 of the *Trademark Law* determines that when a trademark agency commits an act which is prohibited, the administrative authority for industry and commerce shall include it in the credit archives, and – in serious cases – the Trademark Office or the Trademark Review and Adjudication Board may in addition order the suspension of the trademark agency business and announce this publicly.

In 2011, the State Council required the involved regulatory authorities to establish food safety credit archives for all food producers and operators by the end of the year. It repeated its order the following year. Local housing, industrial and commercial authorities are required to record and make publically accessible any violations committed by real-estate agencies and their brokers. The same applies to land and resource authorities. Article 20 of the *Provisions on the Protection of Personal Information of Telecommunication and Internet Users* requires telecommunication authorities to record the violations of telecommunications operators and Internet information service providers. In case of the leaking, loss or tampering with personal information, the *Guideline for Personal Information Protection* requires information administrators to take suitable and timely measures to prevent any further deterioration of the situation and to notify the affected data subjects. So far, this is

the only normative document that requires the direct notification of the data subjects.

With regard to the confidentiality of personal information contained in administrative sanctions and judgments published on the Internet, several provisions require public authorities to delete sensitive personal information.[110]

IX. Data security

The *Decision of the Standing Committee of the National People's Congress concerning Strengthening Network Information Protection* and the *Consumer Protection Law* calls on data administrators to take all technical and necessary measures to ensure data security and avoid the leaking of, damage to, or loss of citizens' electronic information collected in the course of business activities. They shall promptly take corrective measures in case of actual or possible data leaks, damage or loss. Regarding security measures, the *Administrative Regulations on the Credit-Reporting Industry* stipulate that credit-reporting agencies should develop and implement data security policies and procedures and adopt effective technical measures to ensure data security in accordance with the provisions of the credit-reporting regulation authority under the State Council. Consumer credit-reporting agencies shall establish specific rules regarding the extent of staff authority and the inquiry procedure by which their staff access consumer data, keeping a record of each inquiry submitted by their staff, including staff name, time, content and purpose of the inquiry. Staff members should not access information in violation of the rules governing competences and procedures, or disclose any information they obtain. The *Provisions on the Protection of Personal Information of Telecommunication and Internet Users* set out com-

---

[110] For example, Article 6 of the Interim Provisions on the Publicity of Information concerning Administrative Penalties Imposed by Industrial and Commercial Administrative Departments (2014) stipulates that when publishing administrative penalties, the industrial and administrative departments shall delete the content involving business secrets and personal information, such as natural persons' residential addresses (unless identical with the place of business), contact details, ID numbers and bank account numbers. When considering it necessary to publish such information, they shall obtain the approval of the upper level of industrial and administrative department.

Pursuant to Article 6 of the *Provisions of the Supreme People's Court on the Online Issuance of Judgment Documents by People's Courts* issued in 2013, "when a people's court issues a judgment document online, it shall retain the name of parties concerned and other true information, but must use signs to replace the names of the following parties and litigation participants: (1) the parties and their legal agents in a marriage, family or inheritance dispute case; (2) the victims and their legal agents, witnesses and appraisers in a criminal case; (3) the defendants sentenced to fixed imprisonment of no more than three years or exemption of criminal punishment and not being a habitual criminal or recidivist". Article 7 further stipulates: "when a people's court issues a judgment document online, it shall delete the following information: (1) natural persons' home address, contact details, ID number, bank account number, health status and other personal information; (2) information related to minors; (3) legal persons and other organizations' bank account numbers; (4) business secrets; and (5) other content not appropriate for publication."

prehensive measures concerning data security.[111] In addition, telecommunications operators and Internet information service providers shall disseminate relevant knowledge, techniques and security responsibilities to their staff members, inspect the performance of user data protection at least once every year, record the results and remove any potential security issues they have identified in a timely manner.

X. Data control, data portability and the right to access, modify and delete collected data

There are some provisions regulating the control of personal information. Pursuant to the *Administrative Regulations on the Credit-Reporting Industry*, the data subject has the right to request the correction of erroneous or incomplete data gathered, stored or distributed by credit-reporting agencies. Credit-reporting agencies or data providers should label the relevant data in accordance with the requirements of the credit-reporting regulation authority of the State Council, verify and resolve the dispute within 20 days of receiving the request, and make a written response to the data subject. If the verification process shows that the relevant data is erroneous or incomplete, the data provider and the credit-reporting agency should proceed to correct them and delete the request. If the verification process does not confirm any error, the provider or agency shall record the findings of the verification process. If the data subject believes the credit-reporting agency, data provider, or information user has violated their rights or legitimate interests, they can file a complaint with the local credit-reporting regulatory authority, which should verify the matter. The data subject can also file a lawsuit directly before the competent court. In addition, the *Guideline for Personal Information Protection* stipulates that if the data subject finds any error regarding his or her data and requests correction, the data administrator shall check, verify, revise or supplement relevant information without prejudice to data integrity. Upon the data subject's request, the information administrator shall notify them whether the entity possesses their information as well as the content and status of such information truthfully and free of charge, unless the cost or frequency of notification are unreasonable.

---

[111] These measures include the following: 1) define user data security responsibilities for relevant departments, posts and branches; 2) put in place a process and security management system for user data collection, usage and relevant activities; 3) control the data access of staff members and agents, subject batch export, reproduction and destruction to review, and take measures to prevent data leaks; 4) properly maintain paper, optical, electromagnetic and other media that contain user data, and take proper measures for safe storage; 5) conduct access reviews and take anti-intrusion and antivirus measures for the information system where user data is kept; 6) record the person, time, place and items of user data operation; 7) safeguard the security of communication networks as required by telecommunications administration departments; and 8) apply any other necessary measures required by telecommunications administration departments.

XI. Roles and responsibilities of intermediaries

Pursuant to the *Telecommunications Regulations*, telecommunication means the activity of using wired or wireless electromagnetic or optoelectronic systems to transmit or receive voices, text, data, images or any other form of information. In China, Internet platforms thus fall under the scope of telecommunications. The telecommunications business is divided into basic telecommunications services (providing public network infrastructure, public data transmission and basic voice communications services)[112] and value-added telecommunications services (offering telecommunication and information services provided through the public network infrastructure).[113]

In the *Telecommunications Business Classification Catalogue* issued by the MIIT in 2003, basic telecommunications services and value-added telecommunications services are each divided into two categories. Internet Service Providers (ISPs) and Internet Content Providers (ICPs) all belong to Category II value-added telecommunications services. ISP refers to the use of access servers and relevant software and devices to set up nodes, using public telecommunications infrastructure to connect these nodes to the main Internet network and thus providing Internet access to users, while ICP refers to information services provided through the Internet. The business of intermediary Internet platforms falls into the ICP category.

Pursuant to the *Administrative Measures for Internet Information Services,* Internet information services are divided into commercial and noncommercial services.[114] The State subjects commercial Internet information services to a permit system and noncommercial Internet information services to a record-filing system. Inter-

[112] To operate basic telecommunications services, the following conditions shall be met: 1) the operator shall be a legally established company that specializes in basic telecommunications services and in which the State's equity or shareholding is not less than 51%; 2) a feasibility study and a technical plan for the formation of the network have been created; 3) there are funds and specialized personnel commensurate with the business activities to be engaged in; 4) there is a site and corresponding resources to carry out the business activities; 5) the operator has the reputation or the capability to provide a long-term service to its subscribers; and 6) other conditions specified by the State; furthermore, an application shall be submitted to the State Council's department in charge of the information industry.

[113] To operate value-added telecommunications services, the following conditions shall be met: 1) the operator shall be a legally established company; 2) there are funds and specialized personnel commensurate with the business activities to be developed; 3) the operator has the reputation or the capability to provide a long-term service to its subscribers; and 4) other conditions specified by the State; furthermore, an application shall be submitted to the State Council's department in charge of the information industry or the telecommunications administration authority of the province, autonomous region or municipality directly under the central government.

[114] The term 'commercial Internet information services' means service activities such as compensated provision to online subscribers through the Internet of information services or website production, and so on. The term 'noncommercial Internet information services' means the service activity of noncompensated provision to online subscribers through the Internet of information that is in the public domain and openly accessible.

net access providers shall not provide Internet access to any organization or individual that engages in the provision of Internet information services without having obtained permission or carried out record-filing procedures. Where, according to law, administrative regulations or relevant State regulations, engagement in the provision of Internet information services in respect of news, publishing, education, medical treatment, health, pharmaceuticals or medical apparatus, and so forth requires the examination and consent of the relevant competent authority, it shall be obtained in accordance with the law before applying for an operating permit or carrying out record-filing procedures. Anyone engaging in the provision of commercial Internet information services shall have in place sound procedures to ensure network and information security, including procedures to ensure website security, a system to manage the security and confidentiality of information and a system to manage the security of subscriber information. Anyone wishing to engage in the provision of commercial Internet information services shall apply to the telecommunications administration authority of the province, autonomous region or municipality directly under the central government or the State Council's departments in charge of the information industry for an Internet Information Services Value-added Telecommunications Service Operating Permit. If a commercial Internet information service provider applies to be listed in China or abroad or to establish an equity or cooperative joint venture with a foreign investor, it shall first be examined by, and shall obtain the consent of, the State Council's department in charge of the information industry. The ratio of the foreign investment shall comply with relevant laws and administrative regulations.

By the end of 2012, transactions concluded through online platforms constituted 90% of the entire online retail trading market in China. The dominance of online platforms is a characteristic of e-commerce in China. However, shopping via online platforms carries a number of risks. In case of a dispute, some operators may choose to cancel consumers' accounts, leaving them without the possibility to claim compensation. In 2000, a consumer in Shanghai sued an online platform, demanding that the platform assume joint liability for the counterfeit goods sold on the platform. In recent years, there have been a rising number of civil cases against online platforms, as online business operators have offered counterfeit products and infringed patent, trademark and other intellectual property rights.

In order to protect consumers' lawful rights and interests and strengthen their confidence in online shopping, it is necessary to define the responsibility of online trading platforms. The *Tort Liability Law* is the first legal instrument that defines the legal responsibility of intermediate platforms and sets forth the basic principles for the establishment of the platform's responsibility. Article 36 stipulates that Internet users and service providers shall assume tort liability if they utilize the Internet to infringe upon the civil rights of others. If an Internet user commits a tort by using Internet services, the infringed person is entitled to demand that the

Internet service provider take necessary measures, including, among others, the deletion, blocking and unlinking of the user. If the Internet service provider fails to take necessary measures in a timely manner upon notification, it shall be jointly liable together with the Internet user. The same applies if an Internet service provider is aware that an Internet user is infringing on the civil rights and interests of another person through its Internet services and fails to take necessary measures.

Pursuant to Article 44 of the *Consumer Protection Law*, when a consumer purchases goods or receives services through an online trading platform and their lawful rights and interests are infringed upon as a result, he or she may seek compensation from the seller or service provider. When the online platform provider is unable to provide the true name, address and valid contact method of the seller or the service provider, the consumer may seek compensation from the online platform provider; if the online trading platform provider makes any commitment that is more favorable to consumers, it shall be bound by that commitment. If granting compensation to the consumer, the online platform provider shall have the right to recover it from the seller or service provider. The online platform provider bears joint liability if it is or should have been aware that the seller or the service provider is using its platform to harm legitimate consumer rights and interests, but failed to adopt the requisite measures.

However, it remains a complicated issue whether all platform providers should be treated as counter lessors or exhibition sponsors, holding them liable for compensation irrespective of their conduct, even if the business operator no longer uses the platforms, or whether they should be held liable according to the principle of fault liability when they violate the duty of due diligence towards consumers. A draft amendment of the *Consumer Protection Law* proposed treating an online trading platform as a counter lessor, so that when the commodity seller or service provider no longer uses the platform, consumers may demand that the platform provider provide for compensation. However, there is a difference between online platform providers and counter lessors. An online service provider shall bear liability provided that it has committed a fault or breached its due diligence obligations. The e-commerce market would be significantly affected if online platforms were required to guarantee and compensate for any nonconforming operations. Online trading, unlike offline business activities, is virtual in nature, and an online platform usually has a huge number of business operators. Therefore, the relevant legislation has to balance diverse needs and interests. A statutory requirement of obligatory compensation is not necessarily good for consumers and the e-commerce market as a whole. As a result, the *Consumer Protection Law* holds online platform providers liable in the two aforementioned circumstances.[115]

[115] When the online platform provider is unable to provide the true name, address and contact of the seller or the service provider, the consumer may seek compensation from the online platform provider; when it is or should have been aware that the seller or the service provider is us-

XII. Access to user data by third parties

The relevant individuals' consent is required when a third party processes their personal information.[116] The *Decision of the Standing Committee of the National People's Congress concerning Strengthening Network Information Protection* establishes that gathering and using personal information requires obtaining the prior consent of those whose information is collected. The collection and the use of information must not occur in violation of applicable laws and regulations or the agreement between both sides. Thus 'using' includes, among other activities, the act of providing personal information to a third party. Therefore, personal information can be provided to a third party if prior consent is obtained and if it does not violate laws and regulations. The *Administrative Regulations on the Credit-Reporting Industry* contain clear rules for credit-reporting agencies concerning the transfer of personal information to a third party. They establish that any inquiry concerning consumer information requested from the credit-reporting agencies presupposes the written consent of the data subject in accordance with the purpose of data usage agreed upon by the information user and data subject, unless otherwise stipulated by law. If a credit-reporting agency, data provider, or information user obtains the data subject's authorization or consent using the standard contract form, there should be clear and sufficient indications in the contract to attract the data subject's attention and guarantee a clear statement of authorization by the data subject. The information user should use the consumer data only for the purpose agreed upon by the data subject and not for any other purpose. The information user should not provide data to any third party without the data subject's consent. In addition, according to the *Guideline for Personal Information Protection,* the transfer of personal information to other organizations and institutions requires prior assessment of whether or not they can process personal information as required by the *Guideline*, and whether they can ensure that transferred personal information will not be obtained by any individual, organization or institution other than the intended recipient. Personal information shall remain complete and usable after transfer. Without the explicit consent of the data subject, or the explicit approval of the competent authorities, the data administrator shall not transfer personal information to foreign recipients, including individuals outside China and organizations registered overseas.

---

ing its platform to harm legitimate consumer rights and interests, but failed to adopt the requisite measures, it shall bear joint liability.

[116] *Xiao Dong*, Data Protection in China: Overview, <http://uk.practicallaw.com/4-519-9017?q=*&qp=&qo=&qe=> (last accessed 25 June 2015).

XIII. Provisions on data retention

Pursuant to Article 14 of the *Administrative Measures for Internet Information Services*, Internet information service providers that engage in the provision of services such as news, publishing or electronic bulletin board services shall keep a record of the information they provide, the time of dissemination and the URLs or domain names. Internet access service providers shall keep a record of the time online subscribers are online, the subscribers' account numbers, the URLs or domain names and the callers' telephone numbers. Both Internet information service providers and Internet access service providers shall keep copies of such records for 60 days and shall provide them to the relevant State authorities when the latter make inquiries in accordance with the law. According to Article 23 of the *Regulations on the Administration of Internet Access Service Business Sites*, operators of sites of Internet access services shall check and register the users' ID and record their Internet access information, keep copies of such records for 60 days and present them in case of inquiries by the culture administration departments or public security organs.

In addition, Article 62 of the *Telecommunications Regulations* stipulates that if a telecommunication business operator, while providing public information services, discovers information transmitted on its telecommunications network that clearly falls within the scope specified in Article 57,[117] it shall immediately stop the transmission, keep the relevant records and submit a report to the competent authority. In this case, the aforementioned 60-day time limit will not apply.

Pursuant to the *Administrative Measures for Online Trading*, the operator of a third-party online platform shall check, record and store commodity and service information released via the platform and the time of release. The information in respect of an online business operator's business license and personal identity shall be kept for no less than two years from the date when the business operator cancels its registration for the platform, and transaction records and backup copies of other information shall be kept for no less than two years from the date when the

[117] Article 57: "No organization or individual may use telecommunications networks to produce, reproduce, disseminate or transmit information with content that:
1. opposes the fundamental principles determined in the Constitution;
2. compromises State security, discloses State secrets, subverts State power or damages national unity;
3. harms the dignity or interests of the State;
4. incites ethnic hatred or racial discrimination or damages interethnic unity;
5. sabotages State religious policy or propagates heretical teachings or feudal superstitions;
6. disseminates rumors, disturbs social order or disrupts social stability;
7. propagates obscenity, pornography, gambling, violence, murder or fear or incites the commission of crimes;
8. insults or slanders a third party or infringes upon the lawful rights and interests of a third party; or
9. includes other content prohibited by laws or administrative regulations."

transaction is completed. The third-party online platform operators shall use an electronic signature, data backups, failure recovery and other technical measures to ensure the integrity and security of online transaction data and the materials and ensure the authenticity of original data. Relevant service operators that provide online commodity transactions with network access, server custody, virtual space rental and websites, website or webpage design and production, shall require applicants to provide certificates of operation qualifications and truthful personal identity information, sign the service contract and record their online activities in accordance with law. An applicant's business license or identity information shall be kept for no less than two years from the date when the service contract is terminated or performance of the service contract is completed.

XIV. Transfer of data on an international scale, transfer to third countries and requirements for data transfer outside the country

Few provisions exist regulating the transborder flows of personal information. Pursuant to Paragraph 2 of Article 11 of the *Law on Banking Regulation and Supervision*, the banking regulatory authority of the State Council shall make relevant arrangements to preserve the confidentiality of information during the process of exchanging supervisory information with the banking supervisory authorities in other countries or regions. Pursuant to Article 24 of the *Administrative Regulations on the Credit-Reporting Industry*, business activities of organizing, preserving and processing consumer or commercial data, gathered within the territory of China by credit-reporting agencies, should take place within the territory of China. Any transfer of data to foreign organizations or individuals shall comply with the laws, regulations and relevant provisions of the credit-reporting regulation authority of the State Council. The *Guideline for Personal Information Protection* stipulates that without the explicit consent of the data subject, or the authorization of the competent authority, the data administrator shall not transfer personal information to foreign recipients, including individuals outside China and organizations registered overseas.

XV. Enforcement

1. Civil law

Pursuant to Article 50 of the *Consumer Protection Law*, if a business operator is found to have violated a consumer's personal dignity, freedom or right to personal information protection, he must stop the violation, restore the consumer's reputation, eliminate the effects of the violation, apologize and compensate any losses incurred. Loss compensation is the most basic and widely used method for a business operator to assume responsibility, and requires the payment of a certain amount of money to compensate the consumer's losses. Article 20 of the *Tort*

Liability Law[118] contains clear provisions on how to calculate such losses: when a business operation infringes upon the consumer's rights and interests and causes loss of property, the consumer shall be compensated in accordance with the loss suffered; when such a loss is indeterminable and the business operator gained from the tort, loss compensation shall be made on the basis of such gains; if such gains are indeterminable or the consumer and the business operator fail to reach an agreement on the amount of compensation, both of them may file a lawsuit before the people's court and ask it to determine the amount of compensation. Article 54 of the *Civil Procedure Law* stipulates that where the subject matters of an action falls into the same category and one of the parties has numerous litigants but the exact number of the litigants is uncertain when the lawsuit is filed, the people's court may issue a public notice to explain the nature of the case and the claims of the litigation and inform those interested persons who are entitled to the claim that they must register their rights with the people's court within a fixed period. Those who have registered their rights with the people's court may elect representatives from among themselves to proceed with the litigation; if the election fails to meet its purpose, such representatives may be determined by the people's court through consultation with those who have registered their rights with the court. The acts of litigation taken by these representatives shall bind all litigants of the party whom they represent. However, any substitution of representatives, relinquishing claims, acceptance of claims of the opposing party, or negotiating settlements shall be approved by the litigants of the party. The judgments or written orders rendered by the people's court shall bind all those interested persons who have registered their rights with the court. Such judgments or written orders shall also apply to those who have not registered their rights but have instituted legal proceedings during the time of the statute of limitation. The *Civil Procedure Law*, revised in 2012, adds that "relevant bodies and organizations prescribed by the law may bring a suit to the people's court against such acts as environmental pollution, harm of consumers' legitimate interests and rights and other acts that undermine the public interest". Therefore, a business operator is likely to face group action or civil public proceedings if it causes harm to many consumers' personal information rights.

[118] Article 20: "Where any harm caused by a tort to a personal right or interest of another person gives rise to any loss to the property of the victim of the tort, the tortfeasor shall make compensation as per the loss sustained by the victim as the result of the tort. If the loss sustained by the victim is hard to determine and the tortfeasor obtains any benefit from the tort, the tortfeasor shall make compensation as per the benefit obtained by it. If the benefit obtained by the tortfeasor from the tort is hard to determine, the victim and the tortfeasor disagree upon the amount of compensation after consultation, and an action is brought to a people's court, the people's court shall determine the amount of compensation based on the actual situation."

2. Criminal law

Serious infringements of the right to privacy, reputation and personal information are sanctioned by several provisions of the Criminal Law.[119] Article 57 of the *Consumer Protection Law* imposes criminal liability when a business operator provides goods or services in violation of this Law, infringes upon consumers' lawful rights and interests, and such acts have constituted a crime. The *Law on Banking Regulation and Supervision* (2003), revised in 2006, adds the following provision on privacy protection to Paragraph 2 of Article 43: "the supervisory staff of the banking regulatory authority committing embezzlement, bribery or divulgence of national, commercial or personal confidential information shall, if the case constitutes a crime, be investigated for criminal liability according to law, and if the case does not constitute a crime, be subject to administrative sanctions according to law".

The *Notice on Legally Punishing Criminal Activities Infringing upon the Personal Information of Citizens* issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security in 2013 clarifies various boundaries of criminal accountability. The *Notice* stresses the need for "correctly applying the law to achieve organic unity between legal and social effects". The crime against the personal information of citizens is a new type of crime. The public security authorities, people's procuratorates and people's courts at all levels shall,

[119] See Article 246 of the *Criminal Law*: "Whoever, by violence or other methods, publicly humiliates others or invents stories to defame them, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of no more than three years, criminal detention, public surveillance or deprivation of political rights."
Article 252 of the *Criminal Law:* "Whoever conceals, destroys or unlawfully opens another person's letter, thereby infringing upon the citizen's right to freedom of correspondence, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of no more than one year or criminal detention."
Article 253 (A) of the *Criminal Law*, added through the *Amendment (VII) to the Criminal Law* in 2009 in response to violations of the right to personal information protection: "Where any staff member of a state organ or an entity in a field such as finance, telecommunications, transportation, education or medical treatment, in violation of the state provisions, sells or illegally provides personal information on citizens, which is obtained during the organ's or entity's performance of duties or provision of services, to others, shall, if the circumstances are serious, be sentenced to fixed-term imprisonment of no more than three years or criminal detention, and/or be fined.
Whoever illegally obtains the aforesaid information by stealing or any other means shall, if the circumstances are serious, be punished under the preceding paragraph.
Where any entity commits either of the crimes described in the preceding two paragraphs, it shall be fined, and the direct liable person in charge and other directly liable persons shall be punished under the applicable paragraph."
Pursuant to the Supplementary Provisions of the Supreme People's Court and the Supreme People's Procuratorate on Implementing the Accusations as Defined in the Criminal Law of the People's Republic of China (IV), the aforesaid amendment establishes two new crimes prior to the enactment of a substantive law on personal information protection (selling or illegally providing personal information on citizens, illegally obtaining citizens' personal information), embodying the characteristic of Chinese legislation.

in the interest of effectively protecting the safety of personal information of citizens and maintaining social harmony and stability, learn from past successful legal precedents, take into overall consideration the frequency, quantity, and means in respect of selling, illegally providing or illegally obtaining personal information, the amount of profit, the damages caused and other factors, and intensify their efforts in combating against such crimes according to law, to ensure favorable legal and social effects. The subjects of the crime of selling or illegally providing the personal information of citizens include, in addition to the staff of state authorities or entities of finance, telecommunications, transport and health care, the employees of other enterprises and public institutions in the service industry such as the commercial or real-estate industry who obtain the personal information of citizens during the course of performing their duties or providing services. The personal information of citizens includes the name, age, valid certificate number, marital status, employer, educational background, CV, family address, phone number and other information or data that can identify citizens or involves the personal privacy of citizens. For those selling or illegally providing the personal information of citizens obtained during the course of performing duties or providing services to others, if the information is used by others to commit crimes which cause the personal injury or death of the victims, or cause significant economic losses or negative social impacts, or the quantity of personal information of citizens sold or illegally provided is large, or the amount of illegal proceeds is large, they shall be subject to criminal liabilities for the crime of illegally selling or illegally providing the personal information of citizens. For those who illegally obtain the personal information of citizens by stealing, purchase or any other means, if the quantity of information is large, or the amount of illegal proceeds is large or other serious consequences are caused, they shall be subject to criminal liabilities for the crime of illegally obtaining the personal information of citizens. For those who use the illegally obtained personal information to commit other criminal acts, if multiple crimes are constituted, they shall be subject to the joinder of penalties for all the crimes they commit. If an entity commits a crime against the personal information of citizens, the directly liable person in charge and other directly liable persons shall be subject to criminal liabilities. The aim is to reinforce the application of property-related penalties according to law to deprive the criminals of their illegal proceeds and capital, preventing them from reoffending.

The *Notice* also defines the principles of jurisdiction. The crime against personal information often involves an extensive and intricately structured criminal network, and the place of its occurrence, the place it affects and the place where criminals are located may not be the same. Moreover, since such criminal activities are often committed via a variety of means such as the Internet, mobile electronic devices, instant messaging tools and e-mail, investigation and evidence collection is challenging. Public security authorities, people's procuratorates and people's courts at all levels shall, based on their respective duties and responsibilities, fur-

ther strengthen communication, coordination and cooperation to ensure the smooth progress of case filing, investigation, arrest approval, examination and prosecution as well as trial. Cases shall be filed for investigation and transferred for prosecution in a timely manner. When several public security organs are all entitled to jurisdiction, the public security organ that first accepted the cases shall have the jurisdiction, and if necessary, the public security organ of the principal place where the crime was committed shall have the jurisdiction. If the jurisdiction over a criminal case is unclear or disputed, the public security organs concerned shall settle it through consultation. If consultation fails, the jurisdiction shall be designated by their common upper level. For a case under designated jurisdiction, if suspects are to be arrested, the designated public security organ shall submit a request to the people's procuratorate at the same level for examination and approval. If public prosecution is required, the designated public security organ shall transfer the case to the people's procuratorate at the same level for examination and decision. If it decides that the case shall be prosecuted by the upper-level people's procuratorate or another people's procuratorate at the same level, it shall transfer the case to the people's procuratorate that has the jurisdiction. When the people's procuratorate considers it necessary to designate the competent court in accordance with the *Criminal Procedure Law*, it shall consult with the people's court to designate said court. When a case of infringement against citizens' personal information is complicated and difficult, the people's procuratorate may send its staff members in a timely fashion to communicate and coordinate with the public security organ concerning evidence collection and other issues. Concerning the request for approval of arrest and prosecution submitted by the public security organ, if conditions are satisfied, the people's procuratorate shall approve or prosecute as soon as possible in accordance with law. If supplementary investigation is necessary, it shall prepare a specific and detailed outline for supplementary investigation. The people's court shall strengthen the ranks of judges and judgment accuracy and try and conclude the case in accordance with law and in a prompt manner.

3. Administrative law

China has a highly decentralized structure for the administrative enforcement of personal information protection, as various administrative departments enforce such protection in their respective sectors or areas.[120] A uniform and specialized agency for personal information protection is still lacking. Pursuant to Article 56 of the *Consumer Protection Law*, if a consumer's personal dignity or freedom or right

[120] For example, according to Article 3 of the *Provisions on the Protection of Personal Information of Telecommunication and Internet Users*, the Ministry of Industry and Information Technology and the communications administration bureaus in various provinces, autonomous regions, and municipalities shall supervise and administer the protection of personal information of telecommunications and Internet users.

to personal information protection has been violated, administrative penalties set out in specific laws and regulations shall be implemented by the competent administrative authorities. If such penalties do not exist, the industrial and commercial administration departments or other relevant administrative departments shall facilitate the rectification and, depending on the circumstances, impose one or several of the following penalties: issuance of a warning, confiscation of the illegal income and/or imposition of a fine of between one and ten times the amount of the illegal income; where no illegal income is obtained, a fine of no more than RMB 500,000 shall be imposed; where the circumstances are serious, the business operator shall be ordered to cease business operations for reorganization and have its business license revoked. Therefore administrative enforcement usually is carried out by the industrial and commercial administration departments, or by other administrative departments if thus set out in the laws and regulations. Before its amendment, the *Consumer Protection Law* designated industrial and commercial administration departments as the enforcers of administrative penalties (Article 50). Later, the amendment proposed that, in the absence of clear provisions in laws and regulations, other administrative departments may also impose penalties on business operators in accordance with this Law. As a result, "other administrative departments" were added as enforcing authorities. This shows the decentralized structure of administrative enforcement.

Violations of personal information rights through the Internet may occur in and affect a number of places. This has led to uncertainty with regard to the administrative jurisdiction of competent enforcement authorities. As a consequence, Article 41 of the *Administrative Measures for Online Trading* stipulates that violations in respect of online commodity trading or relevant services shall be under the jurisdiction of the industrial and commercial administration departments at or above county level where the business operators that have committed violations are located. For business operators that do business via third-party online platforms, their violations shall be under the jurisdiction of industrial and commercial administration departments at or above county level where the operators of the respective third-party online platforms are located. If it is difficult to enforce the protection of personal information rights according to such jurisdiction rules, cases may be transferred to the industrial and commercial administration departments at or above county level where the persons committing the violations are located. When two or more industrial and commercial administration departments disagree on their jurisdiction regarding violations in respect to online commodity transactions and relevant services, they shall report to the higher industrial and commercial administration department for the designation of jurisdiction. When a violation in respect of online commodity transactions or relevant services is of national significance, or involves a serious infringement upon a great number of consumers, or turns out to be too complicated to be resolved by the industrial and

commercial administration departments, the SAIC may investigate and deal with it, or appoint one of its provincial branches to do so.

XVI. Role of self-regulation and co-regulation

Articles 36 and 37 of the *Consumer Protection Law* define the status and role of consumer associations.[121] In 2004, the Chinese Institute of Certified Public Accountants promulgated the *Interim Measures for the Administration of Members' Credit Archives* ('*Interim Measures*'), the first systematic provisions on members' credit information ever released by an industry association. Pursuant to the *Interim Measures*, an individual member's credit archive consists of basic information, reminding information and alert information. Local branches shall keep confidential personal privacy and business secrets, while provincial branches shall designate specific persons to administrate, supplement and update members' credit archives to ensure their truthfulness and integrity. Pursuant to Article 21 of the *Provisions on the Protection of Personal Information of Telecommunication and Internet Users*, telecommunications and Internet industry associations are encouraged to formulate self-regulatory provisions on personal information protection in accordance with the law, guide members to strengthen self-regulation and improve the level of user data protection. In 2006, the Dalian Software Industry Association issued the *Rules of Personal Information Protection for the Software and Information Service Industry in Dalian*, which constituted China's first local industry self-regulatory rules for personal information protection. They define concepts such as 'personal information', 'data subject', the 'gathering, processing, using and entrusting of personal information' and 'data administrator', and set out the principles, relevant organizations, responsibilities and implementation of personal information protection. They represent an important attempt to facilitate self-regulation in the information service industry and to introduce an internationally accepted practice. Furthermore, they provide a point of reference for the software and information service industry in Dalian in carrying out personal information protection. Therefore, the *Rules* play a positive role

[121] According to the *Consumer Protection Law*, a consumer association exercises the following non-profit duties and functions: (1) provide information and advice to consumers, enable consumers to better safeguard their lawful rights and interests, and guide them to adopt a pattern of consumption that is civilized, healthy, resource saving and environmentally friendly; (2) participate in the promulgation of laws, regulations, rules and statutory standards related to consumer protection; (3) participate in the supervision and inspection of commodities and services by the relevant administrative departments; (4) report to, inquire of or make suggestions to relevant administrative departments on issues concerning the legal rights and interests of consumers; (5) accept complaints by consumers and conduct investigations into and mediations of such complaints; (6) where a complaint involves issues concerning the quality of commodities and services, it may require a qualified appraiser to appraise the quality. Said appraiser shall advise the appraisal findings; (7) assist aggrieved consumers in instituting legal proceedings or bringing actions in accordance with this Law against acts which harm their legal rights and interests; and (8) reveal and criticize acts harmful to the legal rights and interests of consumers through the mass media.

for the standardization of personal information protection in the information service industry across the country. Finally, the *Bylaw of the Internet Society of China* (ISC) establishes the possibility of elaborating self-regulatory provisions for the Internet industry.[122]

C. Consumer Data Protection in Germany *(Prof. Dr. Gerald Spindler)*

I. Introduction

Germany has a population of 80 million citizens; among them, more than 80 % of people older than 10 years use the internet. A total of 87 % of German households (i.e. more than 40 million households) are equipped with IT and 29.7 million use mobile applications. All types of e-commerce are offered in Germany and most Internet users (more than 82 %) purchase goods on the Internet. Compared to other countries in the EU, only the UK has a higher rate of online shopping than Germany.

[122] The mandate of the Internet Society of China is to: (1) unite enterprises, public institutions and social organizations across the Internet industry, transmit the wishes and requests of its members to the authorities, enhance the communication and liaison between the responsible departments and members, and popularize national policies, laws and regulations for members; (2) formulate and implement self-regulations for the Internet industry, harmonize relations, resolve disputes and promote communication and coordination among members, facilitate the self-regulation of the Internet industry, safeguard national cyberspace and information security, and protect the interests of overall industry and users; (3) analyze the development of the Internet industry, the application of new technologies and other key issues that impact upon industry development, publish data and research reports, propose policies to competent government departments, and provide relevant information services for the industry; (4) carry out workshops, forums, annual conferences and other activities relevant to Internet development and management, promote exchange and cooperation across the Internet industry, and promote the Internet to play a positive role in Chinese economic, cultural, social and ecological undertakings; (5) formulate Internet industry standards and carry out credit rating, qualification review, award application, appraisal and recommendation as approved, authorized or entrusted by competent authorities; (6) engage in international exchange and cooperation, and participate in international affairs, including the formulation of global Internet policies, norms and standards; (7) conduct public welfare activities and guide members to strengthen social responsibility and professional ethics; (8) offer specific training in respect of law, management, technology and personnel, improve members' management and service capacity, and enhance personnel qualification; (9) carry out cybercultural activities, guide netizens to use the Internet properly, accept and assist the authorities concerned to handle complaints and reports about online unwholesome information and activities, and purify the Internet environment; and (10) undertake other matters entrusted it by members, other social organizations or responsible departments.

II. Overview and scope of legislation addressing consumer data protection

German data protection law has largely influenced EU data protection directives and implements them; therefore, any overview of the German legal framework would be incomplete without reference to European law. Nevertheless, it is important to bear in mind that Germany has been the "origin" of European data protection, leading the way in the early-1970s with one of the first acts on data protection. Moreover, the German Constitutional Court influenced the international debate heavily by deriving the fundamental right of "personal data self-determination" from the Constitution as part of the fundamental rights of mankind.[123] The legal landscape even today is marked by its rulings, which have enlarged the whole (constitutional) base for data protection, for instance, by installing a new fundamental right of the individual to trust the integrity and solidity of IT systems.[124] However, the following illustration of German data protection is hampered by the fact that the existing legal framework may be changed in a significant way in the coming months if the EU adopts a new proposal of the EC, the so-called General Data Protection Regulation (GDPR). Thus, the following analysis will take into account the existing legal framework as well as the (probable) upcoming new EU regulation.

1. Character of the legislation

German data protection is enshrined in different acts (laws) which are based on different European directives. Directives aim at harmonizing different national laws of EU member states in order to create and foster the internal European market (e.g. product safety standards).[125] They lay down certain objectives to be achieved in every member state. National authorities have to adapt their laws to meet these goals by implementing the directives into national law, but are free to decide how to do so. Nevertheless, the directives have to be implemented in a way that the best result is achieved *("effet utile")*. Article 288 of the Treaty on the Functioning of the EU (TFEU) defines how the EU's competences can be exercised.[126] Directives may differ concerning the grade of harmonization, be it a *"de minimis"* harmonization, which leaves member states some leeway to pass laws, or a full harmonization, preventing member states from going beyond the directive. Each

---

123 German Federal Constitutional Court (Bundesverfassungsgericht), decision of 15/12/1983 – 1 BvR 209/83 among others – BVerfGE 65, 1 (census decision).

124 German Federal Constitutional Court (Bundesverfassungsgericht), decision of 27/02/2008 – 1 BvR 370/07, 1 BvR 595/07 – BVerfGE 120, 274 (online searches).

125 http://ec.europa.eu/eu_law/introduction/what_directive_en.htm.

126 Treaty on the Functioning of the European Union, *Official Journal C 326 of 26/10/2012, 0001 – 0390, available at* http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN. *Article 288 (ex Article 249 TEC): "[…] A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.[…]."*

directive specifies the date by which the national implementing laws must be adopted. A directive is addressed to the member states, not to the citizens. Only if directives state rights for citizens *and* are not implemented in due time by national authorities, may citizens claim those rights directly. By contrast, regulations[127] are passed either jointly by the Council of the EU and European Parliament, or by the EC alone,[128] and are the most direct form of EU law – as soon as they are passed, they have binding legal force throughout every member state. They have the same effect as national laws and, eventually, overrule them. National governments do not have to take action themselves to implement EU regulations.

The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data was adopted by the EC in 1995 to protect the privacy of individuals.[129] The directive generally prohibits the processing of personal data unless the person concerned has expressly consented to the processing of sensitive data or the processing is necessary to "keep the dissolution of the rights and obligations of the data controller in the field of employment law." Areas related to the second and third so-called pillars of the EU, i.e. the common foreign and security policy, police and judicial cooperation in criminal matters, are exempted from the scope of the directive (Art. 3, Para. 2 of the Directive). In addition, the directive allows member states to provide for exceptions in cases of substantial public interest. With regard to telecommunication issues, the DPD is complemented by the Directive 2002/58/EC (Directive on Privacy and Electronic Communications). As Data Protection Directive 95/46/EC (1995) intended to encourage the free movement of personal data within Europe by harmonizing national provisions on data protection,[130] it is today widely considered as being outdated, as it does not deal with the new challenges of the internet.[131] Moreover, the implementation scope of the directive led to different interpretations of the national data protection laws with regard to a minimum standard.[132] Therefore, the EC passed the proposal of a new GDPR in

---

[127] Article 288 of the Treaty on the Functioning of the European Union (ex Art. 249 TEC): A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.

[128] *Wieczorek*, DuD 2013, 644 (646).

[129] *Hon/Millard/Walden,* Who is Responsible for "Personal Data" in Cloud Computing?, The Cloud of Unknowing, Part 2, p. 3.

[130] *Hon/Millard/Walden, The* Problem of "Personal Data" in Cloud Computing – What Information is Regulated?, The Cloud of Unknowing, Part. 1, p. 4; *Leonard*, International Data Privacy Law, 2014, 53 (53).

[131] *Tene*, International Data Privacy Law 2011, 15 (15); *Hon/Millard*, Data Export in Cloud Computing – How can Personal Data be Transferred outside the EEA?, The Cloud of Unknowing, Part 4, p. 2; *Sartor*, International Data Privacy Law 2013, 3 (3).

[132] *Klar*, ZD 2013, 109 (109 ff.); While one could have understood the *Lindqvist decision* of the ECJ (of 06/11/2003 – C-101/91) in the way that Directive 95/46/EC requires only minimum standards of the member states, it is obviously after the *ASNEF decision* (24/11/2011- C-468/10) that the conditions of admissibility of the data handling were largely fully harmonized.

order to ensure a uniform standard of data protection.[133] On 21 October 2013, the European Parliament's LIBE Committee (Committee for Civil Liberties, Justice and Home Affairs) adopted a number of proposed changes to the GDPR published by the EU Commission on 25 January 2012.[134] On 22 October 2013, the Home Affairs Committee of the European Parliament started negotiations with the EC and the Council of the EU – this so-called trialogue. On 12 March 2014, the European Parliament adopted a legislative resolution on the proposal after the first reading, adopting the LIBE Committee's changes to the original proposal.[135] On 15 June 2015, the Council of the EU presented a general approach on the GDPR with several changes and amendments, which led to a new series of trilogue negotiations between the Council, the European Parliament and the EC.[136] The EU expects to complete the regulation by the end of 2015.[137] The proposed data protection regulation would be directly binding without a national act of implementation being necessary. This is an important difference between the current directive and the proposed regulation, since the directive had to be implemented into national laws by the governments of the member states.

However, one has to bear in mind that the ECJ handed down a decision a few years ago stating that the existing Data Protection Directive (DPD) is fully harmonizing, so the differences between the proposed GDPR and the DPD are somewhat lessened. Because of this, member states are not allowed to provide a lower level of protection than the directive demands, nor are they allowed to go beyond it.[138] Directive 95/46/EC imposes complete harmonization of national

133 *Eckhardt/Kramer/Mester*, DuD 2013, 623 (630).

134 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR) in the version adopted by the European Parliament after the LIBE Committee's vote, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//EN; *Heinemeyer*, Verfahrensstand-Anzeiger; *Härting*, CR 2013, 715 (715 ff.).

135 European Parliament legislative resolution of 12/03/2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR), COM (2012) 0011-C7-0025/2012-2012/0011 (COD) (Ordinary legislative procedure: first reading), available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.

136 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR) of 15/06/2015 – ST 9565 2015 INIT, available at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

137 A timetable for the reform is available at http://www.eppgroup.eu/de/news/Data-protection-reform-timetable.

138 ECJ, decision of 24/11/2011 – C-468/10, C-469/10 – Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado.

laws[139] and intends to ensure free movement of personal data, while guaranteeing a high level of protection for the rights and interests of data subjects, equivalent in all member states. Consequently, Art. 7 of Directive 95/46/EC sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as lawful. That interpretation is corroborated by the term "may be processed only if," which demonstrates the exhaustive and restrictive nature of the list appearing in that article. Thus, the member states cannot add new principles relating to the lawfulness of processing data, nor can they impose additional requirements.[140] Therefore, German data protection acts always have to be interpreted in the light of European directives, particularly as the ECJ can harmonize the application of European law at a judicial level. There are hardly any German acts which are not related to European directives in the field of data protection, except in some specific areas of social security or tax law concerning the processing of data by state authorities.

National administrative regulations on a federal level in Germany do not exist, as the enforcement (and, thus, interpretation) of data protection acts is left to the *Länder* (the semi-autonomous provinces in Germany). Consequently, it is up to these authorities to find common administrative regulations. In practice, a (informally established) circle called the "*Düsseldorfer Arbeitskreis*" gathers all representatives of the supervisory authorities of the *Länder* in order to find common solutions. The recommendations of this circle play a significant role in practice – however, they are not binding for supervisory authorities or courts. According to a recent ECJ decision, these supervisory authorities are totally independent of any government; they are free to check data processing carried out by these governments, etc. and can refuse any kind of influence.[141]

Courts, which are independent from government and administration, play an important role, as they have to interpret the law and hand down decisions in particular cases. However, courts in Germany, in contrast to other countries, may not establish general binding rules or principles. Nevertheless, courts often develop fundamental principles in individual cases that touch on basic issues. Even though these decisions do not formally bind other courts, they will often follow the principles established in leading cases by the highest courts, such as the Federal Court of Justice (*Bundesgerichtshof*) or the Federal Administrative Court (*Bundesverwaltungsgericht*). Finally, the Constitutional Court plays an exceptional role, as its decisions have the same binding effect as laws enacted by Parliament. Hence, all general

---

[139] ECJ, decision of 24/11/2011 – C-468/10, C-469/10 – Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado; *Kühling*, EuZW 2012, 281 (282).

[140] ECJ, decision of 04/10/2001 – C-450/00 – Commission/Grand Duchy of Luxembourg.

[141] ECJ, decision of 09/03/2010 – C-518/07 – European Commission/Federal Republic of Germany; criticized by *Frenzel*, DÖV 2010, 925 (925 ff.); see also in respect of Austria: ECJ, decision of 16/12/2002 – C-614-10 – European Commission/Republic of Austria.

principles derived from the Constitution have to be obeyed strictly by other courts, as well as governments and administrations.

2. General legal framework for consumer data protection

The basic act for German data protection is the German Data Protection Act (*Bundesdatenschutzgesetz*: BDSG), implementing the European data directives. This act applies to all activities of processing personal data, be it the public[142] or the private sector. However, this general act is superseded by many sector-specific acts, some of which are discussed in the following; however, not all of them can be listed here.[143]

3. Telecommunication

One of the main branch-specific acts on data protection concerns the telecommunication sector. Based on specific European telecommunication directives, the German Telecommunication Act contains specific provisions for the processing of personal data.[144] Certain parts of these directives[145] and the German Telecommunication Act have been heavily debated with regard to the discussion on data retention.

4. Specific acts for e-commerce

In addition to the BDSG and the Telecommunication Act (*Telekommunikationsgesetz*), a third act has to be complied with regarding e-commerce: the Telemedia Act (*Telemediengesetz*). This act refers to data protection rules based on the European Telecommunication Directive, as well as the so-called E-Privacy Directive.[146]

---

142 As long as the federal government has the competence and not the provinces (*Länder*).

143 This study does not deal with specific legal provisions of tax law, social security law, etc.

144 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector of the European Parliament and of the Council of 12/07/2002 (Directive on privacy and electronic communications – ePrivacy directive), see Art. 5 – 10, Art. 12 – 13; amended by directive 2009/136/EC of the European Parliament and of the Council of 25/11/2009; also Art. 25 (2) of directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) of the European Parliament and of the Council of 07/03/2002, which is integrated in section 47 of the German Telecommunication Act; furthermore Art. 4 (3) of Directive 2002/19/EC on access to and interconnection of electronic communications networks and associated facilities (Access Directive) of the European Parliament and of the Council of 07/03/2002.

145 Directive on the retention of data 2006/24/EC of the European Parliament and of the Council of 15/03/2006, declared invalid by the ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others).

146 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector of the European Parliament and of the Council of 12/07/2002 (Directive on privacy and electronic communications – ePrivacy directive).

Telemedia are all telecommunication-based services which do not qualify as "telecommunication" in the sense of the Telecommunication Act, e.g. websites and host providers.

III. Applicability of data protection acts

Article 4, Para. 1 of the DPD states that each member state shall apply the national provisions it adopts in accordance with the directive regarding the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the member state; when the same controller is established on the territory of several member states, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) the controller is not established on the member state's territory, but in a place where its national law applies by virtue of international public law; (c) the controller is not established on EC territory and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said member state, unless such equipment is used only for purposes of transit through the territory of the EC. Even an end-users machine might be "equipment situated on the territory of a member state" if it is used for storing a cookie or collecting data with JavaScripts.[147] By contrast, if a webpage is accessible from the EU, but hosted by a server in a third country, no equipment situated inside the EU is used. For the territorial scope of the directive, it is not relevant at where a service is aimed, but where the resources used for providing this service are located (this principle will change with the upcoming GDPR, see 4.1.1).[148] A cloud server in Europe would be qualified as "equipment" according to the DPD.[149] Even though Recital 19 of the DPD states that an establishment on the territory of a member state "implies the effective and real exercise of activity through stable arrangements," there is no legal definition of "establishment" in the DPD. On the other hand, it is not necessary for the establishment to be independent from the controller in order to be considered as a controller itself (for the definition of "data controller," see 3.6).[150] One of the cases decided by the ECJ highlighted the

---

[147] As, for example, stated by the German court KG Berlin in its ruling from 24/01/2014, 5 U 42/12, 28 f., available at http://www.berlin.de/imperia/md/content/senatsverwaltungen/justiz/kammergericht/presse/5_u_42_12_urteil_vom_24.1.2014_kammergericht_anonymisiert.pdf?start&start&ts=1392399485&file=5_u_42_12_urteil_vom_24.1.2014_kammergericht_anonymisiert.pdf.

[148] *Hon/Hörnle/Millard,* Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law?, The Cloud of Unknowing, Part 3, p. 7 ff.; *Wieczorek,* DuD 2013, 644 (646); *Gabel*, in Taeger/Gabel*,* BDSG, Para. 1, Recital 59.

[149] *Giedke*, Cloud Computing, p. 205 ff.

[150] The German court *Oberverwaltungsgericht* (OVG = circuit court in administrative affairs) Schleswig-Holstein had to decide whether or not European data protection law was applicable for the data processing of Facebook, also in which European country Facebook's respective establishment is

difficulties in practice of handling the notion of "establishment" in the DPD.[151] In the final judgment, the ECJ followed the General Advocate's opinion[152] and held:

> *In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.*[153]

---

acting. The court ruled that even though the US American parent company Facebook Inc. is the only shareholder of the Irish subsidiary Facebook Ltd., the Irish company can be qualified as an establishment within the EU, as Facebook Ireland obviously handled some of the data processing, OVG Schleswig Holstein, decision of 22/04/2013; however, another German court (*Kammergericht* KG Berlin (circuit court in civil law issue) in its ruling from 24/01/2014) contradicted that perspective, saying that since the parent group Facebook Inc. is responsible for all decisions concerning data processing in the end, the Irish subsidiary Facebook Ltd. is not an establishment in the sense of the directive. This interpretation of "establishment" does not comply with the directive's distinction between "controller" and "establishment."

[151] ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález.

[152] Opinion of Advocate General *Jääskinen*, delivered on 25/06/2013 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja González, Recitals 64 – 67: "In my opinion the Court should approach the question of territorial applicability from the perspective of the business model of Internet search engine service providers. This, as I have mentioned, normally relies on keyword advertising which is the source of income and, as such, the economic raison d'être for the provision of a free information location tool in the form of a search engine. The entity in charge of keyword advertising (called 'referencing service provider' in the Court's case-law) is linked to the internet search engine. This entity needs presence on national advertising markets. For this reason Google has established subsidiaries in many Member States which clearly constitute establishments within the meaning of Article 4(1)(a) of the Directive. It also provides national web domains such as google.es or google.fi. The activity of the search engine takes this national diversification into account in various ways relating to the display of the search results because the normal financing model of keyword advertising follows the pay-per-click principle. 65. For these reasons I would adhere to the Article 29 Working Party's conclusion to the effect that the business model of an internet search engine service provider must be taken into account in the sense that its establishment plays a relevant role in the processing of personal data if it is linked to a service involved in selling targeted advertisement to inhabitants of that Member State. 66. Moreover, even if Article 4 of the Directive is based on a single concept of controller as regards its substantive provisions, I think that for the purposes of deciding on the preliminary issue of territorial applicability, an economic operator must be considered as a single unit, and thus, at this stage of analysis, not be dissected on the basis of its individual activities relating to processing of personal data or different groups of data subjects to which its activities relate. 67. In conclusion, processing of personal data takes place within the context of a controller's establishment if that establishment acts as the bridge for the referencing service to the advertising market of that Member State, even if the technical data processing operations are situated in other Member States or third countries."

[153] ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja González, Recital 55.

Thus, the DPD will be applicable if data processing is carried out in the context of the activities of an establishment in a broad sense. Every instance of processing would then be covered, including the transfer of data to a non-EU country. The directive will be applied, for instance, if a cloud provider processes the data on a server within a member state. If the provider is processing data using a machine physically in a certain member state, this state's law is applicable as long as the provider does not have an establishment in another EU member state. However, according to the ECJ decision "Google Spain," it is already sufficient for the application of the directive that there is an establishment of the cloud provider in the EU that fosters the activities of the cloud provider. It is not necessary that this establishment is directly involved in processing the data or has any particular responsibility concerning the processing; it is sufficient that the establishment supports the activities of the cloud provider from an economic perspective, for instance, in the Google Spain case the selling of an advertisement. Hence, it is sufficient that an establishment operates the monetary relationships for the cloud provider, etc., in order to apply the DPD.

Given the narrow scope of applicability of the DPD before the ECJ handed down the decision in the Google Spain case, it is understandable that the EC tried to extend the applicability in the proposal of the GDPR. The territorial scope of the regulation is specified in Art. 3, Para. 1 – 3,[154] according to which many data processing operations by providers of services outside the EU would fall into the scope of the European data protection law. The (proposed) Recitals 19 and 20 highlight these intentions.[155] The concept of services is governed by Art. 57 of the

[154] Article 3: 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of such data subjects.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

[155] Cf. LIBE proposal, available at http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf: "(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. (20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to

TFEU (freedom to provide services) or by Art. 4, No. 1 of the Services Directive 2006/123/EC.[156] Services are all activities covered under Art. 57 of the TFEU, which are normally provided for remuneration, insofar as they are not subject to the rules on free movement of goods, capital and on the free movement of the person. By making it clear in the definition of the regulation that the service does not have to be paid for, both commercial and noncommercial websites are covered. The definition of goods is governed by Art. 28, Para. 2, of the TFEU. Regardless of the nature of the transactions, this is a set of objects which can, in respect of commercial transactions, be brought across a boundary.[157] These goods do not need to be physical, but do need to have a market value.

If the behavior of a person is monitored, according to Recital 21,[158] Art. 3, Para. 2 (b) of the DPD applies. An example is when Internet activities are tracked by means of data processing techniques which assign a person to a profile. Tracking tools which operate by the use of cookies,[159] for example, for targeted advertising,[160] are particularly affected. Due to the altered wording of "monitoring" in Art. 3, Para. 2 (b), a selective observation is not covered. The regulation applies to the processing of personal data by a controller not established in the EU, but in a place where the national law of a member state applies by virtue of public international law according to Art. 3 Para. 3. Pursuant to Recital 22, this affects places such as diplomatic or consular missions.[161]

---

the offering of goods or services, irrespective of whether connected to a payment or not, to such data subjects, or to the monitoring of such data subjects. In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects residing in one or more Member States in the Union."

156 *Wieczorek*, DuD 2013, 644 (647); *Klar*, ZD 2013, 109 (113); Treaty on the Functioning of the European Union, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN; Directive 2006/123/EC of the European Parliament and of the Council of 12/12/2006 on services in the internal market, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0123&from=EN.

157 ECJ, decision of 09/07/1992 – C-2/90 – European Commission/Kingdom of Belgium (Walloon Waste), Recital 26.

158 Recital 21: In order to determine whether a processing activity can be considered to 'monitor' data subjects, it should be ascertained whether individuals are tracked, regardless of the origins of the data, or if other data about them is collected, including from public registers and announcements in the EU that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of data processing techniques which consist of applying a 'profile,' particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes.

159 *Art. 29 Working Party*, Opinion 04/2012, WP 194, 1 ff.

160 *Peifer*, K&R 2011, 543 (543 ff.); *Rammos*, K&R 2011, 692 (692 ff.); *Klar*, ZD 2013, 109 (113).

161 *Art. 29 Working Part*, Opinion 08/2010, WP 179, 22 ff.; *Wieczorek*, DuD 2013, 644 (648).

Hence, the former territorial principle of Art. 4 of the DPD 95/46/EG shall be abandoned in favor of a more market- and user-orientated model.[162] This very broad territorial scope of the proposal might cause a strong protection of European citizens' rights, since the offerer of services or goods is bound to European data protection law, irrespective of where they are established. The person affected might assert their rights more easily because of the GDPR's broad claim of applicability.[163] They no longer have to worry about the location of the processors' servers.[164] However, this approach might go way beyond what could be considered realistically enforceable. A researcher established outside the EU, for instance, could monitor – among others – EU citizens' internet activities (even if their website is not even supposed to target EU citizens) and therefore be governed by European data protection law without even being aware of it.[165] Moreover, it is not probable that the EU could enforce data protection standards to providers based outside of or without having business in the EU. European supervisory authorities are not able to act outside the EU.[166] So far, there is no solution to this problem.[167] Although Art. 25 of the GDPR states that a controller outside the EU affected by its data protection law shall designate a representative in the EU, there are no possibilities for sanctions or measures against such controllers in the GDPR.[168]

IV. Definitions of consumer and data

Neither the European DPD (and, respectively, the proposed GDPR) nor the BDSG are based upon the notion of the "consumer." By contrast, it is crucial for applying data protection provisions to check whether personal data is affected. In other terms, even entrepreneurs may benefit from data protection according to the European DPD (and German law). Hence, the notion of personal data is essential. Information that is not, or ceases to be, *"personal data"* may be processed without being affected by data protection law requirements.

---

[162] *Härting*, BB 2012, 459 (462); *Piltz*, Datenschutzreform: aktueller Stand der Verhandlungen im Rat, 20/01/2014.

[163] *Roßnagel/Richter/Nebel*, ZD 2013, 103 (104).

[164] Nebel/Richter, ZD 2012, 407 (410).

[165] *Spindler*, GRUR 2013, 996 (1003); *Spindler*, GRUR-Beilage 2014, 101 (107).

[166] Art. 51 GDPR only states: "1. Each supervisory authority shall be competent to perform the duties and to exercise the powers conferred on it in accordance with this regulation on the territory of its own Member State […]."

[167] *Hornung/Sädtler*, CR 2012, 638 (640).

[168] *Leutheusser-Schnarrenberger,* MMR 2012, 709 (710).

1. Personal data under the Data Protection Directive

a. Definition of personal data

The directive protects only the personal data of individuals; corporate entities are excluded from the scope of the directive. According to Art. 2 (a) of the DPD, "personal data" shall mean any information relating to an *identified* or *identifiable* person ("data subject");[169] an identifiable person is one who can be identified, directly or indirectly, in particular by referencing an identification number, or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity. "Personal data" is any information relating to an identified or identifiable person, regardless of which aspects of the person the information may affect. Some examples are privacy issues, such as the private or job-related area, characteristics, skills of an employee, psychological characteristics, or elements of someone's biography.[170] It depends on the circumstances of each individual case if information can be qualified as "personal data." A common family name, for instance, may not single someone out within a country, but probably identifies a student in a classroom. Moreover, if the data processing controller is able to combine information with other data in order to identify individuals, then the information that was originally considered "personal data" may change. In addition, the European DPD (and the German law), as well as the proposed GDPR, distinguish between "normal" and sensitive personal data.[171]

b. Anonymized, pseudonymized and encrypted data

The notion and definition of "*personal data*" is crucial with respect to *anonymized*, *pseudonymized* and *encrypted* data. If these are not qualified as personal data, encryption, anonymization and pseudonymization are means to process data in a legally correct way, in particular in the cloud. Recital 26 of the directive renders the no-

---

[169] *Kokott/Sobotta,* International Data Privacy Law 2013, 222 (223); ECJ, C-92/09, C-93/09, ECR (2010) I-11063 – Volker und Markus Schecke GbR; Hartmut Eifert/Land Hessen, Recitals 52, 53 and 87.

[170] *Dammann*, in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 2, p. 109.

[171] See Art. 8 (1) of the European DPD (Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life); only in case of explicit consent (Art. 8 (2) DPD) or in some exclusively listed cases such as processing data for medical purposes etc. these data may be processed. The proposed GDPR (LIBE) maintains this approach in Art. 9 (1) (The processing of personal data, revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, and the processing of genetic or biometric data or data concerning health or sex life, administrative sanctions, judgments, criminal or suspected offences, convictions, or related security measures shall be prohibited); the cases of legitimate processing are listed exhaustively in Art. 9 (2) GDPR.

tion of "personal data" more precisely.[172] Thus, leaving aside apparently "*nonpersonal*" information, Recital 26 of the DPD recognizes explicitly that information constituting "*personal data*" may be rendered "*anonymous*." Therefore, the data can be used freely by data controller/operators, such as cloud computing operators, if it is being anonymized. Moreover, the transmission of data may fall outside of the scope of the DPD if the data is no longer qualified as personal data; otherwise, the data subject's consent or a specific legal justification are needed.

c. Absolute and relative approach to the identifiablity of persons

However, Recital 26 of the DPD is prone to various interpretations.[173] The criteria concerning the *identifiability* of persons required by Art. 2 (a) of the DPD are still debated, in particular if a so-called *absolute* or *relative approach* has to be the basis for assessing a controller's abilities to identify a person. (1) The so-called "absolute approach" assumes personal data already if there is any chance of the data controller identifying the data subject individually. Thus, all ways and means for a data controller, without any regard to expenses, etc., are taken into account. Even theoretical chances of combining data so that the individual is identifiable are included. If identifiability is assessed *absolutely*, then it is sufficient for the application of personal data acts if *anyone* in the world is able to decrypt or decode the encrypted data.[174] In the case of cloud computing, for instance, as long as anyone in the world is able to decrypt the data set, the operations of the cloud computing provider are subject to data protection legislation, even if the cloud computing provider does not possess the key for decryption. Based on this approach, data protection legislation is applicable regardless of the encryption technique applied, as long as one entity holds the key for decoding. (2) By contrast, the "relative approach" considers the necessary effort for the data controller as relevant in order to identify the data subject.[175] Therefore, only realistic chances of

---

[172] Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.

[173] *Hon/Millard/Walden*, The Problem of "Personal Data" in Cloud Computing – What Information is Regulated?, The Cloud of Unknowing, Part 1, p. 13.

[174] *Art. 29 Working Party,* Opinion 04/2007, 7; OLG Hamburg, MMR 2008, 687 (688); *Pahlen-Brandt*, DuD 2008, 34 (38).

[175] *Dammann* in: Simitis, BDSG, Para. 3, Recital 32; *Gola/Schomerus*, Bundesdatenschutzgesetz, Para. 3, Recital 10; *Spindler*, expertise for the 69th German Jurists Forum in Munich 2012 – Gutachten für die Verhandlungen des 69. Deutschen Juristentages in München 2012 [DJT 2012], Band I, Gutachten, p. F 115, 116; *Schulz* in: Beck`scher Kommentar zum Recht der Telemediendienste, Para. 11 TMG, Recital 24; *Roßnagel/Scholz*, MMR 2000, 721 (723); *Meyerdierks*, MMR 2009, 8 (8

combining data in order to identify an individual are taken into account. With regard to encryption issues, data protection legislation is only applicable if the data controller is able to decrypt a certain data set[176] – or, at least, has a reasonable chance of obtaining the decrypting key.

Despite its enormous practical impact, this aspect has not yet been clarified either by the ECJ[177] or the EC – even though the relative approach seems to be favored in the case law of some courts.[178] On the contrary, some national supervisory authorities (e.g. the *Düsseldorfer Kreis*) support the absolute approach,[179] as well as some other authors.[180] Singular indications of a relative approach can be found in the legislation of some EU member states (in particular, Great Britain and Austria). The British Data Protection Act of 1998 focuses expressly in Part I, 1 on information that is – or is likely to come – into the possession *of the data controller* in order to assess the identifiability,[181] stating that: "'personal data' means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual." This definition clearly differs from the formulations provided in Art. 2 (a) of the DPD and Recital 26 of the DPD by taking (expressly) only the perspective of the controller.[182] One may note this instance while assessing British court decisions. However, it seems most EU member states have not implemented the DPD requirements in the same way by focusing expressly on the controller's perspective.[183] Therefore, a general

ff.); *Eckhardt,* K&R 2007, 601 (603); *Voigt*, MMR 2009, 377 (377); *Hon/Millard/Walden*, The Problem of "Personal Data" In Cloud Computing – What Information is Regulated?, The Cloud of Unknowing, Part 1, p. 46.

176 *Spindler*, expertise for the 69th German Jurists Forum in Munich 2012 – Gutachten für die Verhandlungen des 69. Deutschen Juristentages in München 2012 [DJT 2012], Band I, Gutachten, p. F 115, 116.

177 *Kühling/Klar*, NJW 2013, 3611 (3614).

178 England and Wales High Court (Administrative Court), [2011] EWHC 1430 (Admin), Case No. CO/12544/2009, Recital 51 f.; Upper Tribunal (Administrative Appeals Chamber), [2011] UKUT 153 (AAC), Appeal Number: GI/150/2011, GI/151/2011, GI/152/2011, Recital 128; House of Lords, [2008] UKHL 47*, Recital 27; AG München*, ZUM-RD 2009, 413 (414) = BeckRS 2008, 23037; *OLG Hamburg*, MMR 2011, 281; *LG Wuppertal*, MMR 2011, 65 (66); *LG Berlin*, CR 2013, 471; different point of view *AG Berlin-Mitte*, ZUM 2008, 83 = K&R 2007, 600 (601); *VG Wiesbaden*, MMR 2009, 428 (432).

179 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.pdf?__blob=publicationFile.

180 *Kuner*, European Data Protection Law, p. 92; *Marnau/Schlehahn*, Cloud-Computing: Legal Analysis, TClouds (D 1.2.2), p. 26 f.; *Pahlen-Brandt*, DuD 2008, 34 ff.

181 Cf. *Kuner*, European Data Protection Law, p. 95 f.

182 Cf. *Hon/Millard/Walden*, The Problem of "Personal Data" In Cloud Computing – What Information is Regulated?, The Cloud of Unknowing, Part 1, p. 19, Recital 97.

183 Cf. List of provision formulations in *Kuner*, European Data Protection Law, p. 95 f.

stance of national legislators in the EU that are in favor of a relative approach to interpret the term "personal data" within the DPD cannot be derived from those single provisions. A remarkable gradation was stated in the Austrian data protection law in Para. 4, No. 1 of the DSG 2000.[184] The Austrian law combines the relative and a rather absolute approach. With respect to the provision cited, data generally has to be rendered "personal" if the controller or any other person is capable of identifying the data subject (which indicates an absolute understanding).[185] However, whenever the controllers themselves cannot identify the data subject by using lawful and reasonable means, all processing actions carried out *by them* are privileged in many provisions.[186] This special category is called "indirectly personal" data by Austrian law. Nevertheless, it should be stressed that the DPD does not provide such a sub-category within the category of personal data; there is no differentiation between data that allow a direct identification of the data subject and data which do so indirectly. Both cases expressly constitute (one category of) personal data (see Art. 2 (a) DPD).[187]

However, in October 2014, the German Federal Court of Justice (BGH) requested a preliminary ruling from the ECJ in accordance with Art. 267 of the TFEU on the interpretation of the dispute whether a dynamic IP address can be considered as personal data.[188] Thus, the ECJ will have to decide the dispute between an absolute and relative approach regarding IP addresses and will have to interpret Art. 2 (a) of the DPD;[189] its decision will certainly have a major influence on the handling of data on the internet.[190]

Article 29 of the Data Protection Working Party[191] has also described its stance concerning Art. 2 (a) of the DPD.[192] Its opinion is interpreted by some

---

[184] Austrian Data Protection Act from 2000, BGBl. I Nr. 165/1999, last amendment 23/05/2013, BGBl. I Nr. 165/1999, English version available at https://www.dsb.gv.at/DocView.axd?CobId=41936. "Data" ("Personal Data") ["Daten" ("*personenbezogene Daten*")]: Information relating to data subjects (Subpara. 3) who are identified or identifiable; Data are "only indirectly personal" for a controller (Subpara. 4), a processor (Subpara. 5) or recipient of a transmission (Subpara. 12) when the data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means.

[185] *Pollirer/Weiss/Knyrim*, Datenschutzgesetz 2000, Para. 4, Recital relating to Z 1, p. 20.

[186] *Pollirer/Weiss/Knyrim*, Datenschutzgesetz 2000, Para. 4, Recital relating to Z 1, p. 20f.

[187] Cf. *Bergauer*, Jahrbuch Datenschutzrecht 2011, 55 (60).

[188] German Federal Court of Justice (BGH), decision of 28/10/2014 - VI ZR 135/13 = MMR 2015, 131.

[189] German Federal Court of Justice (BGH), decision of 28/10/2014 - VI ZR 135/13 = MMR 2015, 131 (132 f.), Recitals 27, 29 ff.

[190] *Bär*, MMR 2015, 134 (135 f.).

[191] Http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

[192] *Art. 29 Working Party*, Opinion 04/2007, WP 136, 21: "Anonymous data" in the sense of the Directive can be defined as any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely to be used either by the controller or by any other person to identify that indi-

authors as being cryptic, as the Working Party used indirectly similar notions for other cases (mentioned in the opinion) which are pointing more to the relative approach.[193] Others argue that the opinion includes a rather absolute stance.[194] It should be noted that the Working Group takes into consideration the means potentially used by the controller to identify the data subject rather than the means that might be used by third parties.[195] However, the Working Party apparently recognizes situations in which a set of data has to be regarded as *personal* data with respect to one entity, but not with respect to another one,[196] which, in turn, implies a relative approach. The reason for this seeming contradiction is that the Working Party puts emphasis on the circumstances of the particular situation of the processing action, rather than on the personal perspective (*whose* capacities have to be considered – only the ones of the controller or of any other person in the world?). Hence, the assessment of the data has to take into account means of identification that can be used by the controller or any other third party,[197] on the one hand, but, on the other hand, is limited to those means that are likely to be used *in the concrete situation*. Purely theoretical chances of identification are insufficient to constitute the personal characteristic of the data.[198]

As the absolute approach extends the scope of DPD to nearly all kinds of data processing,[199] the stronger arguments speak in favor of the relative approach.[200]

vidual. "Anonymized data" would, therefore, be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible. Recital 26 also refers to this concept when it reads that 'the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'. Again, the assessment of whether the data allows identification of an individual, and whether the information can be considered as anonymous or not depends on the circumstances, and a case-by-case analysis should be carried out with particular reference to the extent that the means are likely to be used for identification as described in Recital 26. This is particularly relevant in the case of statistical information, where despite the fact that the information may be presented as aggregated data, the original sample is not sufficiently large and other pieces of information may enable the identification of individuals; see also *Leonard*, International Data Privacy Law, 2014, 53.

193 Cf. criticism of *Kühling/Klar*, NJW 2013, 3611 (3614); *Pahlen-Brandt*, DuD 2008, 34 f.

194 Cf. *Eckhardt*, CR 2011, 339 (341, 343); *Stimerling/Hartung*, CR 2012, 60 (63).

195 *Art. 29 Working Party*, Opinion 04/2007, WP 136, 18 f.

196 *Art. 29 Working Party*, Opinion 04/2007, WP 136, 15 f.

197 Cf. also *Bygrave*, Data Privacy Law, p. 132.

198 *Art. 29 Working Party*, Opinion 04/2007, WP 136, 15.

199 *Meyerdierks*, MMR 2009, 8 (10); *Peifer,* K&R 2011, 543 (544); *Spindler*, expertise for the 69th German Jurists Forum in Munich 2012 – Gutachten für die Verhandlungen des 69. Deutschen Juristentages in München 2012 [DJT 2012], Band I, Gutachten, p. F 115.

200 *Dammann* in: Simitis*,* BDSG, Para. 3, Recital 32; *Gola/Schomerus*, Bundesdatenschutzgesetz, Para. 3, Recital 10; *Spindler*, expertise for the 69th German Jurists Forum in Munich 2012 – Gutachten für die Verhandlungen des 69. Deutschen Juristentages in München 2012 [DJT 2012], Band I, Gutachten, p. F 115, 116; *Schulz* in: Beck`scher Kommentar zum Recht der Telemediendienste, Para. 11 TMG, Recital 24; *Roßnagel/Scholz,* MMR 2000, 721 (723); *Meyerdierks*, MMR 2009, 8 (8 ff.); *Eckhardt,* K&R 2007, 601 (603); *Voigt*, MMR 2009, 377; *Hon/Millard/Walden*, The Problem of "Personal Data" in Cloud Computing – What Information is Regulated?, The Cloud of Unknowing, Part 1, p. 46.

Based on the absolute approach, data controllers (or data processors) cannot really assess if the DPD is applicable, since the DPD would be extended to an omnipresent law without any real boundaries.[201] Furthermore, it should be considered that the purpose of the directive is particularly the protection of the right to privacy of natural persons (see Art. 2, No. 1, DPD). In scenarios where no realistic ("reasonable") chances to identify the data subject exist, with respect to the concrete situation of the processing actions, this purpose is not affected at all. Therefore, it does not seem necessary to apply restricting data protection under those circumstances.[202]

However, even on the grounds of the relative approach, re-combinability of "harmless data" and creating profiles out of these data (Big Data) do fall under the scope of the DPD.[203] Even if the data has not been personal at the beginning of data processing, we have to keep in mind that every data processor has to check if the data they have used is already "personal data" or not.[204] Data which are related to things ("Internet of Things") can also turn out to be personal data if the data can be brought with reasonable effort[205] into a direct relationship with a person.[206] As mentioned before, pseudonymization and anonymization may turn personal data into non-identifiable data, so that this data would fall out of the scope of the DPD (as well as German law) after an anonymization procedure. Section 15 of the German Telemedia Act refers explicitly to pseudonymization in order to enable marketing activities for website operators. However, these means also depend upon the capacities and technical means of data processors. If data processors are able to recombine anonymized data in such a way that the data is again related to a person, this data must again be considered as personal data. In particular, means of profiling and collecting data of persons visiting websites may be treated as personal data if the operator is able to identify the user, for instance, using Google Analytics.

As the previous paragraphs have illustrated, the technical requirements of data protection laws concerning cloud computing and encryption – in particular, the

---

[201] *Meyerdierks*, MMR 2009, 8 (10).

[202] Cf. *Eckhard*, CR 2011, 339 (342); *Härting*, ITRB 2009, 35 (37); *Maisch*, ITRB 2011, 13 (14).

[203] Proposal for a Regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD) of 25/01/2012, Recital 24: online identifiers combined with other information, available at http://www.ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_eu.pdf.

[204] *Spindler*, expertise for the 69th German Jurists Forum in Munich 2012 – Gutachten für die Verhandlungen des 69. Deutschen Juristentages in München 2012 [DJT 2012], Band I, Gutachten, p. F 116.

[205] *Gerlach*, CR 2013, 478 (479); *Spindler*, expertise for the 69th German Jurists Forum in Munich 2012 – Gutachten für die Verhandlungen des 69. Deutschen Juristentages in München 2012 [DJT 2012], Band I, Gutachten, p. F 121; *Gola/Schomerus*, Bundesdatenschutzgesetz, Para. 3, Recital 10.

[206] *Art. 29 Working Party,* Opinion 04/2007, WP 136, 19 ff.

standards – are still not fully settled. In a nutshell, encryption technologies must sophisticated enough that efforts to attribute information to persons (to decrypt) are regarded as unreasonable based upon the expenses required, such as time and labor. According to the relative approach, the perspective of the data processor is relevant in order to assess the (un)reasonable efforts to decrypt the data – it does not take an objective point of view and assess whether anyone in the world would be able to decrypt it.

2. Personal data under the General Data Protection Regulation

The definition of personal data under the GDPR would extend from the Directive 95/46/EG.[207] Article 4, Para. 2 now includes data with which an indirect link can be made to a person.[208] Two new definitions have been added with the LIBE proposal: The GDPR will provide precise definitions of "pseudonymous data" and "encrypted data" in Art. 4, Para. 2a[209] and 2b.[210] Unfortunately, the definition of "encrypted data" does not exclude encrypted data from the applicability of the GDPR in general, since the definition concerns "personal data" that has been altered to be unidentifiable. The direct effect encryption of data takes from a legal perspective, as intended by the GDPR, is relatively small. If data has been encrypted, the controller is not required to communicate a data breach to the data subject, according to Art. 32, Para. 3 of the GDPR. The notification requirements in Art. 13 and 13a of the GDPR provide for an indication of whether or not the data processed will be encrypted (but are no longer included in the proposal of the Council). An indirect effect (not explicitly mentioned in the GDPR) that encryption might have on the processing of personal data could be a strengthening of the legitimate interests pursued by the controller during the balancing of interests required for an explicit legal permission to process data according to Art. 6 of the GDPR. The fact that there are regulations concerning encrypted data within the GDPR could be interpreted to mean that encryption does not prevent the applicability of the European data protection law. If encrypted data does not fall under

[207] The current definition of personal data in Art. 2a of the Directive 95/46/EC is available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[208] Article 4, Para. (2): "'Data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;" see *Härting*, CR 2013, 715 (717).

[209] "Pseudonymous data" means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution.

[210] "Encrypted data" means personal data which, through technological protection measures, is rendered unintelligible to any person who is not authorized to access it. The definition is no longer included in the proposal of the Council.

the scope of the GDPR, regulations concerning encrypted data within the GDRP would make no sense at all. This interpretation would support an absolute approach. However, it does not take into account that the qualification of data as personal or nonpersonal depends on the respective controllers' perspectives.

According to this approach (the relative approach), for the party able to decrypt the data, it still has to be considered personal data; whereas, for the party not able to decrypt it, the data should be considered anonymous. Under this approach, the regulations within the GDPR that concern encrypted data are interpreted only as setting rules for the controller that is able to decrypt the data and how they should process it, but the regulations do not mean that encrypted data always has to be considered personal data for every party. The GDPR's acknowledgment of encryption technologies and the benefit granted by Art. 32, Para. 3 to the controller who encrypts data might offer an incentive to controllers to encrypt the data of persons affected before processing it, but it does not answer the question of whether or not the encrypted data is considered personal data for a party that is unable to decrypt it. This still depends on the approach taken to define "identifiability" (see the following). However, the proposal seems to assume that the processing of encrypted data is less dangerous for the privacy of the persons affected than the processing of unencrypted data (because the controller does not have to report a data breach to the data subject if the data was encrypted).

The GDPR will not be applicable to anonymous data. Recital 23, sentences 4 and 5 clarify that the data protection legislation does not apply to anonymous data.[211] Moreover, the anonymity is also mentioned in the context of health data in Art. 81 (in the version of the LIBE proposal, but not contained in the version of the Council), so that they are not covered by the privacy regulation. Hence, an exact definition of when data becomes anonymized is not provided by the regulation, but described by Recital 23. Unfortunately, this "definition" does not resolve the dispute mentioned between the different approaches (relative vs. absolute) to define *anonymization*. Therefore, the same problems persist, such as new techniques to decrypt or to identify data subjects by combining different pieces of information.[212] Techniques such as removing or scrambling direct identifiers – or even indirect identifiers, apparently – cannot anonymize the data virtually irreversibly.[213] With an absolute approach, almost all data has to be considered "personal data."

---

[211] Recital 23: "[…] The principles of data protection should, therefore, not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes." See *Härting*, CR 2013, 715 (718).

[212] *Hon/Millard/Walden*, The Problem of "Personal Data" in Cloud Computing – What Information is Regulated?, The Cloud of Unknowing, Part 1, p. 22.

[213] *Hon/Millard/Walden*, The Problem of "Personal Data" in Cloud Computing – What Information is Regulated?, The Cloud of Unknowing, Part 1, p. 22.

It has been stated that, according to the GPDR's definition of "personal data," it is no longer important whether information relates only to a pseudonym which does not allow any conclusions about the real name[214] – which would greatly extend the scope of the regulation on the European level.[215] On the other hand, it can be argued that it has to be taken into account if the link between the person affected and the data can be made only with an extreme effort. This, too, is based on Recital 23 of the GDPR.[216] Hence, with a relative approach, it can still be pointed out that the recital might take into account the means used by the respective controller and a third person – but only if those means are *reasonably likely to be used*.[217] If a decryption of the data is not reasonably likely to happen, the data could be considered nonpersonal (i.e. anonymous data) because the person affected would not be identifiable. The LIBE version of the proposal has been provided with an explanation, written by *Jan Albrecht*, a draftsperson and Member of the EU Parliament. It allows insight into the motives behind, at least, the LIBE version of the GDPR. it is stated In this explanation that the GDPR's purpose is to protect the fundamental rights of the persons affected. With that in mind, a limitation of the "personal data" definition's scope is rejected.[218] All objective factors should be taken into account when determining if data is "personal data," according to the explanation. This seems to be clearly a vote for an absolute approach, although it can be criticized for the same reasons described above. Moreover, Recital 24 of the LIBE proposal is another hint for the absolute approach of the proposal, whereas the same recital (24) can be read in the Council's proposal as a relative approach of this proposal: "Identification numbers, location data, online identifiers or other specific factors as such should not be considered as personal data *if they do not identify an individual or make an individual identifiable*." Nevertheless, this also leaves room for interpretations and, as the discussions are still

214 Specifying the problem of information relating to a pseudonym: *Härting*, Internetrecht, Recital 185 ff.

215 However, note that this extension depends on the former practice in member states. Germany has already used a wider notion of personal data, even according to the so-called "relative approach," see 2.2.1.

216 Recital 23: "[…] To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly." The proposal of the Council and the LIBE proposal furthermore add: "To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development."

217 Lang, K&R 2012, 145 (146).

218 *Albrecht*, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 0011-C7-0025/2012-2012/0011 (COD) of 16/01/2013, 212, available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/924/924343/924343en.pdf.

going on, one now has to wait for the exact wording of the final version of the GDPR and for the decision of the ECJ regarding this issue mentioned above.

V. Basic concepts

Both the European DPD and the proposed GDPR, as well as the BDSG, are characterized by certain fundamental principles of data protection. The objective of the directive is to protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data, and to guarantee the free flow of personal data between member states.[219] The directive regulates the processing of personal data regardless of whether such processing is automatic or not.[220] Article 3 (2) refers to some exceptions.[221] One of the latter relevant for internet services (and users) refers to exclusive personal and familiar activities, which are exempted. All activities on social networks (user-generated content), for instance, remain in the private sphere and are not affected by the DPD. However, this exception does not affect the obligations of the operator of a social network, it relates only to the responsibility of those individuals who are processing data of third parties on their social network websites Finally, the ECJ clarified that processing for public safety and prosecution purposes is not part of the scope of this DPD.[222] In the same way, the BDSG is applicable only to the processing of personal data; private and familiar activities are out of its scope.

The DPD defines the "processing of data" as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organizing, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying.[223] The extremely broad definition of "processing" leads to the broad applicability of the DPD and, thus, to the general prohibition of processing the data unless the DPD allows for it. From the moment the data is collected to the very last use of that data, every single step in between has to be either explicitly allowed by law or needs the data subject's consent. Thus, data controllers can only avoid the applicability of the

---

[219] Article 1: Object of the directive. (1) In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data. (2) Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

[220] Whereas the directive applies in general for all kinds of processing data there are still some differences made by the directive. In case of non-automatic processing the directive addresses only data processing stored in a (physical) dossier.

[221] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 3, Recital 16.

[222] ECJ, decision of 30/05/2006 – C-317/04, C-318/04, ECR (2006), p. I-4721 – European Parliament/Council of the European Union and European Commission, Recital 59.

[223] Art. 2 (b).

DPD by making the data "not personal." Otherwise, they can comply with the requirements, asking the user for explicit consent or bring forward reasons that fall under the justifications provided by the DPD. If personal data is anonymized, this might technically mean that it gets altered, but for the purposes of the DPD, "alteration" means changing the information's content, not its appearance.[224]

Processing of personal data is generally prohibited unless the processor benefits from consent of the individual, or benefits from justifications provided by data protection acts (or other specific acts). Moreover, the main principle is that personal data should not be processed, unless the data processing operator complies with certain requirements. These basic structures, which also apply for the BDSG, refer to transparency,[225] legitimate purpose[226] and proportionality. According to the proportionality principle, personal data may only be processed if the processing is "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[227] This processing has to be carried out "fairly and lawfully." Furthermore, the data collected must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified." Moreover, the directive demands the controller to "keep [the data] in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use," as stated in Art. 6 (1e). Finally, the directive tightens the requirements for specific sensitive personal data regarding "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and […] data concerning health or sex life." The processing of this kind of data may only be justified if the requirements stated in Art. 8 (2) are fulfilled, such as a specific consent or protecting the vital interests of the data subject.

The proposed GDPR does not abandon this basic approach of the DPD and continues these main principles. The principle of prohibition with a reservation of

---

[224] See also *Gola/Schomerus*, BDSG, Para. 3, Recitals 30, 31.

[225] The individual has the right to be informed should his personal data be processed. Before starting the processing the controller has to provide information about his identity (name and address), the purpose of processing, the recipient of the data and, if necessary, further information to guarantee fair processing in respect of the data subject. Personal Data can be processed only if the controller complies with the requirements stated in Art. 7 and 12. Thus, an explicit consent of the data subject is indispensable for the performance of contractual obligations or the entering into a contract.

[226] Personal data shall only be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes," Art. 6 (b).

[227] See Art. 6.

authorization in the data protection law is not loosened in the proposal;[228] in fact, it has been tightened in Art. 6 of the GDPR.[229] The processing of personal data shall be, as regulated in the DPD, lawful only if the data subject has given consent in accordance with Art. 7 of the GDPR to the processing of their personal data or if after a consideration the processing is necessary for legal purposes. The permissions contained in Art. 6 of the GDPR are kept extremely general and unspecific[230] which, as a consequence, leads to the increased importance of consent.[231] Moreover, in accordance with Art. 4 (8) of the GDPR, the consent must be an explicit declaration of intention. However, the Council removed the word "explicit" from the definition in its proposal and reestablished the possibility of giving implied consent, which may be used for nonsensitive data processing. Furthermore, the LIBE proposal and the Council's proposal do not provide for the invalidity of consent in case of a significant imbalance between the position of the data subject and the controller.[232] Article 7 (3) of the GDPR assigns to the individual the right to withdraw the consent at any time. The scope of the proposal for the GDPR is, as well as in the DPD, defined by the processing of personal data (Art. 2 (1) in conjunction with Art. 4 (2), Art. 1 of the GDPR). The LIBE proposal of Art. 4 (2) of the GDPR provides for a broad definition of personal data, hence, each piece of information that can be individualized shall be personal data.[233] Moreover, the applicability is, according to Art. 2 (2) lit. d of the GDPR, still generally restricted to the processing of personal data outside the private sphere. Thus, the regulation "does not apply to the processing of personal data by a natural person in the course of an exclusively personal or household activity," which implies that the actual cohabitation of the persons affected and not their relationship in terms of family law matters.[234] Article 14 (1) of the GDPR provides for an extension of information to the data subjects in comparison to the transparency provisions of Art. 10 and 11 of the DPD.[235] It includes absolute duties to inform the data subject about, e.g. the identity of the data protection officer, the period

[228] *Taeger* in Taeger/Gabel, BDSG, Para. 4a, Recital 4.

[229] *Härting*, CR 2013, 715 (717), who sees in this provision "a pan-European prohibition of communication with a reservation of authorisation."

[230] *Rogall-Grothe*, ZRP 2012, 193 (195); *Roßnagel/Richter/Nebel*, ZD 2013, 103 (104).

[231] *Hullen*, in v. d. Bussche/Voigt, Konzerndatenschutz, Teil 8, Recital 13.

[232] The original provision has been subject to substantial criticism because of its legal uncertainty, c.f. *Hullen*, in v. d. Bussche/Voigt, Konzerndatenschutz, Teil 8, Recital 14; *Härting*, BB 2012, 459 (463); *Roßnagel/Richter/Nebel*, ZD 2013, 103 (104); however, Recital 34 of the proposal of the Council states again that a consent is not freely given "where there is a clear imbalance between the data subject and the controller."

[233] *Härting*, CR 2013, 715 (717 f.); *Hullen*, in v. d. Bussche/Voigt, Konzerndatenschutz, Teil 8, Recital 12.

[234] *Dammann*, in Simitis, BDSG, Para. 1, Recital 243; Moreover, the LIBE proposal expands this exception in sentence 2 of Art. 2 (2) lit. d of the GDPR to "publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons."

[235] *Härting*, Internetrecht, Recital 369.

for which the personal data will be stored, the existence of the right to request from the controller access to and rectification or erasure of the personal data as well as a right to lodge a complaint to the supervisory authority (Art. 14 (1) lit. a, c, d, e GDPR).

VI. Collecting, storing and processing consumer data

In principle, neither the European DPD nor the proposed GDPR refers to the different phases of collecting, storing and processing personal data. All these actions are qualified as "processing" data; each action has to be justified according to the set of rules provided by the DPD (or GDPR). If the data subject's consent is lacking, lawful processing of data is only possible in accordance with one of the legal permissions established under the DPD[236] (or the proposed GDPR)[237] in its exhaustive list of justifications. This list of legal grounds is exhaustive, meaning they are not just examples among other possible legal grounds, but the only lawful reasons to process data without the data subject's consent. They permit processing only when it is necessary for certain purposes and not beyond that, corresponding with the DPD's fundamental principle of proportionality laid down in Art. 6. Whereas lit (b) to (e) are applicable only for specific purposes, lit (f) allows the member states to provide a legal ground with a larger scope. However, processing on the grounds of a permission based on lit (f) always requires a proportionality test. This means a balance has to be found between the data subjects' and the controllers' interests. Only when the controllers' interests in processing the data without consent outweigh the data subjects' interests in having to consent to the

[236] See Art. 7 (b) to (f) DPD: "[…] (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party, or parties, to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject, which require protection under Article 1 (1)."

[237] See Art. 6 GDPR: "[…] (b) processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller, or in case of disclosure by the third party to whom the data is disclosed, and which meet the reasonable expectations of the data subject, based on his or her relationship with the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data. This shall not apply to processing carried out by public authorities in the performance of their tasks."

processing can the processing be carried out lawfully on the grounds of lit (f). It is questionable, though, if financial advantages are sufficient to outweigh the data subject's interest in a comprehensive data protection. This interest is based on a European fundamental right, Art. 7 and 8 of the CFR, and, therefore, is very worthy of protection. The ECJ had to evaluate a similar conflict of interests in a recent decision: A data subject demanded that Google be required to remove personal data and, by this, no longer make a search result concerning the available data subject.[238] They argued that Google could no longer base the processing of the data on the legal grounds of Art. 7 lit (f). The ECJ stressed the strong position of the data subject in such a balance of interests, stating that, in this case, the economic interest of Google would not be sufficient to justify the processing.[239] It was even stated that the rights of the data subject override, as a rule, the economic interests of the operator of the search engine.[240] Therefore, data processing based on the grounds of Art. 7 lit (f) should not only be justified by a financial advantage of the cloud user.

Regarding the permission scheme contained in Art. 6 of the GDPR, it has been criticized that lit (b) only covers contractual claims and does not include statutory claims.[241] Nevertheless, lit (b) includes the "performance of a contract" without a restriction to claims. Moreover, lit (f) covers all legitimate interests, in the case they are not overridden by the data subject's interests. Therefore, data processing in order to enforce a statutory claim might be lawful without consent of the person affected under certain circumstances. Although if the processing is permitted according to lit (f), the data subject is able to object to the processing at any time and, without any further justification, free of charge (Art. 19, Para. 2 GDPR). This broad right to object does not exist if the processing is based on lit (b), which might cause lit (b) to be the more reliable reason for processing.

VII. Approaches to consent

As noted already, consent of an individual plays a dominant role in practice, as most services can only be used if the individual affected gives his/her preliminarily consent to data processing of the service provider, such as Google or Facebook. Hence, the legal requirements for consent are essential.

---

238 ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález.

239 ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Recital 81.

240 ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Recital 97.

241 *Berg,* PinG 2013, 69 (70).

1. Informed consent according to the Data Protection Directive

Some member states see consent as a preferred ground for lawfulness, whereas others see it as equal as the five legal permissions contained in the DPD. However, while these permissions require a necessity test, the data subject's consent allows the data processor to go beyond even what is necessary.[242] In other words, the data processor is not bound by a strict proportionality test under these circumstances.[243] However, as noted already, the DPD treats specific sensitive data in a specific manner, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life. Requirements for this kind of data are stronger than for other personal data. Consent is only effective when it is given freely, informed and unambiguously. Informed consent implies that the data subject has been given certain information before data is processed, including the recipients or categories of recipients of the data (Art. 10 (c) DPD).[244] It also has to be made clear to the data subject when data will be transferred to a non-EU state.[245] In another paper, the Art. 29 Working Group has formulated certain criteria which have to be met in order to speak of freely given consent.[246] The scope of this restriction is still not clear, particularly if it also affects consent given to service providers, such as dominant search engines or social networks. However, there is consensus that the consent should be freely rescindable. Another requirement refers to "specific" consent – hence, a blanket would not be sufficient. The different aspects of data processing have to be made clear at the outset of data processing, particularly regarding which data is processed and for what purposes.[247] Moreover, the consent has to be given on an "informed" basis, such as that provided by Art. 10 and 11 of the DPD. The Art. 29 Working Party stresses quality of information as well as visibility and accessibility of information.[248] Furthermore, consent has to be "unambiguous." According to the Art. 29 Working Party, the notion hinders tacit or implied actions to be qualified as consent, as well as pre-ticked boxes for consent.[249] These requirements of *ex ante* information and transparency can lead to difficulties, particularly for cloud computing: It might be hard to tell when the data will be transferred to a server (to which server?) and in which country this

[242] *Art. 29 Working Party*, Opinion 15/2011, WP 187, 7f.
[243] *Nägele/Jacobs,* ZUM 2010, 281 (290); *Rath/Rothe,* K&R 2013, 623 (624).
[244] *Taeger*, in Taeger/Gabel, BDSG, Para. 4a, Recital 30; *Nord/Manzel*, NJW 2010, 3756 (3757).
[245] *Simitis*, in Simitis, BDSG, Para. 4a, Recitals 70 ff.
[246] *Art. 29 Working Party*, Opinion 15/2011, WP 187, 12: Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free.
[247] *Art. 29 Working Party*, Opinion 15/2011, WP 187, 17.
[248] *Art. 29 Working Party*, Opinion 15/2011, WP 187, 20.
[249] *Art. 29 Working Party*, Opinion 15/2011, WP 187, 24.

server will be operated.[250] Due to the scalability of cloud computing, the method of storage and the "division of labor" amongst the different servers might be "decided" by automated programs and could change within seconds.[251]

2. Informed consent and obligation of transparency under the General Data Protection Regulation

Article 14 of the GDPR extends the approach adopted in the DPD concerning transparency for data subjects (and also goes beyond existing national laws, such as in Germany)[252] by specifying the information required that the data subject must receive prior to the collection of data.[253] These obligations to inform raise a lot of issues, as, in practice, these requirements could be hard to comply with. The variety of data processing procedures and sub-providers for cloud computing, for instance, may render it nearly impossible to provide such information to the data subject. The recipients of the personal data may not be really identified in a cloud in advance, as the storing and processing depends upon the capacities available. The same applies to the transfer of data to a third country, which cannot be easily assessed in advance. If a controller intends to collect data and to use a cloud service to process this data, it will be even more important for them that the data is

[250] *Nägele/Jacobs*, ZUM 2010, 281; *Schultze-Melling*, in Taeger/Gabel, BDSG, Para. 9, Recital 104.
[251] *Millard*, Cloud Computing, Chapter 1.1, 1.2; *Funke/Wittmann,* ZD 2013, 221 (222).
[252] *Jaspers*, DuD 2012, 571 (572).
[253] Art. 14 GDPR: "[…] (b) the purposes of the processing for which the personal data are intended, as well as information regarding the security of the processing of personal data, including the contract terms and general conditions where the processing is based on point (b) of Art. 6 (1) and, where applicable, information on how they implement and meet the requirements of point (f) of Art. 6 (1); (c) the period for which the personal data will be stored or, if this is not possible, the criteria used to determine this period; (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject, to object to the processing of such personal data, or to obtain data: (f) the recipients or categories of recipients of the personal data; (g) where applicable, that the controller intends to transfer the data to a third country or international organization and on the existence or absence of an adequacy decision by the Commission, or in case of transfers referred to in Article 42, Art. 43, or point (h) of Art. 44 (1), reference to the appropriate safeguards and the means to obtain a copy of them; (ga) where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject; (gb) meaningful information about the logic involved in any automated processing; (h) any further information which is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected or processed, in particular the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk; (ha) where applicable, information whether personal data was provided to public authorities during the last consecutive 12-month period." The proposal of the Council changed several of these paragraphs by shifting or deleting them or by introducing new provisions to Art. 14. In addition to this, the proposal of the Council introduced a new Art. 14a to the regulation due to which the controller shall provide the data subject with several pieces of information in the cases where the data have not been obtained from the data subject.

not considered "personal data" under the GDPR. The controller has to provide the information, according to Art. 14 of the GDPR, *before* personal data is collected – which also includes the collection of data based on explicit legal permission, as provided by Art. 6 (1) (b) of the GDPR – (f). The DPD only requires the controller to provide such information to gain *informed* consent. The GDPR, on the other hand, requires that such information is also provided before data is collected, even on the grounds of a legal permission. Whereas the DPD only requires freely given consent, particularly an informed consent, the GDPR demands much more from a controller. Article 4 (8) of the GDPR intensifies the requirements for a valid consent by demanding an "explicit" consent (in contrast to Art. 7 lit. a of the DPD, which considers it to be sufficient if "the data subject has unambiguously given his consent") and, moreover, "a statement or a clear affirmative action." However, as mentioned above, the Council removed the word "explicit" from the definition in its proposal. In accordance with Art. 6 (1) lit. a of the GDPR, processing of personal data shall be legitimated by a consent only if this consent refers to specific and defined purposes. Nevertheless, the proposal of the Council introduced some exceptions to the principle of strict purposes.[254] Additionally, "further processing of personal data for archiving purposes in the public interest or scientific, statistical or historical purposes shall in accordance with Article 83 not be considered incompatible with the initial purposes." Moreover, Art. 7 (3) gives the data subject the right to withdraw their consent at any time without any further requirements and it has to be informed of thereof prior to giving consent. Furthermore, in Art. 8 (1), sentence 1 of the GDPR, "the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent." Sentence 2 states that "the controller shall make reasonable efforts to verify such consent, taking into consideration available technology without causing otherwise unnecessary processing of personal data." Finally, Art. 7 (4) of the LIBE proposal provides the adoption of the principle of a purpose-limited consent and of a ban on tie-ins, instead of a provision which would have meant the invalidity of a consent "where there is a significant imbalance between the position of the data subject and the controller."[255] However, this paragraph has not been included in the Council's proposal.

These obligations to inform are complemented by the new provision in Art. 13a of the regulation, which requires the data controller to provide standardized and easily legible information (which is, in detail, prescribed by the annex of the

[254] E.g. by stating in Art. 6, Para. 4, sentence 2 that: "Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject."

[255] *Nink*, in Spindler/Schuster, Recht der elektronischen Medien, § 4a BDSG, Recital 8; The former provision respective an imbalance has been heavily criticized, see *Hullen*, in v. d. Bussche/Voigt, Konzerndatenschutz, Teil 8, Recital 14; *Roßnagel/Kroschwald*, ZD 2014, 495 (500).

regulation proposed). Concerning the information of Art. 14, the information has to be specified according to the individual circumstances of the data subject; for instance, the national competent supervisory authority or options to file a complaint.

VIII. Publicity and transparency

1. Information

One of the core elements of European data protection refers to the information which must be provided for the data.[256] The controller has to inform the data subject in cases when data is processed which has not been obtained from the data subject.[257] Once again, this obligation aims at providing the necessary information for the data subject in order to enable them to act, for instance, to object to the data processing or to rectify the data. The GDPR proposed pursues this approach and details in Art. 11 and Art. 14. Moreover, Art. 14 (4) specifies the procedure of the information which has to be provided Without going into more detail here, these provisions already shed a light on the sophisticated and very detailed obligations of controllers to provide for information. The GDPR extends the general information obligations to a specific communication to the data subject in the case of a personal data breach (Art. 32) Thus, the GDPR envisages enabling the data subject to file claims against the controller, therefore, providing the utmost transparency for the data subject.

[256] Article 10 DPD requires that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information , except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended ; (c) any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

[257] Thus, Art. 11 (1) requires, in principle, that the controller or his representative must, at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the data subject with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing; (c) any further information such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. Article 11 (2) provides for options for member states to introduce exemptions for these obligations.

2. Notification

As a general principle, Art. 18 of the DPD requires the controller to notify the supervisory authority "before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes."[258] The GDPR carries this approach on and is even extending it to the "personal data breaches" in Art. 31 mentioned already. These have to be reported by the controller to the supervisory authority "without undue delay." Moreover, the processor is obliged, according to Art. 31 (2), to "alert and inform the controller without undue delay after the establishment of a personal data breach." The obligation to report data breaches covers all kinds of personal data. Even unauthorized access to data within the controller's company or agency is considered to be a data breach and, thus, has to be notified to the supervisory authority.[259] Finally, the controller has to document "any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken," in order to enable the supervisory authority "to verify compliance" with Art. 31. The Data Protection Authority must keep a public register of the types of breaches notified. Article 31 refers to all kinds of data breaches, making no difference between third-party attacks (hackers, etc.) and internal access by unauthorized employees. Still unresolved – and implicitly left to member states – is the issue of civil liability for data breaches, particularly if omitted breach notifications may constitute grounds for civil action.

3. Privacy by design and default

One of the main innovations of the proposed regulation refers to the "Privacy by Design" principle, which requires all producers, data controllers, etc., to respect data protection issues whilst developing or implementing new IT systems or products.[260] Thus, any privacy issue shall already be addressed during the devel-

[258] Article 19 specifies the information to be given to the supervisory authority, at least: (a) the name and address of the controller and of his representative, if any; (b) the purpose or purposes of the processing; (c) a description of the category or categories of data subject and of the data or categories of data relating to them; (d) the recipients or categories of recipient to whom the data might be disclosed; (e) proposed transfers of data to third countries; (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

[259] Article 31 (3) details the content of the notification at least: (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (c) recommend measures to mitigate the possible adverse effects of the personal data breach; (d) describe the consequences of the personal data breach; and (e) describe the measures proposed or taken by the controller to address the personal data breach and mitigate its effects.

[260] Article 23 GDPR*; see Decker*, Die neue europäische Datenschutzgrundverordnung – welche Änderungen sind für deutsche Unternehmen zu erwarten?; *Schaar*, Privacy by design; *Krempl*, EU-Datenschützer fordert Einbau von Datenschutz in die Technik.

opment of new technologies. Data Protection by Design must particularly take into account the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding accuracy, confidentiality, integrity, physical security, and deletion of personal data. However, the GDPR obliges the controller and the processor to respect the principle of Privacy by Design, but not the developer of a data processing technology.

4. Privacy seal

According to Art. 39 of the GDPR, the data protection authority can act as a certification authority. Each controller and data processor has the right to apply for a certification procedure, as mentioned in Art. 39 (1).[261] The certification procedure may turn out to be, in practice, one of the most important tools for data controllers to bring evidence required by Art. 26 (1) concerning the selection of processors with sufficient guarantees for data protection, particularly appropriate technical and organizational measures.[262] This might be a partial solution for the dilemma arising from the disparity of power between the cloud computing participants: The cloud provider will be able to request a certification the cloud user is allowed to rely on. However, there is no obligation for certification.[263] Moreover, Art. 39 (1d) provides for third-party certification procedures if the data protection authority has accredited them.[264] A certificate of the processor (issued by an accredited third party) may, thus, be considered as evidence in order to prove the compliance with these obligations. Not only the processor can request a certification; the controller might have an interest in getting certified, too. A cloud user (as the controller) might be able to prove to their clients that they use a cloud service that is compliant with data protection law and that, especially, provides sufficient technical and organizational safeguards.[265] The EC will be empowered to adopt delegated acts to further specify the criteria and requirements for the certification

[261] Article 39 (only in the LIBE proposal): (1a) Any controller or processor may request any supervisory authority in the Union for a reasonable fee, taking into account the administrative costs, to certify that the processing of personal data is performed in compliance with this Regulation - in particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject's rights. (1b) The certification shall be voluntary, affordable, and available via a process that is transparent and not unduly burdensome.

[262] *Brennscheidt*, Cloud Computing und Datenschutz, p. 116

[263] *Härting*, CR 2013, 715 (720).

[264] *Brennscheidt*, Cloud Computing und Datenschutz, p. 116; *Härting*, CR 2013, 715 (720).

[265] However, the Council's proposal straightens out in Art. 39, Para. 2 that: "A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a." Moreover, Art. 26, Para. 2 (aa) states that: "Adherence of the processor to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 *may* be used as an element to demonstrate sufficient guarantees referred to in paragraphs 1 and 2a."

mechanisms, according to Art. 39, Para. 3 of the GDPR; however, the Council proposal does not contain these vast delegations/empowerments. Although the certification of the processor can make it much easier for the controller to bring evidence required by Art. 23 (1), a certificate will expire after five years.[266] Before relying on a certificate, the processor will, therefore, at least be obliged to validate if it is expired or not.[267]

IX. Data security

Regarding data security, both the DPD and the proposed GDPR envisage provisions that make organizational and technical measures mandatory – and which have been respectively implemented in German law (Sec. 9 and 9a BDSG). Under the DPD, appropriate technical and organizational measures have to be provided in order to avoid data leaks, data loss and illegal forms of personal data processing (Art. 17, Para. 1). The core security objectives are availability, confidentiality and integrity; transparency, accountability and portability also have to be taken into account.[268] As the DPD does not specify exactly which measures have to be taken, data controllers are, to some extent (and depending upon the practice of national supervisory authorities), flexible to adopt the appropriate measures. Existing ISO/IEC standards can be adopted and applied by data processing entities to ensure the provision of appropriate technical and organizational measures. They can be used as a general guide for initiating and implementing the IT security management process.[269] Moreover, the IT infrastructure (networks, IT systems, applications) has to be secure, including physical resources, such as buildings and employees.[270] Providing availability of data means ensuring timely and reliable access to personal data. Integrity implies that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission. Thus, for instance, a remote administration of a cloud platform should only take place via a secure communication channel.[271] Article 17 of the DPD states that the measures taken have to protect the personal data against unauthorized disclosure or access. The "state-of-the-art" measures and systems should be considered in order to assess which measures are appropriate.

The GDPR will change the specification of technical and organizational measures. Article 30 of the GDPR regulates the controllers' and processors' duties regarding the detailed measures to be taken. Nevertheless, the core principles set

---

266 It only lasts three years in the Council's proposal, see Art. 39, Para. 4.

267 *Sydow/Kring*, ZD 2014, 271 (275).

268 See also *Art. 29 Working Party*, Opinion 05/2012, WP 196, 14.

269 For a list of ISO standards with further explanation, see *German Federal Office for Information Security Technology,* BSI Standard 100-1 Information Security Management Systems, p. 8.

270 *German Federal Office for Information Security Technology*, Safety Recommendation for Cloud Computing Providers, p. 28 ff.

271 Art. 29 Working Party, Opinion 05/2012, WP 196, 14f.

out in Art. 30 are similar to those developed by the DPD. The GDPR, however, declares them "officially" to be a task of the board of directors. Hence, data protection and data risk management now is one of the core elements of the overall corporate risk management system: It is a "chief's affair."[272] To determine the state of the art, the European Data Protection Board[273] will be entrusted to issue guidelines, recommendations and best practices (Art. 30, Para. 3 GDPR, but not included in the Council's proposal). Encryption of data will still be a very useful tool to accomplish the task of ensuring integrity and confidentiality, set by Art. 30 of the GDPR.[274] As mentioned above, encryption technologies are developed to prevent unauthorized access to data.[275] Hence, it will be necessary to monitor the Data Protection Board's publications and always use encryption that is considered as "state-of-the-art."

X. Data control, data portability and the right to access, modify and delete data collected

Even though the European DPD treats the individual affected as the sovereign of his/her personal data, there are no provisions which refer to data portability. Instead, the DPD concentrates on rights of access to data, particularly to get information about data processed and stored by a controller[276] and to delete data. However, the proposed GDPR envisages changing that situation by introducing an explicit right for data portability.[277] Based upon this article and on Art. 8 of the Charter of Fundamental Rights of the European Union, the ECJ recently strengthened the rights of the individual affected in the Google Spain case (some-

---

[272] The GDPR includes them explicitly; see Art. 30, Para. 1a GDPR: "Having regard for the state-of-the-art and the cost of implementation, such a security policy shall include: (a) the ability to ensure that the integrity of the personal data is validated; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services."

[273] A board composed of the heads of the supervisory authorities of the member states and the European Data Protection Supervisor similar to the Art. 29 Working Party Art. 64 GDPR.

[274] The measures shall at least, protect personal data stored or transmitted against accidental or unlawful destruction, or accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure (Art. 30, Para. 2 lit. b GDPR).

[275] This shall be accomplished by having regard for the state-of-the-art and the costs of their implementation (Art. 30. Para. 1 GDPR).

[276] Art. 12 DPD, entitled "Rights of access," provides that: Member States shall guarantee every data subject the right to obtain from the controller: […] (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.

[277] See Article 18 of the Commission's proposal and of the Council's proposal, which is Art. 15 in the LIBE proposal.

times also called the "right to be forgotten").[278] In particular, the court stated that the interests of the individual generally outweigh the commercial interests of a search engine, even if the information published on the internet had been legally processed (in the relevant case articles published in a journal online, thus, benefitting from the media privilege in the DPD). Only in cases where it is in the general public's interest to have access to information may the individual interests be overwhelmed.[279] Whereas the (heavily-debated) "right to be forgotten and to erase" providers affected seriously by obliging them to ensure that data would also be deleted on third-party caches and servers, the LIBE proposal of the GDPR provides only for a "right to delete" or erasure in Art. 17.[280] Although the term has changed, the original proposal's content continues to exist. Therefore, data controllers should be obliged to provide information about a deletion request of an interested party to third parties to whom data has been passed on. The Council's proposal reintroduced the term "right to be forgotten" in Art. 17. Personal data shall be erased "without undue delay" and the data subject in this proposal only has to object to the processing of personal data,[281] in contrast to the LIBE proposal, which demands a final court judgment before the data has to be erased. However, no data shall be erased in accordance with Para. 3, e.g. when processing of the personal data is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation which requires processing of personal data by EU or member state law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for archiving purposes in the public interest or for scientific, statistical and historical purposes. However, many details remain unresolved: for instance, how to balance the right of the public to be informed by archives and historical information with the right of the individual to have the data deleted.

XI. Roles and responsibilities of intermediaries

The European DPD and the proposed GDPR do not distinguish between different intermediaries, as it used to do, for example, the E-Commerce Directive (distinguishing between access or host provider). The DPD and the GDPR refer in principle to the "controller" of the data processing and the processor who is processing data on behalf of the controller.

---

[278] ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález.

[279] For a more thorough analysis, cf. *Spindler*, JZ 2014, 981 (985 f.).

[280] *Fazlioglu*, International Data Privacy Law, 2013, 149; *Sartor*, International Data Privacy Law 2013, 3 (9); *Krügel*, ZD-Aktuell 2014, 03870; *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107).

[281] And if there are no overriding legitimate grounds for the processing.

1. Controller and processor under the Data Protection Directive

a. The controller

All requirements needed to fulfill compliance with the data protection law have to be ensured by the controller; possible fees and court rulings will apply to them. Article 2 (d) of the DPD defines the controller as a natural or legal person that, alone or jointly with others, is responsible for the processing of data. Hence, a "data controller" determines the purposes and means of the processing. It is not necessary for the controller to process the data; it is sufficient that he/she has control over the procedures. The two important elements included in the definition of the controller need further clarification. Firstly, the controller is the *determining* person making the decisions with respect to the specific data processing action. Secondly, the subjects left to the controller's determination are the *purposes and means* of the processing. Who really "controls" the data processing cannot be determined in general; it depends on the circumstances of the concrete situation and the factual control. The controlling capacity might also derive from an explicit legal competence if one entity is either explicitly appointed as a controller or is entitled with particular data processing duties by legal provisions or through traditional roles, which usually involve certain data responsibilities (e.g. the collection of specific information about employees by the employer). Finally, the factual influence has to be assessed by analyzing the contractual relations between the parties. If the role of the controller is attributed to one party, or one party can be considered dominant relating to data issues altogether, this might be an important indication. However, contractual provisions are not decisive in every case – especially if they do not reflect the factual circumstances. Where doubts exist, the actual control of the parties has to be measured and assessed, taking into consideration the degree of influence actually exercised and the reasonable expectations of the data subjects concerned.[282] The difficulties of how controllership is assessed may be explained by the example of cloud computing: As a lot of entities are involved in the process of storing and using data in the cloud, it is crucial to determine the respective controller who has the actual control. Whereas the cloud user might have clients who are working with his/her data, the cloud provider might have subcontractors, who use his/her resources when their own capabilities are limited.[283] A distinction must be made between "single" controllers, joint controllers, processors, and third parties.

b. Joint controlling

The DPD acknowledges the possibility of a multitude of controllers, called "joint controllers." Article 2 (d) explicitly includes the notion of "control *jointly* executed

[282] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 8 ff.
[283] *Brennscheidt*, Cloud Computing und Datenschutz, p. 59.

by more than one entity." Various entities can take the role of joint controllers in scenarios where many parties are involved. In this case, each of these parties is bound to the provisions of the DPD with respect to the entire processing action.[284] The general criteria to assess this form of controlling are, in principle, the same as for single controlling of only one party.[285] In other words, two or more parties are joint controllers if they determine the essential means and the purposes of the data processing together.[286] However, in practice, the line between joint controlling, on the one hand, and order processing of data, on the other hand, is hard to draw, and often leads to disputes with supervisory authorities. The entities do not need to have a close relationship to each other – for instance, a civil partnership or similar close contractual relations. They can generally choose any legal form to establish their relationship – though, this does not affect the responsibility imposed by data protection law.[287] However, contractual agreements can contain important indications for assessing joint controlling in many cases. In the end, and if doubts occur, the factual circumstances are decisive if the parties make the decisions jointly, or if only one party has to be regarded as a ("single") controller.[288] Therefore, it is not important who has the formal right to decide what happens with the data, but it is crucial who has the actual competence to determine the purposes and means of the processing.[289]

The legal assessment is unambiguous where the different parties jointly determine both the purposes and the means of one particular processing action. However, the Art. 29 Working Party's opinion includes a broader approach to define the scope of joint controlling. According to this opinion, joint controllers do not need to share the same purposes of data processing – they might differ. Depending on the situation, it is sufficient when they merely set up an infrastructure of data processing and determine the essential elements of the means to be used, or if they share the same purpose without jointly deciding on the means.[290] Furthermore, as the Art. 29 Working Party argues, the question of joint controlling is not a matter of one particular data processing action. As Art. 2 (b) DPD states, the term "processing" is not limited to one single action, but also includes a "set of operations."[291] There can be many parties involved in different data processing operations of a particular set of personal data, especially in the context of IT infrastructures. A distinction has to be drawn between "single" controllers acting independently from each other, and joint controllers (or if it is even a case of order

[284] *Wolff/Brink*, Datenschutz in Bund und Ländern, Para. 3, Recital 112.
[285] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 18.
[286] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 18; *Funke/Wittmann*, ZD 2013, 211 f.; see also: *Alich/Nolte*, CR 2011, 741, (743 f).
[287] *Dammann*, in: Simitis, BDSG, Para. 3, Recital 226.
[288] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 18; see also 2.3.1.2.
[289] *Jandt/Roßnagel*, ZD 2011, 160, *Jotzo,* MMR 2009, 232 f.
[290] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 19 f.
[291] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 18.

processing). It is possible that the parties involved divide different tasks and processing operations in a way that each single action appears to be independent and executed by only one controller. However, the entities can also be regarded as joint controllers by taking into consideration the whole set of operations – the "macro-level." This result can be derived from jointly determined purposes, from a jointly set framework that determines the essential means, or when the decisions relating to both questions are taken together.[292] Again, the question of joint controlling is – similar to "single" controlling – a matter of the specific circumstances if the parties factually determine the purposes and/or essential means together.

Though many different scenarios with different legal assessments may occur, one example will illustrate this issue.[293] An airline, a hotel chain and a travel agency establish a platform provided through the internet that allows for a better collaborative travel reservation management between them. They jointly state which data are to be stored on the platform, how reservations are managed and confirmed, to whom access to the data shall be granted, etc. Here, all three parties are joint controllers, with respect to the processing executed by using the common internet platform, since they decided, at least, about the essential means of the processing.

However, one should keep in mind that the Art. 29 Working Party opinions do not have binding effects (see Art. 29, Sec. 1 DPD). In particular, whether such a wide understanding of joint controlling is acceptable may be subject to further discussion. The ECJ's recent Google Spain judgment seems to embrace such an understanding. The ECJ affirmed joint controllership, although the controllers neither intended to cooperate, nor decided together about the purpose of the data processing.[294] Simply the fact that both parties were able to control the processing was sufficient for the ECJ to assume joint controllership.[295]

c. Processing on behalf of the controller

As mentioned above, the controller does not necessarily have to be the entity which actually is processing the data. On the contrary, companies whose main business is not in the IT sector tend to outsource data processing. According to Art. 2 (d) of the DPD, a "processor" is any legal entity processing the data on behalf of the controller (i.e. the outsourcing company will remain in control of the data). All data processing carried out by the processor will be considered as processing carried out by the controller (the outsourcing company); its responsibility relating to these processing actions is not affected. As a consequence, all consent given to the controller and all legal permissions for him/her are valid to permit

[292] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 20.
[293] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 20.
[294] ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Recital 40.
[295] Cf. *Spindler*, JZ 2014, 981 (981).

the processor's actions regarding personal data. The processor is treated as if he/she belonged to the controller's entity. Therefore, no permission is needed for data transfers between the controller and the processor. This scenario is sometimes also called "order processing."

Acting 'on behalf' of the controller contains two basic elements. On the one hand, a processor acts in the controller's interests and not for his/her own purposes. On the other hand, he/she is bound to the controller's instructions (see Art. 16 DPD), at least with respect to the purposes of the processing and the essential means that are used. In this respect, the purpose is the anticipated outcome that is intended or that guides the actions planned, while the means can be defined as how a result is obtained or an end is achieved.[296]

Furthermore, only an entity legally separated from the controller is generally able to act as a processor.[297] The distinction between controller and processor has to be carried out on the basis of the potential control of the party in question. Whoever determines the purposes and essential means (at least by giving instructions) is regarded as a controller and not as a processor (or even a third party).[298] In this context, it is crucial to specify which particular decisions might be delegated to the processor, without entangling the change from processor to controller. The decisions that might be subject to delegation can be divided into two categories requiring different legal assessment. Decisions concerning the purpose of the processing cannot be delegated and are exclusively reserved to the controller's authority.[299] A cloud service provider, for example, will be considered a controller if they collect their users' personal data for their own purposes.[300] In principle, decisions concerning the means of processing might be delegated to the processor (e.g. which software should be used). However, this does not include every technical or organizational question. Some are deeply linked to the lawfulness of the processing and, therefore, essential in a way that they can only be answered by the controller. This relates especially to the duration of the processing, granting access to third persons and the choice of which data should be processed.[301] In a typical cloud computing scenario, the provider only provides the technical framework which is used by the controller. The latter is the one who determines the purposes of the processing. The controller usually decides which data is processed and how long the processing will take and, therefore, governs the (essential) means, whereas the cloud provider only computes the data, as they

296 *Art. 29 Working Party*, Opinion 01/2010, WP 169, 13 f., 25.
297 *Art. 29 Working Party*, Opinion 01/2010, WP 169, 25.
298 *Brennscheidt*, Cloud Computing und Datenschutz, p. 67; *Gola/Schomerus*, BDSG, Para. 11, Recital 9.
299 *Art. 29 Working Party*, Opinion 01/2010, WP 169, 15 f.
300 *Giedke,* Cloud Computing, p 202; *Art. 29-Working Party*, Opinion 08/2010, WP 179, 27; *Art. 29 Working Party*, Opinion 05/2012 WP 196, 10.
301 *Art. 29 Working Party*, Opinion 01/2010, WP 169, 14.

are bound by the contract concluded with the cloud user, thus, having little discretionary power that normally does not lead to a controllership.[302]

To make things even more complicated, cloud computing scenarios are being heavily debated in scenarios in which the provider acts neither as a processor nor as a controller. It is possible that the cloud user does not give any instructions to the cloud service provider on how to handle the data. One might only use the provider's software in a SaaS (Software-as-a-Service) solution to compute self-processed input and receive the results. The provider does not exercise any data processing, but only establishes and maintains the technology to support data processing that is completely initiated and conducted by the controller. In such cases, some argue that one party does not "process" on behalf of another party, but is only indirectly concerned with the data processing; thus, it is not the processor.[303] Others argue that, under those circumstances, the provisions for data processors apply as well, since the risks for the personal data do not differ significantly when compared to a situation in which the processor processes the data directly.[304] At the very least, the provider's mere physical control over the data requires the implementation of sufficient safeguards to sustain data security in those cases (assuming one shares that approach), for instance, measures to prevent data from accidental loss.[305] However, this discussion should not be given undue importance. Whenever a cloud service includes any form of data storage (on the provider's servers) beyond a mere temporary caching, then this storage constitutes a relevant act of data processing. Accordingly, the provider is a processor.[306] This applies even more if the provider fulfills monitoring tasks with respect to the personal data, for example, concerning the access or use.[307] However, there might be situations in which the provider fulfills the requirements of controlling and, therefore, acts as a controller and not as a processor. Here are some examples: A former processor starts processing data for his/her own or another person's purpose, contrary to what was originally determined by the (former) controller. If the "processor" starts to use stored customer data in order to provide commercial

---

[302] *Brennscheidt,* Cloud Computing und Datenschutz, p. 67 f.; *Hennrich*, CR 2011, 546 (548); cf. also *Wolff/Brink*, Datenschutz in Bund und Ländern, Para. 3 BDSG, Recital 111;*Niemann/Paul*, Praxishandbuch Rechtsfragen des Cloud Computing, chapter D, Recital 31 ff.

[303] *Hon/Millard/Walden*, Who is Responsible for "Personal Data" in Cloud Computing?, The Cloud of Unknowing, Part 2, p. 17; *Spindler/Schuster*, Recht der elektronischen Medien, Para. 11 BDSG, Recital 7.

[304] Cf.*Schneider,* Handbuch des EDV-Rechts, chapter B, Recital 266 f.

[305] *Hon/Millard/Walden*, Who is Responsible for "Personal Data" in Cloud Computing?, The Cloud of Unknowing, Part 2, p. 22.

[306] *Pohle/Ammann,* K&R 2009, 625 (630); *Spindler/Nink*, in Spindler/Schuster, Recht der elektronischen Medien, Para. 11 BDSG, Recital 8; see also more differentiated if the provider has a mere passive role: *Hon/Millard/Walden*, Who is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2, p. 18 ff.

[307] *Hon/Millard/Walden*, Who is Responsible for "Personal Data" in Cloud Computing?, The Cloud of Unknowing, Part 2, p. 17.

advertising in a manner not intended by the user, he/she becomes a controller with respect to this new processing action, since he/she set up a new purpose.[308] The same might apply if he/she exceeds other competencies, such as granting data access to unauthorized third parties.[309] Furthermore, the provider can be responsible not only for providing the technical framework, but also for completing the task that leads to the processing action. Whenever the provider is empowered with the competences to decide the essential means and purposes with respect to that task, he/she becomes a controller – even though the involved parties might consider him/her a processor.[310] The outsourcing of a company's bookkeeping might be a typical example in this respect.[311]

There are certain legal requirements to be fulfilled before (order) processing can take place on behalf of the controller (Art. 17, Para. 3 DPD). Processing, for example, requires a contract or legal act binding the processor to the controller. The processor must be bound to the instructions of the controller, and technical and organizational measures must be guaranteed to protect personal data against leaks. The main aim is to oblige the processor to follow the controller's instructions, similar to an employee's obligation. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the technical and organizational measures shall be written down or kept in an equivalent form.[312] One may note that users do not usually have a considerable influence on the contractual clauses provided in a standardized form by the provider. However, it is still part of the controller's responsibility to agree to processing contracts that comply with the respective legal data protection provisions. A lack of actual power does not justify concluding an unlawful processing contract.[313] The EU's Art. 29 Working Party recommends certain issues to be covered in a contract between the cloud provider and the user.[314] However, in practice, these requirements are sometimes difficult to fulfill. On the one hand, it

[308] *Art. 29 Working Party,* Opinion 05/2012, WP 196, 14.

[309] *Hon/Millard/Walden*, Who is Responsible for "Personal Data" in Cloud Computing?, The Cloud of Unknowing, Part 2, p. 20.

[310] Cf. *Brennscheidt*, Cloud Computing und Datenschutz, p. 67; *Funke/Wittmann*, ZD 2013, 221 (223); *Hoeren*, in: Roßnagel, Handbuch Datenschutzrecht, chapter 4.6, Recital 97.

[311] *Petri*, in: Simitis, BDSG, Para. 11, Recital 28.

[312] *Art. 29 Working Party,* Opinion 05/2012, WP 196, 12.

[313] *Art. 29 Working Party*, Opinion 01/2010, WP 169, 26; *Hilber*, Handbuch Cloud Computing, p. 357.

[314] They require, for example: details concerning the client's instructions to be issued to the provider and relevant penalties, including potential actions against the provider, in case of noncompliance, specification of the security measures the provider must comply with, subject and time frame of the cloud service to be provided, a confidentiality clause, the controller's rights to monitor, the cloud provider's obligation to cooperate, a list of locations in which the data may be processed, and a prohibition of communicating data to third parties or subcontractors not mentioned in the contract. The whole list of recommendations has 14 items and can be found in *Art. 29 Working Party,* Opinion 05/2012, WP 196, 12 f.

is highly unlikely that big global players in the cloud computing business will actually be bound and controlled by mid-sized or small companies concerning cloud computation (e.g. referring to inspections on the spot). On the other hand, a company not operating in the IT sector might not even be interested in or be able to provide this kind of control.[315] Since the data might be stored not in one but in many different locations, visiting the provider's data centers for an on-site audit seems to be impossible, particularly for the cloud user. In addition, it might even be hard to tell where exactly the data will be stored due to the scalability of cloud services.[316] Besides the difficulties for a user to visit and audit all data centers their provider is using, it would constitute a data security risk for the provider to let (all of) their users inspect all of their data centers. This model of control is reliant on the classic outsourcing model, with only one data centre to be controlled that is unlikely to be based in another country.

However, other options to fulfill obligations to control the processor have been proposed: As the directive does not require the controller to ensure the processor's compliance directly, they could rely on a qualified third party to control the processor (third-party auditing model).[317] On the other hand, the user would still have to pay for this third party, something that might be impractical even for private individuals. The controller could demand inspection reports from the processor recording their processing activities, but this would not ensure the processor's actual compliance, since those reports would be made by the processor themselves.[318] An effective, yet practical, way to ensure compliance is data protection certification.[319] Here, a third party provides the necessary assessment particularly of a cloud provider. Compared to the third-party audit-model mentioned before, the difference is that not every client of the provider has to hire the third party individually. The certification costs are initially covered by the provider and then redistributed to all possible clients by the provider, making it possible to professionally control every data centre and affordable even for private customers. Being certified might provide a competitive advantage for global players, since this advertises a high standard of data protection to possible clients. The directive does not mention such certificates explicitly; nevertheless, they could be used by a controller to ensure the compliance of the processing done on their behalf.[320]

---

315 *Heidrich/Wegener,* MMR 2010, 803 (806).

316 *Brennscheidt*, Cloud Computing und Datenschutz, p. 102.

317 *German Federal Office for Information Security Technology*, Safety Recommendation for Cloud Computing Providers, p. 63.

318 *Brennscheidt,* Cloud Computing und Datenschutz, p. 105.

319 *Art. 29 Working Party,* Opinion 05/2012, WP 196, 22.

320 For a detailed description of data protection seals, see *Brennscheidt,* Cloud Computing und Datenschutz, p. 105 ff.

2. Controller and processor under the General Data Protection Regulation

The GDPR also distinguishes between the controller as the responsible entity and the processor as the entity actually processing the data. Nevertheless, there will be changes in the particular responsibilities of those entities and new ways for the controller to make sure their processor complies with the law. The model of "order processing" will be possible under the GDPR when all prerequisites described below are met. Some have criticized the lack of a provision that states explicitly that transfers from a controller to his/her processor are generally allowed if "order processing" takes place.[321] However, this does not take into account that the legitimation for such transfers lies in the model of "order processing" itself. Without this legitimation, all provisions regarding processing on behalf of the controller would make sense.[322] The processing occurs on behalf of the controller, i.e. the law treats the acts of processing as if the controller would realize them directly. Therefore, it is the controller who decides on why and how to process the data.

a. Rules for the controller

Article 4, Para. 5 of the GDPR defines the controller as the natural or legal person, public authority, agency, or any other body which, alone or jointly with others, determines the purposes, conditions and means of personal data processing. There are no significant changes in the definition of "controller," compared to the DPD. The cloud user as the entity determining the purpose and the means of the data processing is the controller. They are responsible for data processing and will be accountable if legal requirements are not met.[323] To reach that goal, the controller has to implement technical and organizational measures and adopt appropriate policies. Article 22, Para. 1 provides certain criteria to determine if these measures are valid to ensure compliance with the data protection law and the data subjects' privacy. In addition to the obligation to ensure compliance and to provide policies that respect the data subjects' free choices (Art. 22, Para. 1a), the

321 *Nebel/Richter,* ZD 2012, 407 (411); *Roßnagel/Nebel/Richter*, ZD 2013, 103 (105); c.f. *Koós/Englisch*, ZD 2014, 276 (284), who see the legitimation in Art. 6 lit. f GDPR whether data transfers between the controller and the processor will be considered as necessary for the purposes of the legitimate interests pursued by the controller and not overridden by the interests of the data subject (see 2.4.2.2) and, therefore, be based on a express legal permission.

322 C.f. regarding the DPD, but with the same problem: Drews/Montreal, PinG 14, 143.

323 The controller's main duties are regulated in Art. 22 of the GDPR: "1. The controller shall adopt appropriate policies and implement appropriate and demonstrable technical and organizational measures to ensure and be able to demonstrate in a transparent manner that the processing of personal data is performed in compliance with this regulation, i.e. having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself" (LIBE proposal). The wording of Art. 22 of the proposal of the Council is different to the LIBE proposal, but includes no significant changes, it just leaves out the examples given in the proposal of the Parliament.

controller also has to be able to demonstrate the adequacy and effectiveness of those measures and policies.[324] Moreover, the Council's proposal adds in Art., 22 Para. 2 (b) that "an approved certification mechanism pursuant to Art. 39 may be used as an element to demonstrate compliance with the requirements set out in Para. 1 and 2."[325]

b. Joint controllers

According to the GDPR definition of "controller," several entities can be "joint controllers." Since there have been only slight changes in the GDPRs definition of a "controller" compared to the DPDs definition, the distinction between one "controller" or several "joint controllers" remains the same. Art. 24 of the GDPR binds joint controllers to come to an arrangement that clarifies each controller's duties. According to Recital 62 of the GDPR, the arrangement should reflect the controllers' roles and relationships. The essence of the arrangement has to be made available to the data subject.

c. Rules regarding the processor

The processor (also often called "order processing") means a natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the controller (Art. 4, Para. 6). The controller's duties regarding the processor begin before the processing on their behalf takes place: they have to choose a processor who will comply with the GDPR's requirements.[326] The regulation follows the approach of the DPD and requires the controller to make sure that he/she ensures the control over the data processing (determining the means of the processing, the organizational and technical measures required,[327] process-

[324] To achieve this goal, Recital 60 GDPR recommends independent internal or external auditors. Article 28 requires documentation of the data processing by the controller (and the processor, as well). They must cooperate with the supervisory authority of Art. 29; take technical and organizational measures to ensure the security of processing Art. 30; alert and inform clients about data breach, according to Art. 31, Para. 2; conduct a privacy impact assessment under certain conditions of Art. 32a and 33, Para. 1 or seek a prior authorization in accordance with Art. 34, Para. 1; appoint a data protection officer, as requested in Art. 35, Para. 1; as well as comply with rules for transfers to third countries, as mentioned in Art. 40 ff. The powers of regulators may be expressly addressed to the processors, according to Art. 53 Para. 1 (a).

[325] Still, the LIBE proposal and the Council's proposal leave several paragraphs out that the proposal of the EC introduced to the GDPR in 2012, e.g. measures such as "designating a data protection officer pursuant to Article 35(1)."

[326] Article 26, Para. 1: Where processing is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this regulation and ensure the protection of the rights of the data subject, particularly with respect to the technical security measures and organizational measures governing the processing to be carried out, and shall ensure compliance with those measures.

[327] Article 30 GDPR clarifies what is meant by "technical and organisational measures." Those measures shall, among other things, at least "protect stored or transmitted personal data against

ing only on their instructions, their inspection rights, etc.) by contractual obligations of the processor.[328] However, the aforementioned practical problems will still be the same.[329] In contrast to the DPD, the legal consequence of a breach of

accidental or unlawful destruction, or accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure" (Art. 30, Para. 2 lit. b GDPR). Of course, they still have to take organizational measures to fulfill all of their duties regulated in Art. 30 GDPR.

[328] Article 26 (2) defines a set of rules that must, in practice, be endorsed in the contract, such as: (a) proposal of the Commission: "act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;" LIBE proposal: "process personal data only on instructions from the controller, unless otherwise required by Union law or Member State law;" proposal of the Council: "process the personal data only on instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;" (b) "employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality" (not included in the Council's proposal); (c) "take all required measures pursuant to Article 30;" (d) proposal of the Commissions: "enlist another processor only with the prior permission of the controller;" LIBE proposal: "determine the conditions for enlisting another processor only with the prior permission of the controller, unless otherwise determined;" proposal of the Council: "respect the conditions for enlisting another processor (...), such as a requirement of specific prior permission of the controller;" (e) LIBE proposal: "insofar as this is possible, given the nature of the processing, create in agreement with the controller the appropriate and relevant technical and organizational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights, laid down in Chapter III;" not included in the Commission's proposal; proposal of the Council: "taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III;" (f) proposal of the Commission: "assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;" LIBE proposal: "assist the controller in ensuring compliance with the obligations, pursuant to Articles 30 to 34, taking into account the nature of processing and the information available to the processor;" proposal of the Council: "assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;" (g) proposal of the Commission: "hand over all results to the controller after the end of the processing and not process the personal data otherwise;" LIBE proposal: "return all results to the controller after the end of the processing, not process the personal data otherwise, and delete existing copies unless Union or Member State law requires storage of the data;" proposal of the Council: "return or delete, at the choice of the controller, the personal data upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject;" (h) proposal of the Commission: "make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article;" LIBE proposal: "make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow on-site inspections;" proposal of the Council: "make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits conducted by the controller. The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions."

[329] The cloud user, as the controller, might not be in the position to determine contractual clauses but might have to agree to whatever the much stronger processor (the cloud provider) dictates.

this agreement is explicitly regulated.[330] The switch of roles for the processor (from mere processing to determining and controlling any data processing) leads, thus, to a re-qualification of the processor now as a data controller – with all obligations and duties. According to Art. 26 (2) (d), the processor may use services of other processors if the data controller has given their prior consent.[331] Thus, a cloud provider, for example, may mandate other subcontractors (sub-cloud providers, etc.) to process the data. However, the data controller is still in charge of controlling the whole process, so that he/she has to ensure that the inspection rights are also enforceable in the relationship with the third-party processor (sub-cloud provider).[332]

XII. Access to user data by third parties

Access to user data by third parties has to be justified either by consent or by legal permission, for example, enforcing a contract, as mentioned already. Hence, there is no general right for a third party to have access to data of a person affected. In particular, data brokering is not allowed unless a person affected has given consent to it, or it is no longer personalized data (in the case of pseudonymization or anonymization).

XIII. Provisions on data retention

Provisions on data retention had originally been foreseen by the EC directive on data retention,[333] as well as the implementing acts in Germany regarding the Telecommunication Act. However, the ECJ declared the directive as void.[334] Previ-

It might also be impossible for the cloud user to do on-site inspections for the reasons described above. This problem has been addressed by the GDPR, since it is now possible for the controller to rely on data protection seals and third-party audits.

330 Article 26 (4) states: "If a processor processes personal data other than as instructed by the controller or if they become the determining party in relation to the purposes and means of data processing, the processor shall be considered to be a controller in respect of that processing, and shall be subject to the rules on joint controllers laid down in Article 24."

331 *Brennscheidt*, Cloud Computing und Datenschutz, p. 116.

332 In the proposal of the Council, Art. 26, Para. 2 (a) stipulates these principles as follows: "where a processor enlists another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor (…) shall be imposed on that other processor (...) Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."

333 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L of 13.4.2006, p. 105 ss.

334 ECJ, decision of 08/04/2014 – C-293/12, C-594/12 – Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others.

ously, the German Constitutional Court had already declared the German provisions in more or less the same manner as void.[335] The main arguments referred to the unspecified powers for state prosecutors and the police to process data, as the relevant provisions did not implement necessary precautions (such as judicial control) for the individuals addressed. Moreover, both courts stated that there were no precautionary rules concerning the safety of retained data and controls of how the data could be used by third parties. According to a recent statement of the EC, there are no plans to revitalize a data retention directive.[336] However, the German Government has recently presented a new proposal for a (national) data retention act.[337]

XIV. Transfer of data on an international scale, transfer to third countries and requirements for data transfer outside the country

1. By processor outside the EU/European Economic Area (EEA)

If the processor does not fall under the jurisdiction of an EU/EEA member state, data transmission between the controller and the processor generally has to comply with the conditions described. In addition, the requirements of data transfer to third countries have to be met; under no circumstances shall personal data be transferred to a third country that is not providing an adequate level of protection without the requirements described. Nevertheless, the contract binding the processor to the controller can be used to ensure necessary safeguards. Therefore, in other words, only if either an adequate level of protection is provided within the third country or other sufficient safeguards are ensured, will the DPD allow it to constitute an order processing, including the legal privileges.[338]

2. Data transfer to third countries

a. Data Protection Directive

Transferring data to a 'third country' (a state not within the EU or the EEA) is principally forbidden unless the data subject consents or the provisions of the DPD expressly permit it.[339] The same problems mentioned above can also occur

---

[335] German Federal Constitutional Court (*Bundesverfassungsgericht*), decision of 02/03/2010 – 1 BvR 256/08 – BVerfGE 125, 260 (retention of data).

[336] See the news of the European Commission, dated 09//03/2015, available at http://ec.europa.eu/deutschland/press/pr_releases/13145_de.htm.

[337] Cf. *Gesetzesentwurf des Bundeskabinetts* of 27/05/2015: http://www.bmjv.de/SharedDocs/Kurzmeldungen/DE/2015/20150527_Hoechstspeicherfrist_Kabinett.html.

[338] *Brennscheidt*, Cloud Computing und Datenschutz, p. 76.

[339] In detail *Art. 29 Working Party,* Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74.

in connection with the data subject's consent to data processing in a cloud when the data subject has to agree to a transfer in an unsafe country.[340] Hence, there is a difference between the legal permission to process data and the legal permission to transfer the data to a third country. Only if both requirements are fulfilled separately, is the data transfer lawful. One of the main exceptions refers to the "adequate level of protection" in the third country (Art. 25 of the directive).[341] An adequate level of protection assumes that the data protection standards in the respective country are comparable to the European standards. This has to be officially acknowledged by the EC. It did so, for instance, for Andorra, Argentina, Australia, Canada, Switzerland, Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, the United States (Safe Harbor), and the Eastern Republic of Uruguay.[342] Being of particular relevance, the USA has not been generally acknowledged.[343]

In addition to these countries acknowledged officially (where no explicit consent by the user is needed), the data controller who wants to transfer data in other countries may use other forms of justification provided by the DPD. It is generally possible if the controller adduces evidence of adequate safeguards with respect to the protection of the data subject's rights, Art. 26, Para. 2 of the directive. Those safeguards can be based on appropriate standard contractual clauses which the EC has acknowledged regarding processors in third countries[344] between the controller and the entity receiving the data, and ensuring an adequate level of protection. Those clauses are used to establish rules for the third-country parties that are protecting the data subject's rights as equally as the EU data protection law does. However, the benefit of a lawful transfer to the third country only exists if the clauses acknowledged by the EC are used exactly as the EC provided them,

---

340 See also *Brennscheidt,* Cloud Computing und Datenschutz, p. 175.

341 *Hon/Millard*, Data Export in Cloud Computing – How Can Personal Data be Transferred outside the EEA?, p. 5.

342 All decisions by the European Commission regarding the acknowledgment of third countries are available at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

343 No such decision has been made by the commission; *Gabel,* in Taeger/Gabel, BDSG, Para. 4b, Recital 23; *BITKOM,* Leitfaden Cloud Computing, p. 53.

344 See also *Art. 29 Working Party,* Opinion 03/2009, WP 161; Standard Contractual Clauses I, Commission Decision of 15/06/2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, C(2001) 1539 (2001/497/EC), available at https://www.datatilsynet.no/Global/04_skjema_maler/EUs%20standardkontrakter1_ENG.pdf; Standard Contractual Clauses II, Commission Decision of 27/12/2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, C(2004) 5271 (2004/915/EC), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF; Commission Decision 2010/87/EU of 05.02.2010 on Standard Contractual Clauses for Data Processors established in Third Countries, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

without any alteration.[345] For a cloud user who wishes to transfer data to a cloud provider within a third country, the standard contractual clauses would then only be useful if the cloud provider agrees to those exact clauses. It seems unlikely that a cloud provider contracting with many cloud users would alter his/her normal contractual agreements and, instead, agree to the standard contractual clauses. Another way of providing adequate safeguards are the so-called Binding Corporate Rules (BCR). Other than the standard contractual clauses, BCR are not mentioned explicitly in the directive. Nevertheless, Art. 26, Para. 2 is not exhaustive, which means appropriate safeguards might be measures other than the standard contractual clauses mentioned explicitly; they are only an example among a number of possible safeguards.[346] The BCR are supposed to ensure that there is an adequate level of data protection for data transfers within a corporation, regardless of the countries in which the corporation might be seated.[347] The BCR have to be binding or legally enforceable and should be regarded as "sufficient safeguards" within the meaning of Art. 26, Para. 2 of the DPD. They are meant to be used by multinational companies to allow international data transfers.[348] There are no model BCR provided by the Art. 29 Working Group or the EC, as with standard contractual clauses. However, the Art. 29 Working Group proposed crucial elements of BCR and how these rules might be structured in a single document.[349] The BCR have to be acknowledged by a supervisory authority in an EU member state. In case of such an acknowledgement, authorities of most EU member states acknowledge BCR automatically, thus, creating some form of European passport (notwithstanding the fact that the DPD does not contain such a procedure).[350] In some specific cases, BCR may be used for cloud computing-related data transfers, however, these will be restricted to internal data transfers across borders.[351] On the other hand, most cloud-related data transfers to third countries will not be within a corporation, but occur rather in a cloud, thus, transferring data from a

[345] *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 4c, Recital 14; Spindler, in Spindler/Schuster, Recht der elektronischen Medien, Para. 4c BDSG, Recital 20.

[346] *Art. 29 Working Party,* Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74, p. 6.

[347] *Art. 29 Working Party*, Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74, p. 8: "The rules must apply generally throughout the corporate group, irrespective of the place of establishment of the members, or the nationality of the data subjects whose personal data is being processed, or any other criteria or consideration."

[348] *Art. 29 Working Party*, Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP 74, p. 8.

[349] C.f. Art. 29 Working Party, Working Document Setting up a Framework for the Structure of Binding Corporate Rules, WP 154.

[350] *Brennscheidt*, Cloud Computing und Datenschutz, p. 173.

[351] *Niemann/Paul*, K&R 2009, 444 (449).

cloud user to a cloud provider. Therefore, BCR do not provide a general solution for cloud computing related to third-country transfers.[352]

Although the Safe Harbor Agreement has been criticized for not living up to the requirements of European data protection law, US American companies who joined the Safe Harbor agreement and are following its principles were considered for a long time to be providing an adequate level of protection.[353] Some national authorities, such as the German supervisory authorities, began to require a real ("on-the-spot") examination of the validity of the US company's claim to obey the Safe Harbor agreement.[354] Due to their inability to access their cloud provider's data processor, smaller cloud users faced severe problems to pass these tests. Therefore, compliance by means of the Safe Harbor Agreement seems to be impractical for cloud solutions, at least given the actual practice of some supervisory authorities.[355] The CJEU confirmed recently that the Safe Harbor Agreement does not respect the fundamental rights of European citizens regarding data protection, because the EC did not check the adequacy of US data protection law and it did not review the Safe Harbor Agreement after Edward Snowden's revelations, thus, infringing fundamental rights of data subjects:[356]

> *74 It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.*
>
> *75 Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country result-*

[352] *Brennscheidt*, Cloud Computing und Datenschutz, p. 174.

[353] The Safe Harbor Principles are available at http://export.gov/safeharbor/; *Hon/Millard*, Data Export in Cloud Computing – How Can Personal Data be Transferred outside the EEA?, p. 15.

[354] *Düsseldorfer Kreis*, Decision of 28th/29th April 2010, available at http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile; *Marnau/Schlehahn*, DuD 2011, 311 (315).

[355] *Brennscheidt*, Cloud Computing und Datenschutz, p. 166; *Heidrich/Wegener,* MMR 2010, 803 (806); *Giedke,* Cloud Computing, 233.

[356] CJEU 6.10.2015 - C-362/14 Schrems ./. Facebook, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddfd64713c5ac748b3903d92afe7911381.e34KaxiLc3qMb40Rch0SaxuRbN90?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=245729 (last accessed 27 October 2015).

ing from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

76 Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard.

77 Moreover, as the Advocate General has stated in points 134 and 135 of his Opinion, when the validity of a Commission decision adopted pursuant to Article 25(6) of Directive 95/46 is examined, account must also be taken of the circumstances that have arisen after that decision's adoption.

78 In this regard, it must be stated that, in view of, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection, the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict (see, by analogy, judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 47 and 48).

b. General Data Protection Regulation

Concerning the transfer of data to companies/data processors located outside the EU, the regulation follows the approach of the DPD.[357] The GDPR also demands the two steps necessary for a lawful transfer, as mentioned above. The first step refers to the permission to process the personal data. The second one concerns the transfer to a third country, thus, safeguarding an adequate level of protection (comparable to the European level), which is crucial for any transmission. The instruments which a data processor can use to comply with these requirements remain essentially the same.[358] Concerning the benchmarks and relevant criteria

[357] *Nebel/Richter,* ZD 2012, 407 (412).

[358] The transmission can be based on: an acknowledgement of adequacy by the EC (Art. 42 GDPR), "binding corporate rules" (Art. 42 (2 a) and Art. 43 GDPR), a European Data Protection seal

which the EC will use for acknowledgement of an adequate level, Art. 41 (2) of the GDPR requires the EC to take into consideration the legal framework, the existence of adequate supervisory authorities and the international commitments of the third country.[359]
In addition, Recital 81 of the GDPR states that "In line with the fundamental values on which the Union is founded, particularly the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law." Moreover, the Council's proposal adds *inter alia*,

> *The third country should offer guarantees that ensure an adequate level of protection in particular when data are processed in one or several specific sectors. In particular, the third country should ensure effective data protection supervision and should provide for co-operation mechanisms with the European data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.*

In a nutshell, the EC has to balance all of these elements and compare the level of data protection in the third country to the one in Europe.

Transfers by the way of BCR are specified in Art. 43 of the GDPR. The BCR have to fulfill certain criteria to make a data transfer to a third country lawful. They have to ensure all essential principles and enforceable rights of the GDPR to be considered an appropriate safeguard for third-country transfers. Their purpose is to enable corporate groups to transfer data to entities within the same corporate

---

(Art. 42 (2 aa) GDPR – only included in the LIBE proposal; the Council's proposal nevertheless includes "an approved certification mechanism pursuant to Article 39 together with binding and enforceable commitments of the controller or processor" (Art. 42, Para. 2 (e)) (see 2.3.2.4), standard data protection clauses adopted by the Commission (Art. 42 (2 b) - not included in the LIBE proposal - or standard contract clauses (Art. 42 (2 c) GDPR), or contract clauses approved by a supervisory authority (Art. 42 (2 d) GDPR (Art. 42, Para. 2a (a) in the Council's proposal)).

[359] In particular, Art. 41 (2) requires to "give consideration to the following elements:
(a) the rule of law, relevant legislation in force, both general and sectorial, including concerning public security, defense, national security and criminal law as well as the implementation of this legislation, the professional rules and security measures which are complied with in that country or by that international organization, jurisprudential precedents, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;
(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organization in question responsible for ensuring compliance with the data protection rules, including sufficient sanctioning powers, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and
(c) the international commitments the third country or international organization in question has entered into, in particular any legally binding conventions or instruments with respect to the protection of personal data."

group (Recital 85 GDPR). The BCR will be approved by the EC if they fulfill the criteria set out in Art. 43. The LIBE committee of the EU Parliament changed the former version significantly. The BCR have to bind not only members of the controller's group, but also subcontractors – an amendment which is aimed specifically at cloud computing services.[360] Moreover, the European data protection seal (Art. 39) can be used to provide evidence of a processors' compliance with the GDPR by the controller if a processing on their behalf shall take place. The seal can provide evidence for appropriate safeguards concerning the level of data protection in order to permit a transfer to a third country. Hence, the data protection seal can be important for both steps needed to render a third-country transfer lawful. Appropriate safeguards can also be provided by means of standard contractual clauses or contract clauses approved by a supervisory authority. In each model, the contract has to be concluded between the controller transferring the data and the party receiving the data in the third country. Thus, the receiving party shall be bound to the European data protection principles. Although the person whose data is being processed is not part of the contract, this person has to be provided with information, according to Art. 14 of the GDPR. Whereas standard contract clauses acknowledged by the EC have general validity (Art. 62 1 (b) GDPR),[361] individual contract clauses of a controller need to obtain prior authorization from the competent supervisory authority (not the EC), Art. 42, Para. 4 of the GDPR.[362] The Council's proposal, nevertheless, adds to Recital 79 that "Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this regulation or any other provisions of EU law and include safeguards to protect the rights of the data subjects." This amendment will not make it easier to achieve international agreements compliant with this regulation.

Finally, the Safe Harbor Agreement will not be affected by the GDPR.[363] Data transfers to a controller or a processor within the USA will, therefore, still be possible if the receiving party follows the Safe Harbor principles. This does not solve

---

[360] *Kelly,* ITRE Committee Opinion on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 –C7-0025/2012 – 2012/0011(COD)) 26th of February 2013, p. 140 available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/itre/ad/927/927816/927816en.pdf.

[361] Not anymore included in the Council's proposal, but in accordance with Art. 42, Para. 2c, the clauses have to be adopted by a supervisory authority and the EC pursuant to the examination procedure referred to in Art. 87, Para. 2.

[362] Article 42, Para. 2a in the Council's proposal.

[363] Recital 79 states that: "This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data, including appropriate safeguards for the data subjects- ensuring an adequate level of protection for the fundamental rights of citizens." See also *Nebel/Richter,* ZD 2012, 407 (412).

the problems arising from the rather self-regulatory character of Safe Harbor described above. If appropriate safeguards have not been taken to guarantee an adequate level of data protection, the transfer of personal data to a third country can only be carried out if Art. 44 of the GDPR's requirements are met. Thus, either the data subject has to give their consent (causing the same problems as those described above) to the transfer, or one of the legal permissions in Art. 44 (b) to (g) should be applicable. Those permissions are similar to Art. 6 of the GDPR's legal permissions for processing personal data. Note that Art. 44 takes effect on the second step (if the transfer to a third country is lawful) and not on the first step (if the processing itself is lawful).

c. Place of jurisdiction

As mentioned already, either according to the DPD interpreted by the ECJ in the Google Spain case, as well as according to the proposed GDPR, it is sufficient that there is a subsidiary in the EU, even if the subsidiary is only engaged in marketing activities, or that the service is addressed to European citizens so that their data is being processed.

d. Third-country actions against data controllers

Article 43a, Para. 1 of the LIBE proposal provides a verdict on enforceability and "reject-ability" of judgments of a court, a tribunal or a decision of an administrative authority of a third country regarding the requirement of a controller or processor to disclose personal data.[364] This negative clause is clearly aimed at activities of third countries that oblige providers (data controllers, processors) to disclose personal data – following the National Security Agency scandals and revelations of Edward Snowden. Although the first unofficial draft of the regulation by the EC in late November 2011 (which had been leaked to the public) contained a similar provision in its Art. 42, the official proposal in January 2012 omitted this provision.[365] The EU Parliament reintroduced this article in an obvious reaction to the monitoring activities of foreign intelligence agencies.

Moreover, a US Court recently obliged a cloud provider to disclose data not only stored in the United States, but also on a server based in Ireland.[366] The court

[364] *Stadler*, Der Datenschutz bietet keine Handhabe gegen die Überwachungspraxis der Geheimdienste; *Klinger*, jurisPR-ITR 6/2014 annotation 2.

[365] *Logemann*, LIBE-Ausschuss bestätigt Gesetzentwurf zur EU-Datenschutz-Grundverordnung; *Bergemann*, EU-Datenschutzverordnung darf nicht Merkels NSA-Feigenblatt werden; Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR), Version 56 (29/11/2011), available at http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf.

[366] In Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., F. Supp. 2d., No. 13 Mag. 2814, 2014 WL 1661004, at *11 (S.D.N.Y. Apr. 25, 2014), CRi 2014, 91 and available at http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398.

denied to assign a warrant after Microsoft filed an instant motion against it. The warrant based on the US Stored Communications Act (SCA) obliged Microsoft to disclose information to the US government, and was specifically referring to an e-mail account hosted in Dublin and, therefore, stored within the EU. Whereas Microsoft argued that the SCA cannot be applied extraterritorially, the court refused to accept this argument and extended the application of the SCA to third countries.

To protect persons within the EU from having their personal data transferred to a third country based on a third-country ruling which is not compliant with the European data protection law, Recital 90 of the GDPR of the LIBE proposal states: "In cases where controllers or processors are confronted with conflicting compliance requirements between the jurisdiction of the EU, on the one hand, and that of a third country, on the other, the Commission should ensure that EU law takes precedence at all times." In case of an order issued by a third-country court or supervisory authority, the controller or processor and, if existing, the controller's representative shall notify the supervisory authority of the request without undue delay *and must obtain prior authorization for the transfer or disclosure by the supervisory authority* (Art. 43a, Para. 2). In principal, no judgment of a court or tribunal of an administrative authority in a third country will be recognized in the EU if a controller or processor is forced to disclose personal data (Art. 43a, Para. 1). The supervisory authority has to assess the compliance of the disclosure requested with the regulation and, in particular, if the disclosure is necessary and legally required in accordance with Art. 44, Para. 1 d and Art. 44, Para. 5. Without prejudice to Art. 21, the controller or processor must also inform the data subjects of the request and of the authorization by the supervisory authority and, where applicable, inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to the point of Art. 14, Para. 1. Thus, the European data protection law can require data controllers and processors to break a third country's law in order to comply with Art. 43 (a). If the supervisory authority does not acknowledge the data transfer required by a third-country authority, according to the GDPR, the controller or processor will be in a collision of obligations.[367] This difficult situation is addressed in Recital 90 of the GDPR.[368] Nevertheless, this declaration of will does not really provide a clear solution for the dilemma of a cloud provider under the control of European law and the law of a third country.

[367] Plath, Datenherausgabepflicht für Cloud-Anbieter nach US-Recht v. EU-Datenschutzrecht, available at http://www.cr-online.de/blog/2014/05/13/datenherausgabepflicht-fuer-cloud-anbieter-nach-us-recht-vs-eu-datenschutzrecht/.

[368] Recital 90 GDPR: The Commission should provide guidance and assistance to the controller and processor, and it should seek to resolve the jurisdictional conflict with the third country in question.

XV. Enforcement

1. Civil law

The European DPD provides in Art. 23 a general liability rule for civil claims concerning damages suffered by the person affected, combined with a reversal of burden of proof concerning the responsibility of the controller. Hence, the German Data Protection Law reserves for an individual the right to sue the data controller who is infringing data protection rules, Sec. 7 of the BDSG. However, there are scarcely any decisions to be noted which are based upon Sec. 7 of the BDSG; the bulk of civil court decisions refer to violation of "personality rights" based upon Sec. 823 of the German Civil Code. Moreover, there are no rules or principles for assessing immaterial damages occurred due to data protection infringements.[369]

The GDPR intends to maintain this situation. If data has been processed unlawfully, the data subject should then have the right to claim compensation, even for nonpecuniary damages, according to Art. 77 of the GDPR. Unlike the DPD, it is not only the controller who is liable for such damages. If an "order processing" takes place, the processor also faces liability.[370] This might have a huge impact, as it could be more promising, for instance, to hold the solvent provider liable (usually the cloud user's client) than holding the cloud user liable. The GDPR includes the possibility to avoid liability for damages if the "controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage," Art. 77 (3) (not included in the LIBE proposal). Since it is the processor or the controller who need to prove that they are not responsible for the damage, they should both take the technical and organizational measures that the GDPR demands and fulfill their duty to document the processing, according to Art. 28 of the GDPR. It is an advantage for the person affected claiming compensation for damages that it is up to the processing parties to prove that they are not responsible. On the other hand, the person affected still has to provide evidence for the causation of the unlawful processing for the damages. It has been criticized that this might not be possible for the person affected, because they will not have insight into or be able to document the controller's or the processor's internal procedures.[371] Where more than one controller or processor is involved in

---

[369] Cf. *Spindler*, expertise for the 69th German Jurists Forum in Munich 2012 – Gutachten für die Verhandlungen des 69. Deutschen Juristentages in München 2012 [DJT 2012], Band I, Gutachten, p. F 56 f.

[370] Article 77 (1): Any person who has suffered damage, including non-pecuniary damage, as a result of an unlawful processing operation or of an action incompatible with this Regulation, they shall have the right to claim compensation from the controller or the processor for the damage suffered.

[371] *Roßnagel/Richter/Nebel,* ZD 2013, 103 (108).

the processing, each of those controllers or processors shall be jointly and individually liable for the entire amount of the damage, unless they have an appropriate written agreement determining their responsibilities, pursuant to Art. 24 (Art. 77 (2)). Joint liability for joint controllers makes it important for them to come to an agreement that fully reflects their responsibilities in the data processing. In this way, only the respective controller will be liable in their respective relation for damages caused by their actions.

However, the Council's proposal grants a privilege to processors who are not responsible for the damage caused by the processing of a controller, Art. 77, Para. 2: "A processor shall be liable for the damage caused by the processing only where it has not complied with obligations of this regulation specifically directed to processors or acted outside or contrary to lawful instructions of the controller." This exception is a positive provision to cloud computing providers who act as processors in contrast to the strict regulations of the LIBE proposal. The processor shall be exempted from liability if it can be proved that it is not in any way responsible for the damage (Para. 3). If a controller or processor is liable for the damage, it can claim back parts of the compensation from the other responsible party(ies) in accordance with Para. 5 of the Council's proposal: "Where a controller or processor has (...) paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage in accordance with the conditions set out in paragraph 2."

2. Criminal law

There are some provisions related to data protection concerning criminal law, in particular Sec. 44 of the BDSG, which sanctions infringements of obligations mentioned in Sec. 43 (2). However, very few final convictions based on Sec. 44 have been reported so far.[372] In theory, an infringer can be sentenced to two years imprisonment, provided that they had acted deliberately. The European DPD does not enshrine such provisions, as the EU has no competence in criminal law. The lack of enforcement is one of the most important concerns of the current data protection legislation. By contrast, Art. 78 of the EC's proposal for a GDPR (Art. 79b of the Council's proposal) obliges member states to introduce "penalties" for infringements of the GDPR which have to be "effective, proportionate and dissuasive."[373] In addition, the GDPR provides for sanctions which are simi-

[372] In 2011, throughout Germany, only eight convictions, c.f. *Ehmann*, in Simitis, BDSG, Para. 44, Recital 4; Moreover, the German High Federal Court (BGH) has applied this section just once, see its decision of 04/06/2013 – 1 StR 32/13, NJW 2013, 2530 (2532 ff.).

[373] Article 79 (2): "To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions: (a) a warning in writing in cases of first and non-intentional non-compliance; (b) regular periodic data

lar to antitrust fines. These fines, based on the turnover (not the net profits!), have been discussed intensively, as they may turn out to constitute an existential threat to enterprises. Finally, Art. 63, Para. 1 of the GDPR seeks to strengthen cross border enforcement.[374] Thus, the provision introduces some form of mutual acknowledgement of enforceable orders in Europe.

3. Administrative law

The enforcement of the European DPD (and its implementing national laws) is in the hands of independent supervisory authorities. The ECJ recently reinforced the status of independence of these authorities.[375] The GDPR pursues this approach by confirming the status of independence of authorities explicitly in Art. 47 (1) ("with complete independence"). Thus, governments may not interfere with the activities of these supervisory authorities/agencies. However, there are often complaints (by supervisory authorities) that they lack sufficient manpower to enforce data protection rules in every part of the economy. According to Sec. 38 (1), sentence 8 in conjunction with Sec. 21, sentence 1 of the BDSG, anyone may appeal to the supervisory authority if he or she believes that his or her rights have been infringed.[376] The data subject affected has to explain specifically the alleged violation of their rights.[377] Only in this case is the supervisory authority obliged to deal with the petition.[378] Thus, individuals do have a right to request the authority to intervene. If the supervisory authority does not act after a conclusive request by a data subject, it can be forced with an action for performance to act.[379] As the supervisory authorities are located at the level of the *Länder*, there is no aggregation of their activities at the federal level in the sense of an overall report of their activities.[380]

protection audits; (c) a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater."

374 Article 63 (1): "For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned (only in the Commission's proposal)."

375 ECJ, decision of 08/04/2012 – C-288/12 – European Commission/Hungary.

376 *Grittmann*, in Taeger/Gabel, BDSG, Para. 38, Recital 52; *Petri*, in Simitis, BDSG, Para. 38, Recital 35.

377 *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 38, Recital 15; *Weichert*, in Däubler/Klebe/Wedde/Weichert, BDSG, Para. 38, Recital 14.

378 *Plath*, in Plath, BDSG, Para. 38, Recital 34.

379 *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 38, Recital 17; Administrative Court of Darmstadt, decision of 18/11/2010 – 5 K 994/10.DA = MMR 2011, 416; different opinion: Administrative Court of Munich, decision of 11/02/2008 – 5 C 08.277.

380 Hence, their annual reports are crucial in order to find evidence of their supervising activities. These, however, do not distinguish between general activities, such as providing legal opinions for parliaments or courts, on the one hand, and administrative actions and sanctions, on the other hand. As an example we scrutinized one of the most prominent supervising authorities in Germany, the *Unabhängiges Landeszentrum für Datenschutz* (ULD), and looked at the recent report on activities for 2014 (published at https://datenschutzzentrum.de/tb/tb35/index.html). The

According to budget plans and information given by data supervisory authorities, it seems that they are hardly able to monitor the complex issues of data protection in a thorough way today.[381]

4. The Data Protection Officer

Not strictly belonging to administrative law, but worthwhile noting, is a specific feature of German law (not enshrined in the DPD, but foreseen in the proposal of the GDPR, Art. 35 – 37): the Data Protection Officer (DPO: *Datenschutzbeauftragter*). This is a specific privacy officer who has to be installed in every corporation (with more than nine persons regularly involved in data processing, Sec. 4f (1) of the German Data Protection Law). This officer is in charge of checking compliance with data protection rules and has to report breaches of rules to the board of directors. Municipalities do not have their own data protection supervisory authority. According to Sec. 38 (6) of the BDSG, the task of monitoring and supervising the private bodies has been transferred to the *Länder*, which have installed the authorities for this purpose.[382] All *Länder*, apart from Bavaria, have assigned the supervision of the private and public sector and assigned it to the data protection commissioners of the *Länder* (*Landesdatenschutzbeauftragte*).[383] According to the Data Protection Acts of the *Länder*,[384] every public body which processes personal data has to appoint a data protection officer automatically, in accordance with Sec. 4f of the BDSG, however, a specific municipal supervisory authority next to the supervisory authorities of the *Länder* does not exist.

ULD reports on a wide range of activities, which, however, do not result in formal actions, rather in guidances and opinions for data controllers, which led obviously, in most cases, to an enhancement of data protection. Formal legal actions and sanctions seemed to be rarely handed down. Only one administrative sanction (*Bußgeldbescheid*) was reported for 2014, amounting to 18,000 € of penalty. Moreover, no administrative decisions (*Bescheide*) have been reported. Hence, the bulk of activities seem to take place (and seemingly successfully) in the forefront of any administrative formal sanction. The supervisory authority, such as the ULD, often reports that they confronted the infringing data controller with the possibility of inaugurating a formal procedure or investigation procedure, which has obviously already resulted in the yielding of the data controllers to the wishes of the supervising authorities.

381 The practice, for example, of administrative actions and sanctions in some selected provinces is as follows: Berlin (25 administrative actions in 2014, total sum of sanctions in 2014: 88,205 €, 17 criminal proceedings); Hesse (34 administrative actions in 2013, total sum of sanctions: 12,1250 €); Baden-Wurttemberg (34 administrative actions, total sum of sanctions: 21,550 €); Bavaria (no competence for administrative actions and sanctions, no criminal proceedings); Budget for 2014 and jobs in some provinces: Berlin (5,032,600 €, 39 full-time jobs); North Rhine-Westphalia (3,872,900 €, 54 full-time jobs), Baden-Wurttemberg (1,727,400 €, 29.5 full-time jobs); Lower Saxony (2,484.00 €, 30.6 budget jobs); Bavaria (2,177,500 €; 31 jobs).

382 *Weichert*, in Däubler/Klebe/Wedde/Weichert, BDSG, Para. 38, Recital 4.

383 *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 38, Recital 29; *Grittmann*, in Taeger/Gabel, BDSG, Para. 38, Recital 42.

384 C.f. sec. 8a of the Data Protection Act of Lower Saxony or sec. 32a (1) of the Data Protection Act of North Rhine-Westphalia.

a. The position of the Data Protection Officer

Data Protection Officers can be natural persons employed by the controller (internal DPOs), or external DPOs, including legal persons.[385] The DPO needs to have comprehensive knowledge of data protection law, and also sufficient specific knowledge of the business sector in question.[386] Furthermore, according to Sec. 4f (2), sentence 1 of the BDSG, it is necessary that he or she demonstrates the reliability necessary for the performance of the duties concerned, in particular that no conflicts of interests may arise.[387] The duties of the DPO are laid down in Sec. 4g of the BDSG, however, this is not exhaustive.[388] The main task of the DPO is to ensure compliance with the Data Protection Act and other data protection provisions at the data processing company, Sec. 4g (1), sentence 1 of the BDSG. He or she has an obligation to monitor all the data processing operations within the controller and ensure they comply with the data protection law, to monitor the use of computer programs according to the rules, and to perform training courses and further education within the company.

However, the monitoring of the DPO does not relieve the controller of his or her responsibility for compliance with data protection rules.[389] He or she advises and analyzes, but has no authority to impose duties requiring action or instructions on the controller; consequently, the DPO has no decision-making powers concerning those data protection measures he or she considers to be necessary.[390] Furthermore, the appointment of a DPO has the effect that the obligation to register automated processing procedures (Sec. 4d (1) BDSG) shall, in accordance with Para. 2, not apply.[391] In addition, in accordance with Sec. 4f (3), sentence 1 of the BDSG, the DPO shall be directly subordinate to the head of the controller, so that the independent exercise of their monitoring and consulting function is en-

[385] *Scheja*, in Taeger/Gabel, BDSG, Para. 4f, Recital 82; *Simitis*, in Simitis, BDSG, Para. 4f, Recital 48 ff.; *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recital 10; *Knopp*, DuD 2015, 98 (99 ff.); different opinion: *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, par. 4f, Recital 19, which states that the qualification and reliability needed for this task can only be fulfilled by a natural person; *Schaffland/Wiltfang*, BDSG, Para. 4f BDSG, Recital 45.

[386] *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 4f, Recital 20 ff.; *Wybitul*, MMR 2011, 372 (375).

[387] Examples for conflicts of interest are the head of the IT Unit or the head of Human Resources, see further examples at *Haag*, in Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil II, Kap. 1, Recitals 58 ff.

[388] *v. d. Bussche*, in Plath, BDSG, Para. 4g, Recital 1.

[389] *Simitis*, in Simitis, BDSG, Para. 4g, Recital 29; *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 4g, Recital 2.

[390] *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recitals 2, 41; *Scheja*, in Taeger/Gabel, BDSG, Para. 4g, Recital 8.

[391] *Scheja*, in Taeger/Gabel, BDSG, Para. 4d, Recital 20; *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recital 3.

sured. The DPO is, therefore, directly connected to the management and occupies a job outside the company hierarchy.[392]

b. Rights and powers of the Data Protection Officer

The DPO has to be granted access and the right to inspections to all the areas within the firm by the company if this appears to be necessary for the performance of their task.[393] Additionally, in accordance with Sec. 4f (5) of the BDSG, the company has to support the DPO in the performance of their duties. In this way, by providing appropriate material, personal and organizational conditions, their freedom of action shall be guaranteed.[394]

c. Independence of the Data Protection Officer and the special dismissal protection

According to Sec. 4f (3), sentence 2 of the BDSG (as well as Art. 18 (2) of the DPD and Recital 49 of the DPD), the DPO is free to use their specialized knowledge in the area of data protection, and is largely independent of the controller in terms of a professional and functional independence.[395] Furthermore, they enjoy a discretion to decide when, where and how to monitor compliance with data protection provisions.[396] However, a purely organizational supervision by the controller is permissible[397] and the controller is entitled to give orders in case of incorrect behavior of the DPO.[398] The independence of the DPO does not assign them decision-making powers; these remain a competence of the controller.[399]

Because of their function, the DPO must not face any disadvantages, especially regarding their career advancement.[400] There is a special revocation and dismissal protection for the DPOs. They can, in accordance with Sec. 4f (3), sentence 4 of the BDSG, only be revoked by the controller if there is an important reason, i.e. further activity as a DPO has to be unreasonable (as defined by Sec. 626 of the German Civil Code) for the controller.[401] In accordance with Sec. 38 (5), sentence 3 of the BDSG, their dismissal can be demanded by the supervisory

[392] *Haag*, in Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil II, Kap. 1, Recital 68.
[393] *Wybitul*, MMR 2011, 372 (376).
[394] *Scheja*, in Taeger/Gabel, BDSG, Para. 4f, Recital 90.
[395] *Haag*, in Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil II, Kap. 1, Recital 64.
[396] *Simitis*, in Simitis, BDSG, Para. 4f, Recital 86; *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recital 34.
[397] *Simitis*, in Simitis, BDSG, Para. 4f, Recital 86, 125; *Scheja*, in Taeger/Gabel, BDSG, Para. 4f, Recital 86; *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recital 35.
[398] *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recital 35.
[399] *Scheja*, in Taeger/Gabel, BDSG, Para. 4f, Recital 87; *Simitis*, in Simitis, BDSG, Para. 4f, Recital 127; *Haag*, in Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil II, Kap. 1, Recital 67.
[400] *Scheja*, in Taeger/Gabel, BDSG, Para. 4f, Recital 89; *v. d. Bussche*, in Plath, BDSG, Para. 4f, Recital 42; *Wybitul*, MMR 2011, 372 (376).
[401] See regarding possible reasons for a dismissal: *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recital 59.

authority if they do not possess the specialized knowledge and cannot show evidence of the reliability necessary for the performance of their designated duties.[402] Moreover, the DPO who is employed by a company benefits from a special dismissal protection (see Sec. 4f (3), sentence 5 BDSG). However, this protection only applies to companies that, in accordance with Sec. 4f (1) of the BDSG, are legally obliged to appoint a DPO due to the size of the company, and not for those that voluntarily appoint a DPO on a voluntary basis.[403] Section 4f (3), sentence 5 of the BDSG clarifies that this protection, furthermore, only applies to internal DPOs who can only be dismissed if there is reason for the controller to terminate the appointment for just cause without complying with a notice period. After the DPO has been removed from office, the special dismissal protection is extended to one year. However, external DPOs can be dismissed without this special protection, because their contractual relationship with the controller is not a contract of employment.[404]

d. Status and duties of the Data Protection Officer towards the data protection supervisory authority

In accordance with Sec. 4g (1), sentence 2 of the BDSG, in cases of doubt, the DPO *may* consult the competent authority responsible for data protection control with regard to the controller concerned. Thus, the DPO and the data protection supervisory authority should cooperate (Art. 37 of the GDPR proposal even intensifies this cooperation), particularly in cases of doubt about the application and interpretation of legal regulations.[405] In any case, the DPO is obliged to have recourse to the supervisory authority if an infringement has been identified due to a complaint by a person affected.[406] Moreover, the DPO may use the advice given by the supervisory authority according to Sec. 38 (1), sentence 2 of the BDSG. On the other hand, in accordance with Sec. 38 (5), sentence 3 of the BDSG, the supervisory authority may demand their dismissal if they do not possess the specialized knowledge and demonstrate the reliability necessary for the performance of their duties.[407]

---

[402] C.f. regarding this procedure: *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 4f, Recital 37a.
[403] *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 4f, Recital 40.
[404] *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 4f, Recital 40; *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recital 61.
[405] *Scheja*, in Taeger/Gabel, BDSG, Para. 4g, Recital 36; *Simitis*, in Simitis, BDSG, Para. 4g, Recital 23; different opinion: *Scheja*, in Taeger/Gabel, BDSG, Para. 4g, Recital 37.
[406] *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 4g, Recital 15.
[407] *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 38, Recital 27; *Petri*, in Simitis, BDSG, Para. 38, Recital 74.

e. The Data Protection Officer and the proposal for a General Data Protection Regulation

The proposed GDPR aims to raise the threshold from 9 to 250 persons or even more (Art. 35 regarding private entities). This has been criticized in Germany and in other EU member states as well, but in a contrary way, because those countries are unfamiliar with DPOs and fear an intervention in entrepreneurial freedom.[408] The LIBE proposal once again has changed these requirements by switching from a number of employees to the number of persons affected. In accordance with Art. 35 (1) lit. b, the requirements are put in force if "the processing is carried out by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period or if the core activities of the controller or the processor consist of processing special categories of data pursuant to Art. 9 (1), location data or data on children or employees in large scale filing systems" (lit. d).

In contrast to this, the proposal of the Council leaves the designation of a DPO directly to the discretion of the controller or the processor themselves, except as required otherwise by EU or member state law (Art. 35 (1)). In addition to the professional qualities of the DPO, their absence of any conflict of interests is explicitly defined in Art. 35 (5). According to the Council, the DPO shall inform and advise not only the controller and the processor, but also the employees who are processing personal data. The informing, advising and the following monitoring have to concern the obligations due to the GDPR and also to the other EU or member state data protection provisions (Art. 37 (1) lit. a, b). This seems to be an extension of the DPO's tasks required by the proposal of the Council. However, the DPO shall have to take into account the nature, scope, context, and purposes of the processing data operations in order to determine their risks (Art. 37 (2a)). In addition, the proposal of the Council did not include the obligation of the DPO of giving notifications to the supervisory authority anymore (Art. 37 (1e)), which will lead to cost savings for business.

By contrast, the reliefs which German data protection law provides for controllers with an independent DPO (such as Sec. 4d (2) of the BDSG: no obligatory registrations, Sec. 4d (6) of the BDSG: prior checking) are not matched by the GDPR.[409] Moreover, the GDPR does not provide for a special dismissal protection for the DPO.[410] Article 35 (7), sentence 3 of the GDPR only enshrines a revocation protection, according to which "the data protection officer may only be dismissed if the data protection officer no longer fulfils the conditions required for the performance of their duties," which, however, is an intensification in com-

[408] *v. d. Bussche/Voigt*, Konzerndatenschutz, Teil 2, Kap. 1, Recital 78; *Eckhardt/Kramer/Mester*, DuD 2013, 623 (628); *Jaspers/Reif*, RDV 2012, 78 (78).
[409] *Eckhardt/Kramer/Mester*, DuD 2013, 623 (628).
[410] *Gürtler-Bayer*, Der behördliche Datenschutzbeauftragte, p. 288; *Jaspers/Reif*, RDV 2012, 78 (80).

parison to the BDSG's provision.[411] Furthermore, the direct link between the DPO and the management (Sec. 4f (3), sentence 1 of the BDSG) has not been adopted to the GDPR, signifying a lower level of independence for the officer in the new proposal.[412] Furthermore, the GDPR does not require the DPO to ensure compliance within the company in addition to mere monitoring and supervision.[413] However, the GDPR provides in Art. 37 (1) lit. g and h a closer cooperation of the DPO with the supervisory authority than in German data protection law.[414]

Finally, enforcement in the EU raised conflicts of competences between the supervisory authorities of different member states, such as data protection authorities in Germany and Ireland concerning the data processing of Facebook. In order to overcome such conflicts, the GDPR provides for a so-called consistency mechanism (Art. 57 – 63 of the GDPR) and the establishment of an independent European data protection board (Art. 64 – 72 GDPR).

XVI. Role of self-regulation and co-regulation

The DPD and the GDPR encourage the adoption of codes of conduct.415 In Germany, the Association for Self-regulating the Internet (Verein zur Selbstregulierung der Internetwirtschaft) has developed such codes, particularly concerning geolocation services.416 Moreover, the German Association of Insurances developed a Code of Conduct (Verhaltensregeln für den Umgang mit personenbe-

411 *Gürtler-Bayer*, Der behördliche Datenschutzbeauftragte, p. 288.

412 *Gürtler-Bayer*, Der behördliche Datenschutzbeauftragte, p. 289; *Hullen*, in v. d. Bussche/Voigt, Konzerndatenschutz, p. 402.

413 *Gürtler-Bayer*, Der behördliche Datenschutzbeauftragte, p. 293; *Jaspers/Reif*, RDV 2012, 78 (84).

414 *Gürtler-Bayer*, Der behördliche Datenschutzbeauftragte, p. 294 f.

415 Article 27 DPD: "The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors. In addition recital 61 of the DPD states: Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation. Art. 38 (1) GDPR refers to codes for fair and transparent data processing, respect for consumer rights; the collection of data, the information of the public and of data subjects; requests of data subjects in exercise of their rights; information and protection of children; transfer of data to third countries or international organisations; mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it; out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data."

416 http://www.sriw.de/index.php/geodatenkodex.

zogenen Daten durch die deutsche Versicherungswirtschaft) in 2013, which has been approved by the data supervisory authority of Berlin.[417]

D. Review of International Initiatives on Consumer Data Protection *(Consumers International)*

This section of the study will review summarily some international initiatives related to consumer data protection.

I. UN Guidelines for Consumer Protection

The United Nations Guidelines for Consumer Protection (UNGCP) were approved by the General Assembly on April 9th 1985. They are a set of recommendations for governments to develop an adequate consumer protection policy in their countries, in areas ranging from product safety to consumer education, dispute resolution and international cooperation. The UNGCP were updated in 1999 to include sustainable consumption.

At the time they were approved data protection was not an issue for consumers, so there is not a single mention of it in the text of the UNGCP. In 2012, the United Nations Conference on Trade and Development (UNCTAD), which is in charge of consumer issues within the UN system decided to launch a consultation among its members and other relevant stakeholders to assess the state of consumer protection in the world and to analyse the need for an update of the UNGCP. In an Ad Hoc Consumer Protection Expert meeting held in Geneva in July 2013, UNCTAD decided to start a process to update the UNGCP. Though the initial call only included financial services and electronic commerce, the list of issues to be included in the new UNGCP was extended to other relevant areas of consumer concern, including data protection and privacy. Consumers International was one of the parties that insisted on this inclusion.

The successive drafts of the revised text for the UNGCP varied from the first one circulated in December 2014. This draft was preceded by a Report prepared by UNCTAD on the basis of a set of questionnaires sent to all member states and stakeholders to inquire about their preferences of issues to include. Most respondents supported the inclusion of data protection and privacy while a minority were against it.

[417] http://www.gdv.de/wp-content/uploads/2013/03/GDV_Code-of-Conduct_Datenschutz_2012.pdf

Nevertheless, data protection and privacy were at the centre of a controversy on whether and how they should be included in the Guidelines.

The latest draft of the text included references to consumers' privacy in the Preamble of the Resolution[418], and in the Guidelines. The Preamble contains a specific recognition of member states` common interest to promote and protect consumers' privacy:

> *"Recognizing that, Member States have a common interest in promoting and protecting consumer privacy, and the global free flow of information"*

The most important inclusion is the recognition of privacy as one of the legitimate needs of consumers which the Guidelines are intended to meet (Guideline 5 (k)). These legitimate needs, commonly referred to as "consumer rights", are the essence of the Guidelines, and consumers' privacy has now been included among them.

Furthermore, a new clause of the Guidelines which refers to good business practices states: "11(e) Protection of privacy. Businesses should protect consumers' privacy through appropriate control, security, transparency and consent mechanisms relating to the collection and use of their personal data."

Finally, the draft contained new text on what national consumer policies should cover, which for the first time includes consumer privacy and data security (Guideline 14 (g)).

The seventh United Nations Conference to Review All Aspects of the Set of Multilaterally Agreed Equitable Principles and Rules for the Control of Restrictive Business Practices in July 2015 adopted a Conference Resolution that invited the General Assembly of the United Nations to consider the adoption of the Draft Resolution and Revised Guidelines on Consumer Protection as annexed to it at its 70th Session in 2015.[419] The Resolution was finally adopted on 22 December 2015.[420]

II. OECD Guidelines

The Organisation for Economic Cooperation and Development (OECD) has a long history of working on data protection and privacy issues. Their Guidelines on the Protection of Privacy and Transborder Flow of Personal Data were made public in 1980 and they are still one of the main documents on these issues. They are a set of basic principles that can serve as a basis for the creation or updating of

[418] This resolution has a preamble and an instrumental section, followed by an annex with the updated text of the Guidelines.

[419] http://unctad.org/meetings/en/SessionalDocuments/tdrbpconf8_resolution_en.pdf (last accessed 7 August 2015).

[420] United Nations, General Assembly, Resolution A/RES/70/186.

national legislation and a tool to coordinate and harmonise international cooperation in this field. As the Preface of the Guidelines in the 1980 version[421] states:

> *"The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly… to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.*
>
> *On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.*
>
> *For this reason, OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it."*[422]

The OECD Guidelines were updated in 2013 after a thorough analysis and work of the OECD CCP.[423]

These Guidelines "apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties."[424]

The scope of the Guidelines is personal data held by public or private sectors that can pose a danger for the privacy and individual liberties of people.

---

[421] The OECD Guidelines were updated in 2013. This preface was deleted for the new updated version.

[422] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

[423] C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79

[424] Article 2 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

The Guidelines consist of five parts. According to the Explanatory Memorandum of the OECD,

> *"[p]art one contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7-14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, i.e. principles which are chiefly concerned with relationships between Member countries. Part Four deals, in general terms, with means of implementing the basic principles set out in the preceding parts and specifies that these principles should be applied in a non-discriminatory manner. Part Five concerns matters of mutual assistance between Member countries, chiefly through the exchange of information and by avoiding incompatible national procedures for the protection of personal data. It concludes with a reference to issues of applicable law which may arise when flows of personal data involve several Member countries."425*

The Memorandum states that the

> *"core of the Guidelines consists of the principles set out in Part Two […]. It is recommended to Member countries that they adhere to these principles with a view to:*
>
> *a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;*
>
> *b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;*
>
> *c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and*
>
> *d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows.*
>
> *As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.*
>
> *Finally, Parts Four and Five of the Guidelines contain principles seeking to ensure:*
>
> *a) effective national measures for the protection of privacy and individual liberties;*

---

425 OECD, Explanatory Memorandum to the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, para. 23-24, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

b) avoidance of practices involving unfair discrimination between individuals; and

c) bases for continued international co-operation and compatible procedures in any regulation of transborder flows of personal data."[426]

The eight basic principles set out in the Guidelines are the following:

1) *Collection Limitation Principle:*

"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[427]

2) *Data Quality Principle:*

"Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."[428]

3) *Purpose Specification Principle:*

"The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."[429]

[426] OECD, Explanatory Memorandum to the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, para. 25-26, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

[427] Article 7 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

[428] Article 8 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

[429] Article 9 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

4) *Use Limitation Principle:*

"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: *a)* with the consent of the data subject; or *b)* by the authority of law."[430]

5) *Security Safeguards Principle:*

"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."[431]

6) *Openness Principle:*

"There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."[432]

7) *Individual Participation Principle:*

"An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
1. within a reasonable time;
2. at a charge, if any, that is not excessive;
3. in a reasonable manner; and
4. in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

[430] Article 10 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

[431] Article 11 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

[432] Article 12 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."[433]

8) Accountability Principle:

*"*A data controller should be accountable for complying with measures which give effect to the principles stated above."[434]

The OECD Guidelines served as a basis for the development and enhancement of privacy protection and legislation for member and non-member countries for many years. However, the technological advancements that happened since their introduction, mainly the growing use of the internet and the way information is exchanged between people and borders, made the OECD initiate a process to update the content of the Guidelines. In 2007, a Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy was approved, encouraging members to improve their national legislation on privacy and to develop effective international mechanisms for facilitation of the enforcement of privacy law, as well as provide mutual assistance among each other. In 2010, when the Guidelines completed their 30th anniversary, OECD began the preparations for a revision of the text, to align it to the new developments in privacy issues. An Expert Group was appointed to suggest the path and content for that revision.

The OECD Privacy Framework states the following:

"The approach that emerged from the work of the Expert Group suggested that, although the environment for privacy and transborder data flows has changed significantly, an update to the 1980 Guidelines was preferred rather than a fundamental rethinking of its core principles. The Expert Group took the view that the balance reflected in the eight basic principles of Part Two of the 1980 Guidelines remains generally sound and should be maintained. The Expert Group introduced a number of new concepts to the OECD privacy framework, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other

[433] Article 13 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

[434] Article 14 of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 7 August 2015).

aspects of the 1980 Guidelines were expanded or updated, such as accountability, trans-border data flows and privacy enforcement."[435]

As technology advances, the difficulties for people to control the use that is given to their data have become more evident. In a sort of oxymoron, the availability of technological tools often brought more confusion to consumers because of the increasing complexity and the frequent changes in privacy policies from the companies. As it was stated by OECD:

"Although the individual is an active player in personal data flows, the ability to exert control over his/her own personal data is now more difficult. Individuals often face a lack of information or overly complex information about how, why and by whom their personal data may be used. Relying on "rules of thumb" when making decisions, presenting inconsistencies when weighing probabilities, placing more value on the present than on the future, affect how individuals understand information that is presented to them and may affect how they make privacy decisions. A further complication may arise when privacy policies change too frequently, which may also add to the general confusion of individuals. Obtaining access to their personal data can also be challenging both for individuals and organisations, given business models and the volume of data. The degree of protection ensured by obtaining individuals' consent to uses and individuals' control of their personal data by having access to it is less clear and may need further consideration."[436]

III. The Global Privacy Enforcement Network (GPEN)

The Global Privacy Enforcement Network (GPEN) is a group of privacy enforcement agencies that works on cross-border cooperation. Its mission is described as following:

"In June 2007, OECD governments adopted a Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. The Recommendation called for member countries to foster the establishment of an informal network of Privacy Enforcement Authorities.

It further specified a number of tasks for the network:

- *Discuss the practical aspects of privacy law enforcement co-operation;*
- *Share best practices in addressing cross-border challenges;*
- *Work to develop shared enforcement priorities; and*

[435] OECD, The OECD Privacy Framework,2013, available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last accessed 7 August 2015).

[436] Ibidem.

- *Support joint enforcement initiatives and awareness campaigns.*

In the summer of 2008, privacy authorities began to exchange experiences and discuss the practical aspects of enforcement cooperation via a Web utility. Since then, several agencies from OECD and non-OECD countries have joined the network."[437]

The GPEN Action Plan highlights that

"[c]onsistent with the objectives and scope of the Recommendation, the members intend that this network focus primarily on facilitating cooperation in the enforcement of privacy laws governing the private sector, while also recognizing that members may wish to cooperate on matters involving the processing of personal data in the public sector. This network is not intended to interfere with governmental activities related to national sovereignty, criminal and civil law enforcement, national security, or public policy ('ordre public')."[438]

GPEN has a Committee of up to 5 members that perform the following tasks:

"- Process applications from authorities wishing to participate in GPEN and make recommendations for membership to participating authorities.

- Activate user accounts for access to GPEN website.

- Edit public pages of the website.

- Facilitate arrangements for GPEN teleconferences and meetings.

- Liaise with OECD Secretariat over administration of website.

The GPEN Committee may perform other functions that support GPEN's mission.

Wherever possible, the GPEN Committee should include members from different geographic regions of the world."[439]

As stated on the webpage, GPEN has the following mission:

---

437 https://www.privacyenforcement.net/ (last accessed 7 August 2015).

438 Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

439 Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

"A. Statement of Mission:

GPEN connects privacy enforcement authorities from around the world to promote and support cooperation in cross-border enforcement of laws protecting privacy.

It primarily seeks to promote cooperation by:

- *exchanging information about relevant issues, trends and experiences;*
- *encouraging training opportunities and sharing of enforcement know-how, expertise and good practice;*
- *promoting dialogue with organizations having a role in privacy enforcement;*
- *creating, maintaining and supporting processes or mechanisms useful to bilateral or multilateral cooperation; and*
- *undertaking or supporting specific activities as outlined below."*[440]

The agencies that want to be part of GPEN must fulfil the following requisites: be responsible for enforcing laws or regulations the enforcement of which has the effect of protecting personal data; and have powers to conduct investigations or pursue enforcement proceedings.[441] "More than one privacy enforcement authority from a single country, economy, or jurisdiction may participate in GPEN when there are several agencies with the power to enforce laws and regulations related with personal data and privacy."[442] For example, the US members of GPEN are the Federal Trade Commission and the Federal Communications Commission. "Participants should designate a point of contact within their authority to facilitate GPEN-related communications and enforcement cooperation dialogue."[443]

GPEN has produced an Action Plan that defines the activities that they will carry on. These activities include:

[440] Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

[441] See Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

[442] Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

[443] Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

"- Periodic conference calls and meetings to discuss enforcement issues, trends, and experiences.

- *Presentations on effective investigative techniques and enforcement strategies and about various privacy enforcement regimes.*
- *Exploration of similarities and differences in procedural, substantive and evidentiary rules to address challenges to cooperation.*
- *Facilitation of coordination of investigations involving multiple authorities.*
- *Cooperation with other organizations or networks involved with related activities.*
- *Supporting cross-jurisdictional educational projects addressing privacy and data security-related issues for business or consumers.*
- *Posting relevant content to the GPEN website.*
- *Maintaining, in cooperation with international organizations, an authoritative contact point directory for enforcement purposes for countries around the world.*
- *Training sessions on privacy and data security-related matters with non-governmental advisors, such as representatives from industry, academia, international organizations and professional associations.*
- *Secondments and office visits between participating authorities.*

Such activities may be arranged depending upon the priorities and interests of participating authorities. Activities may sometimes be arranged in conjunction with other networks or non-participants."[444]

GPEN may undertake additional activities that support its mission.[445] The Action Plan states that:

"[p]articipation in particular activities is not a mandatory part of GPEN participation but is up to individual participants as appropriate and subject to each participant's jurisdiction, interest and available time and resources.

Participants may also seek opportunities for providing assistance to one another on a bilateral basis, in appropriate privacy investigations and enforcement matters, prioritizing cases for cooperation that are the most serious in nature."[446]

---

444 Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

445 See Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

In addition, the Action Plan

> *"does not create any new legally binding obligations by or amongst the Participants [, and cooperation] remains subject to the domestic laws and international obligations applicable to the [members of the network, and they do not have] to provide confidential or sensitive information or cooperate in particular cases. […The Action Plan can] be refined or changed by consensus amongst the participants, as new issues arise.*
>
> *GPEN is focused on the practical aspects of privacy enforcement cooperation and Participants do not intend for GPEN to issue public opinions, position papers, or recommendations on privacy policy. However, GPEN may develop and share consensus views with other bodies on means to advance cross-border privacy enforcement cooperation."*[447]

IV. Convention 108

Convention 108 refers to the Convention for the Protection of Individuals with regard to automatic processing of personal data, which was adopted by the Council of Europe in 1981.

This Convention is "the first legally binding international instrument adopted in the field of data protection"[448], with the objective of securing in the territory of each nation for every individual, whatever their nationality or residence, respect for their rights and fundamental freedoms, and in particular the right to privacy, with regard to automatic processing of personal data relating to them. Its purpose is:

> *"to secure [...] for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data."*[449]

As expressed on the webpage of the European Data Protection Supervisor, the Convention

---

[446] Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

[447] Global Privacy Enforcement Network, GPEN Action Plan, adopted 15 June 2012; Part E amended 22 January 2013, available at: https://www.privacyenforcement.net/public/activities (last accessed 7 August 2015).

[448] European Data Protection Supervisor, Data protection legislation, available at: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2. (last accessed 7 August 2015).

[449] European Data Protection Supervisor, Data protection legislation, available at: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2. (last accessed 7 August 2015).

"sets out minimum standards aimed at protecting the individuals against abuses which may accompany the collection and processing of personal data. It also seeks to regulate the transborder flow of personal data."[450]

The right to protection of personal data encompasses the protection of privacy, but also extends beyond it. Data protection is about securing respect for rights and fundamental freedoms, in particular (i.e. not only) the right of the data subject to privacy. This is further explained in the Convention's explanatory statement. Paragraph 25 states:

'The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms […] it acknowledges that the unfettered exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example: privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit). It is in order to maintain a just balance between the different rights and interests of individuals that the convention sets out certain conditions or restrictions with regard to the processing of information. No other motives could justify the rules which the Contracting States undertake to apply in this field.'

A total of 41 European states have ratified the Convention so far."[451]

The Electronic Privacy Information Center summarizes the aim of the Council of Europe and the effects of the Convention as follows:

"The aim of the Council of Europe was to achieve greater unity between its members based on the respect for the rule of law, human rights and fundamental freedoms. Included among these rights is the right to the respect for privacy, especially taking into account the increasing flow of personal data across national frontiers through automatic processing.

[…]

To this day, the Convention remains the only binding international legal instrument with a worldwide scope of application in the field of data privacy, open to any country, including countries which are not Members of the Council of Europe. In addition, this Convention has withstood the test of time by being adaptive and fairly rigorous. Today the prin-

450 European Data Protection Supervisor, Data protection legislation, available at: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2. (last accessed 7 August 2015).

451 European Data Protection Supervisor, Data protection legislation, available at: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2. (last accessed 7 August 2015).

ciples of this agreement are being examined for their applicability to the collection and processing of biometric data."[452]

V. Regional Initiatives

1. Asia Pacific Economic Cooperation (APEC)

In 2004, the heads of governments of APEC countries endorsed a document that created a Framework for Information Privacy Protection. The framework was developed by the Asia Pacific Economic Cooperation's (APEC) Electronic Commerce Steering Group (ECSG). The preamble recognised the need to set clear guidance on the development of national legislation on privacy as well as a set of principles that that legislation should follow. It also encourages cooperation on cross-border flow of personal data. The Preamble states that:

"this Framework on information privacy protection was developed in recognition of the importance of:

- *Developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;*
- *Recognizing the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;*
- *Enabling global organizations that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;*
- *Enabling enforcement agencies to fulfil their mandate to protect information privacy; and,*
- *Advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners."*[453]

The Framework declares that its main source are the OECD Guidelines, something that seems very logical as many of APEC countries are members of OECD:

"The APEC Privacy Framework comprises a set of nine principles that apply to "personal information" (equivalent to "personal data") about a living individual (equivalent to "data subject") processed by a "personal information controller"

[452] Electronic Privacy Information Center, Council of Europe Privacy Convention, available at: https://epic.org/privacy/intl/coeconvention (last accessed 7 August 2015).
[453] APEC Privacy Framework. Published by APEC Secretariat, Singapore, 2005.

(equivalent to "data controller") and infers the existence of "data processors"[454]. The 9 principles are: 1) preventing harm; 2) notice; 3) use; 4) collection limitation; 5) choice; 6) security safeguards; 7) integrity; 8) access and correction, and 9) accountability.[455]
According to Chris Pounder, editor of Data Protection Quarterly,

> *"[l]ike the OECD Guidelines, implementation of the APEC framework is not mandatory; China for instance has indicated that it will have nothing to do with them. […T]he principles are enforced by a diffuse regulatory framework based around a consensus view as to what the data protection standard should be. Such standards will emerge from discussion and debate between APEC member states, no doubt with input from data protection experts. There is a requirement to establish an enforcement mechanism, but this can be very low key, and there is no requirement to establish a Privacy Commissioner, although member states can do so if they want. […]The data protection principles are drafted as a number of general objectives which are capable of diverse interpretations. The principles relate to: preventing harm to data subjects; provision of a notice; limitation on collection of personal data; limit on the uses of personal information; individual choice over use and disclosure; maintaining the accuracy and integrity of personal information; security safeguards; access and correction; and accountability via a regulatory framework.These headings are unremarkable – unlike the detail that is underneath each heading."*[456]

He concludes as follows:

> *"The APEC Privacy Framework is missing a great deal of data protection detail. In the absence of this important detail, the Framework:*
>
> - *is unlikely to provide an adequate level of protection as required by the European Data Protection Directive;*
> - *is likely to result in inconsistent implementation by APEC member states and a confused hotchpotch of national data protection laws, regulations or rules;*
> - *is likely to be policed by a very weak regulatory regime;*
> - *is likely to allow member states to adopt divergent policies on important privacy aspects with the result that the Framework is unlikely to provide a sound, long-term, basis for the international trade in personal data; and*

[454] Chris Pounder, Why the APEC Privacy Framework is unlikely to protect privacy, http://www.out-law.com/page-8550 (last accessed 7 August 2015).
[455] Chris Pounder, Why the APEC Privacy Framework is unlikely to protect privacy, http://www.out-law.com/page-8550 (last accessed 7 August 2015).
[456] Chris Pounder, Why the APEC Privacy Framework is unlikely to protect privacy, http://www.out-law.com/page-8550 (last accessed 7 August 2015).

- *contains principles and procedures which could be implemented in a way that results in an unacceptable or minimal level of protection for personal data."*[457]

The principles, according to his view, are "ambiguous as to their effect and are capable of a vast number of interpretations and implementations"[458], considering that:

> *"[i]t is possible that an APEC member state, for example, Australia or New Zealand, could develop rules compliant with European Directive standards. But other member states could use the Framework's flexibility to implement a minimalist approach to privacy compliance that falls very far short of what would be deemed 'an adequate level of protection'."*[459]

2. Association of South East Asian Nations (ASEAN)

The Asian nations also have an encouraging work on data protection within its limits. The most remarkable efforts are those made by the Association of South East Asian Nations (ASEAN), a group of Asian countries that develop several activities in many fields, one of which is privacy and data protection.
According to Chris Connolly, Director of Galexia, an independent consultancy specialising in privacy and electronic commerce from Australia, ASEAN

> *"has also recognised the importance of harmonised data protection legal infrastructure. The ten Member Countries of ASEAN have a combined population of 575 million and a combined GDP of $US 1.8 trillion, making it one of the largest and most integrated regional organisations outside Europe. Although ASEAN has a lower profile than APEC, it does have a history of the successful harmonisation of laws - something that is absent in APEC.*
>
> *The Association of South East Asian Nations (ASEAN) has recognised that the absence of harmonised data protection legal infrastructure has the potential to become a barrier to cross-border trade and investment. Significant business opportunities in business process outsourcing may gravitate to jurisdictions with privacy protection that meet these requirements.*
>
> *ASEAN has committed to the establishment of an integrated ASEAN Economic Community (AEC) by 2015. A significant target within this commitment is the devel-*

[457] Chris Pounder, Why the APEC Privacy Framework is unlikely to protect privacy, http://www.out-law.com/page-8550 (last accessed 7 August 2015).
[458] Chris Pounder, Why the APEC Privacy Framework is unlikely to protect privacy, http://www.out-law.com/page-8550 (last accessed 7 August 2015).
[459] Chris Pounder, Why the APEC Privacy Framework is unlikely to protect privacy, http://www.out-law.com/page-8550 (last accessed 7 August 2015).

> *opment of a harmonised legal infrastructure for E-Commerce, as set out in the Roadmap for Integration of e-ASEAN Sector."*[460]

According to experts, ASEAN countries are among the most active ones in relation to data protection and privacy, mostly since 2010 to the present.[461] Between 2014 and 2015, countries like Thailand, Singapore and Vietnam were active in reforming or adding (Vietnam, Singapore) and enacting (Thailand) new legislation on data protection. In other countries, such as Indonesia, Malaysia, Philippines and Brunei, there were some activity recently but no big changes, while in Cambodia, LaoDR, Myanmar and Timor Leste, those developments were not significant.

3. Economic Commission for Latin America and the Caribbean (ECLAC)

In line with developments in many parts of the world, and fostered by the UN Economic Commission for Latin America and the Caribbean (ECLAC), Latin American and Caribbean countries launched an initiative in 2004 called Action Plan for the Latin American and Caribbean Information Society, known as eLac. The plan is a series of recommendations for governments to help the development of a sound environment for the use of technological tools in the region.

ELac has developed several work plans since 2005 where privacy and protection of personal data is included. These plans mention that the enhancement of a good environment for the growth of the information society must take into account the protection of personal data. It must foster dialogue and cooperation among governments on the issue, and develop adequate frameworks that address the challenges it poses.[462]

During the fifth Ministerial Conference on the Information Society held in México in September 2015, eLac presented its workplan until 2018, and a study "La Nueva Revolución Digital" (The New Digital Revolution), that present the challenges an opportunities for the region, and where privacy and data protection occupy an important place. In the study, Chapter E deals with online consumer protection and in point 4, there is a call to enhance data protection in Latin American and Caribbean countries. On challenges ahead for the digital economy, the study pointed out the need for new and modern regulation, and consumer

---

460 Chris Connolly, A new regional approach to privacy in ASEAN, October 2008, http://www.galexia.com/public/research/articles/research_articles-art55.html (last accessed 7 August 2015).

461 Graham Greenleaf, ASEAN data privacy developments 2014-2015, *UNSW Law Research Paper No. 2015-48* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2645702 (last accessed 10 December 2015)

462 See http://www.cepal.org/cgi-bin/getprod.asp?xml=/elac2015/noticias/paginas/4/44104/P44104.xml&xsl=/elac2015/tpl/p18f.sl&base=/elac2015/tpl/top-bottom.xsl (last accessed 7 August 2015).

protection is one of the axis of these new rules; specifically, consumer trust and confidence is outlined as a challenge.[463]
Finally, within the structure of the working groups of eLac there is one that will deal with consumer protection.

[463] CEPAL, The new digital revolution, August 2015. http://repositorio.cepal.org/bitstream/handle/11362/38604/S1500587_es.pdf?sequence=1 (last accessed 10 December 2015)

Chapter 3
Law in Practice: Current Issues, Challenges and Case-Law for the Enforcement of Laws and Regulations on Consumer Data Protection

A. Current Judicial and Administrative Issues of Consumer Data Protection in Brazil (*Prof. Dr. Danilo Doneda*)

I. Credit scoring

Credit scoring was deemed legal (REsp 1.419.697/RS) by the Brazilian Superior Court of Justice (STJ) as a method for risk assessment if consumer data is treated with transparency and good faith according to consumers' rights. The STJ recognized that the use of sensitive, excessive or incorrect information can generates

moral damage. Following the vote of Minister Paulo de Tarso Sanseverino, the STJ determined that the sole existence of an unfavorable score regarding a consumer does not justify compensation for moral damage. However, the use of sensitive and excessive information or a proven unjustified refusal of credit by the use of incorrect or outdated data can reasonably justify compensation to the consumer.

There are approximately 250,000 lawsuits in Brazil on the subject – 80,000 just in Rio Grande do Sul – where consumers seek to be compensated because of the scoring system (in some cases, because of the mere existence of the score). The thesis began to guide lower court judges who address the same issue.

The judges from the STJ had to establish whether the scoring system was, in fact, a database and, therefore, the application of Law No. 12.414 of 2011 (Positive Credit Information Law) was feasible. Judge Minister Paulo de Tarso stated that it is a mathematical formula that gets a certain credit risk score from consumer data, usually taken from databases available on the market. The Minister recalled that credit bureaus, such as SPC and Serasa-Experian, are regulated by the CDC and, subsequently, by Law No. 12.414 of 2011, that disciplined the treatment of positive credit information databases, highlighting the need for transparency of information, which should always be easy to understand, in order to protect the consumer's privacy and honor. On this matter, the Minister stated that the methodology itself is protected by business secrecy rules and does not need to be revealed.

However, the secrecy rules do not apply to the data when required for consultation by the consumer. Transparency duties must be provided with clarity and precision, including the specification that the consumer can rectify incorrect or outdated data in order to improve the performance of the score. Similarly, the minister considered transparency rules essential for the consumer to assess the possible use of sensitive information (e.g. social origin, skin color, sexual orientation), to prevent discrimination and excess (personal tastes).

1. Case

After the first special appeal[464] had been brought before the STJ, the *Núcleo de Recursos Repetitivos e Repercussão Geral (*NURER) from Rio de Grande do Sul's Court of Justice informed the STJ of more than 80,000 similar cases. The second special

[464] Special Appeal, *Recurso Especial* in Portuguese, is an exceptional appeal before the STJ against a decision contrary to federal law, international or regional treaty from a second Court of Justice. It is also used to unify jurisprudence or against a Court of Justice's decision contrary to established jurisprudence. Federal Constitution, Art. 105, III, a, b and c. Civil Procedure Code, Arts 541 and 546. Law No. 8.038 of 1990, Arts 26 to 29. STJ's Internal Rules, Arts 255 to 257.

appeal – Special Appeal No. 1.419.697/RS[465] – brought before the STJ faced the same company – Boa Vista Serviços S/A – and concerned the same object: consumer's inclusion on a credit scoring system is illegal and causes moral damages that generate monetary compensation.

Upon the receipt of five *amici curiae* petitions (from the Brazilian Central Bank, the National Confederation of Store Managers – CDNL, SERASA S.A., the Brazilian Bank Federation – FEBRABAN, and the Institute for Retail Development – IDV), Judge Paulo de Tarso Sanseverino called a public hearing with several interested stakeholders to better form his judgment regarding the controversy. Judge Paulo de Tarso Sanseverino stated in his sentence that he had no previous knowledge about the case and the credit system thus analyzed and the public hearing was of special importance to guide him when weighing the interests, stressing the novelty of data protection issues to the Brazilian juridical system. The decision identified seven main points.

2. Concept of credit scoring

The court defined credit scoring as a risk assessment system that operates through the association of a certain score to each consumer. "Scoring" is an English term that does not have a strict equivalent in Portuguese. It does not refer to a database, but instead to a mathematical method of assessing credit risk. Today, with the ease of access to several databases, especially considering the Internet, some companies, such as Boa Vista S/A, have developed statistical methods to evaluate a consumer based on a diverse set of variables and sources of data. Those variables are determined by the corporate experience:

> *O SCPC Score Crédito agrupa os consumidores em faixas de risco, tendo como parâmetro o comportamento médio esperado em termos de inadimplência baseado no histórico de informações de mercado compartilhadas em nossas bases. A pontuação do Score varia de 0 a 1.000 e indica menor risco para a concessão de crédito a medida que se aproxima de 1.000.*[466]

The appellant consumer in the case received a score of 553 and the company stated that no debit, protest or prosecutions were used to determine the score.

---

[465] Details and documentation of the case can be found in Portuguese through this link < https://ww2.stj.jus.br/processo/pesquisa/?src=1.1.2&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201303862850> (last accessed August 6, 2015).

[466] "SCPC Credit Score group consumers in risk groups, based on the expectancies of behavior related to the lack of solvency present in the information shared in our databases. This score's punctuation varies from 0 to 1000 and indicates that the lesser the risk, the higher the score." Special Appeal No. 1.419.697/RS p. 8.

3. Credit risk assessment in general contracts

The Judge describes the history of risk assessment before automatized systems were available and how it became an exploitable market. Therefore, during the elaboration of the Consumer Defense Code (CDC), in the 1990s, legal writing and regulation in Brazil were especially concerned with consumer credit databases.

4. Regulation of consumer credit databases in the Consumer Defense Code

Consumer credit databases are regulated in article 43 of the CDC. Article 43 encompass both debtors and credit protection databases.

The Judge notes that Art. 43 had a strong relation to consumer privacy, following an international inspiration, such as the North-American Fair Credit Reporting Act, ensuring decisions made through means of the data and information collected were informed, responsible and transparent. Again, the Judge brings in the European Directive 96/45/CE as an example of an international norm considering the protection of personal data as a fundamental right.

Art. 43, therefore, does not prohibit consumer credit databases, but established a set of rules to legitimize their use. The STJ settled jurisprudence recognizes this legality and the importance of clear rules for information databases:

> *the benefits are evident, fostering agility and security of commercial transactions, just as one cannot deny the seller the right to be informed about customer's credit, and to communicate with third parties data that it has.*[467]

Moreover, regarding the regulation of consumer credit databases, the decision recalls three *súmulas*, which are small entries by the court concerning settled jurisprudence or majority of understanding:

***Súmula* 323/STJ:** *A inscrição do nome do devedor pode ser mantida nos serviços de proteção ao crédito até o prazo máximo de cinco anos, independentemente da prescrição da execução.*[468]

***Súmula* 359/STJ:** *Cabe ao órgão mantenedor do Cadastro de Proteção ao Crédito a notificação do devedor antes de proceder à inscrição.*[469]

[467] Special Appeal No. 22.337/RS p. 25.

[468] The name of an individual who has not paid his financial duties can be kept in a credit protection database for a maximum of five years, even if no action can be proposed against him due to prescription.

[469] The credit bureau shall notify the individual who has not paid his financial duties before entering his name into a credit protection database.

***Súmula* 385/STJ:** [470]*Da anotação irregular em cadastro de proteção ao crédito, não cabe indenização por dano moral, quando preexistente legítima inscrição, ressalvado o direito ao cancelamento.*

5. Positive Credit Information Law (Law No. 12.414 of 2011)

The Positive Credit Information Law – Law No. 12.414 of 2011 – aims to regulate credit information systems, especially borrowers' payment histories. Under the CDC, there was no doubt about the lawfulness of recording "negative" data about a consumer, that is, information about consumer debts. There was, however, legal uncertainty about storing borrowers' payment histories ("positive information"). It was, therefore, important for the Credit Information Law to provide detailed regulations concerning credit information databases, thus, establishing a secure legal framework that simultaneously encourages data flow and protects personal data, as stated:

> *2. Initially, it must be highlighted that the creation of one's credit history conceives the gathering not only of debt information which is already legitimized by Consumer Defense Code, but also of due payment information ("positive information"), which did not have a clear legal framework for their use. With the collection and dissemination of fair credit information, one can benefit from fair credit information on the creation of the credit history. Thus, the credit and retail market could more efficiently differentiate good from bad payers, with the consequent reduction of credit risk per operation, which will reduce the costs linked to the overall credit expansion.*[471]

Upon bringing up the Positive Credit Information Law, although it does not recognizes "credit scoring" as a database, but as a calculus method, the Judge recalls some of the articles of the law which aim at consumer data protection through the establishment of the necessity and purpose principles and some rights such as access, information and deletion:

---

[470] There is no right to non-pecuniary damages if an undue inscription of an individual is made on a consumer credit database in a situation where there is a precedent rightful inscription.

[471] Free translation from Motivation of MP 518/2010, paragraph 2 – "Inicialmente, deve-se destacar que a formação do histórico de crédito de pessoas naturais e jurídicas permite o recebimento e o manuseio pelos bancos de dados não somente de informações de inadimplemento, hoje já permitido e disciplinado pelo Código de Defesa do Consumidor, mas também de adimplemento (informações "positivas"), que não apresentava um marco legal claro para sua utilização. Com a coleta e disseminação de informações sobre adimplemento, as pessoas poderão se beneficiar do registro de pagamentos em dia de suas obrigações, de modo a permitir a construção de seu histórico de crédito. Dessa forma, o mercado de crédito e de varejo poderá diferenciar de forma mais eficiente os bons e os maus pagadores, com a consequente redução do risco de crédito por operação, que permitirá a redução dos custos vinculados à expansão do crédito de uma forma geral."

8. Seeking to protect citizen's privacy and prevent the misuse of information, paragraph 1 of Art. 3 indicates that the stored information must be objective, clear, accurate and easy to understand, and necessary to assess the economic situation of the registered. In this sense, paragraph 3 of Art. 3 states that information deemed excessive or sensitive are prohibited from being stored

10. Art. 5 list the citizen's rights, such as:

(I) cancellation of the registration upon request;

(II) access, for free and at any time, to information about the

databases' existence, including ones credit history. The database controller must keep a secured, telephone or electronic, consultation system to inform the existence of fair credit information registered of a specific consultant;

(III) contest incorrect information and have their immediate correction or cancellation and the communication about the correction or cancellation to the databases which the information was shared

(IV) know the main elements and criteria considered for the risk analysis, with respect to business secret;

(V) previous information about the data stored, database controllers's identity, the purpose of the processing of personal data and the sharing of information;

(VI) request the review of the decision taken solely by automated means; and

(VII) have their personal data used only in accordance with the purpose for which they were collected

11. Strengthening the safeguards given to the registered, Art. 6 sets out obligations for the database controllers regarding the data subject's information right, such as a copy of the contract containing a summary of the subject's rights, as defined by law or infra-legal rules relevant to the process, and the list of government agencies to which the data subject can appeal when these rights have been violated.[472]

[472] Idem free translation of paragraphs 8, 10 and 11, respectively: 8. Buscando resguardar a privacidade do cadastrado e o uso indevido das informações, o § 1º do art. 3º estipula que as informações armazenadas devem ser objetivas, claras, verdadeiras e de fácil compreensão, e devem se restringir àquelas que sejam entendidas como necessárias para avaliar a situação econômica do cadastrado. Neste mesmo entendimento, o § 3º do art. 3º disciplina que as informações tidas como excessivas ou sensíveis estão proibidas de serem anotadas.
10. O art. 5º explicita ao cadastrado os seus direitos, como o de: (i) obter o cancelamento do cadastro quando solicitado; (ii) acessar gratuitamente, a qualquer tempo, às informações sobre ele existentes nos bancos de dados, inclusive o seu histórico, cabendo ao gestor destes manter sistemas seguros, por meio eletrônico ou telefone, de consulta para informar a existência ou não de cadastro de informação de adimplemento de um respectivo cadastrado aos consulentes; (iii)

6. Legality of the credit scoring system

Thus, undeniably, the Judge remarks "credit scoring" as a method to discriminate against good and bad payers, being a legal risk assessment in the credit market and not a database. Risk analyses are even laid down by Positive Credit Information Law in its Arts 5 and 7.

7. Limitation: privacy and transparency

A credit scoring system must respect the fundamental right to privacy foreseen in the Brazilian Constitution in Art. 5, X, and personality rights established in the Civil Code, Arts 11 to 21. The Judge calls them "essential rights" or natural rights according to the Declaration of the Rights of Men and the Citizen from 1789. The decision states that privacy or intimacy violations occur when facts or data are accurate or true, but represent a trespass of the individual's private sphere.

The CDC sets a variety of principles, two of them very important for the credit scoring system: transparency and good faith.[473] Transparency is seen here as clear and correct information about the process, and good faith as a general interpretation clause for contracts. A combination of both CDC and Positive Credit Information Law establishes a micro privacy system stating a set of rules for the credit scoring system:

a) duty of truth;
b) duty of clarity;
c) duty of objectiveness;
d) prohibition of use of excessive information; and
e) prohibition of use of sensitive information.

---

solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter sua imediata correção ou cancelamento e comunicação aos bancos de dados para os quais houve compartilhamento da informação;
(iv) conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;
(v) ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento;
(vi) solicitar a revisão de decisão realizada exclusivamente por meios automatizados; e
(vii) ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados
11. Reforçando as garantias dadas ao cadastrado, o art. 6º estabelece obrigações aos gestores dos bancos de dados no fornecimento de informações àquele, com destaque para a cópia de texto contendo sumário dos seus direitos, definidos em lei ou em normas infralegais pertinentes à sua relação com bancos de dados, bem como a lista dos órgãos governamentais aos quais poderá ele recorrer, caso considere que esses direitos foram infringidos.

[473] CDC, Art. 4, caput and III.

Although a *credit scoring* system is not a database within the scope of the Positive Credit Information Law, it must comply with information and transparency rules about collection, use and sharing of data with respect to industrial secrecy. In addition to that, even though previous consent is not mandatory, other control and limitation aspects of the use of personal data established in the CDC and Positive Credit Information Law must be respected.

If it can be proved that sensitive, excessive, incorrect, or outdated information were used, the organization responsible, the data source and the consultant are objectively and jointly liable for material and moral damages caused to the consumer under Art. 16 of the Positive Credit Information Law.

8. Moral damages

The sole fact, however, of giving an unsatisfactory score to a consumer does not entail, in itself, a moral damage. An unsatisfactory score should only create opportunities for consumers to obtain clear information about the data used in this statistical system. However, if the score derives from excessive or sensitive information in violation of the consumer's honor and privacy, there will be moral damage

II. Consumer rights violations databases

There is no specialized database on consumer data violations. Nonetheless, there are two databases about consumer rights violations that are worth mentioning.

1. Sindec

The National Consumer Secretariat at the Ministry of Justice (Senacon/MJ) was created in 2012 by Decree No. 7738 of 2012. The Senacon/MJ's main lines of action focus on planning, coordinating and implementing the Plandec of the National Consumer Affairs Policy, with the following objectives: (i) ensure the protection and defense of consumer rights, (ii) promote harmonization in consumer relations, and (iii) encourage the integration and joint action of members from the SNDC. Among the fundamental actions of the secretariat highlight worth mentioning is the National Consumer Protection Information System (Sindec). This is an information system that integrates and consolidates information from more than 200 Consumer Protection and Defense Bodies (Procons) from 25 units of the Federation's municipalities. Such information is structured as an open-source quantified and qualified sample of the various demands and complaints from consumers taken daily at those consumer protection bodies. This national database can be seen as a valuable source of information concerning consumer complaints and violations from all sources, being the main and the most personal

source of what drives consumers to complaint and what they identify as violations of their rights.

2. Consumidor.gov.br

The Senacon/MJ is also responsible for the management, provision and maintenance of Consumidor.gov.br, in collaboration with other bodies and agencies of the SNDC, through technical cooperation, support and work.

The Consumidor.gov.br is a new public service created in 2014 to work around consumer disputes through the Internet, and it allows direct dialogue between consumers and businesses. This is a technological platform for information, interaction and sharing of data, monitored by the Procons and Senacon.

The Consumidor.gov.br database on complaints is not only limited by the time of implementation, but also by scope; since it is a voluntary service provided and maintained by the government, with an emphasis on interactivity between consumers and businesses to reduce consumer disputes, the participation of companies in Consumidor.gov.br is permitted only to those who adhere formally to the system.

In an overall analysis of Sindec's database, no records of violation of consumer data or privacy complaints could be tracked, for a variety of reasons, the most crucial of them being the difficulty and the bureaucracy involved in filing such a complaint in a Procon. A shift of the complaint profile can be observed with the automated instant way of complaining provided by the consumidor.gov.br system: consumers who would not go to Procon use this system and complaints that did not arrive at the Procon bureaus because of a lack of benefits in comparison to the inconveniences can be registered. Nowadays, complaints focused on the consumer's perception of a violation of their privacy and data rights arrive at Consumidor.gov.br when related to the companies part of the system.

Research based on the key words "data," "information" and "personal" revealed 32 consumer complaints based on consumer data protection since Consumidor.gov.br was implemented in 2014 and the January of 2015. The most current claim related to personal data harm among consumers who visited consumidor.gov.br is about the sharing of data to third parties which consumers can or cannot identify. Two cases are worth mentioning:

a. Wal-Mart

During last year's Black Friday sales promoted by *Wal-Mart*, several consumers purchased a variety of products and, after paying for them, received a message with the cancellation of their purchase from a third party company, named Tecno Ferramentas, saying the sale was a system failure and they had canceled the prod-

uct. This was a surprise to all the customers that did not know that *Wal Mart*'s website was a platform for third party offers.[474]

b. Internet connection services

A particular case has reached Procon's offices. After contracting an Internet connection service, many consumers received calls from Internet Service Providers (ISPs) stating they also needed to contract an ISP service in order to have Internet connection. This happened mainly with the custumers of a major Brazilian telecom company, "Oi," contacted by the ISP UOL.[475]

The sharing of personal data without the consumer's consent due to the lack of transparency and information asymmetries is the harm most acknowledged by consumers. The lack of information and transparency regarding the sharing of credit and paying information between banks and credit bureaus is the second highest rated group of consumer claims at Consumidor.gov.br (13%). Incorrect data and the collection of data without a purpose or excessive to the performance of the service pair occurred in 6% of the cases. Consumers who identified that the data was excessive or not serving the purpose did not identify the problem specifically in these terms; instead, they already sensed the possibility of the harm of sharing those kinds of information, as one of the reports states.[476]

474 "I purchased directly at walmart.com.br on November 29, 2014 and paid the bill of R $ 175.21 on December 1, 2014. I got a call from Tecno Ferramentas, asking me to cancel the purchase and I am surprised to know that even without my authorization, the cancellation was made. I'm concerned to know that my personal data was transferred to another store without my knowledge."

475 "I would like to record here my indignation with this service provider that provides our personal data to third party companies without even contacting the customer that they would like to switch provider. On October 31, 2014 I called Oi requesting to increase the speed of my Internet connection but I was told that there was no technical feasibility and they told me to give my data so that they could contact me to warn about the availability. The next day, they called me saying they would increase my speed and they would charge only R$ 15.00 in my monthly bill and R$ 24.90 on my credit card. At first I thought it was strange then I came to believe I felt into a scam after seeing complaints on the Internet about this case and saw that I just signed a contract with a provider that does not provide me increase of my Internet speed but charge me for services I get for free on the Internet."
"On September 22, I received a call from UOL saying that to hire VELOX I would have to hire that provider. I found out that this is a lie by contacting Oi. But then I asked: Who gave my information to UOL and said that I was hiring VELOX?"

476 "Good afternoon, my friends. I'm getting text messages from Bradesco to return a call, when I do, they want my personal data, like CPF full name, and they do not tell me the purpose of the call and I'm afraid, because it is my personal data. The only connection I have with the bank is a credit card from Casas Bahia that I pay every month, religiously."

B. Current Consumer Data Protection Issues Before Chinese Tribunals *(Prof. Dr. Zhou Hanhua)*

The following examples of current case law on data protection aim to provide a broad overview of judicial disputes that are related to the protection of customers' personal information before Chinese courts.

I. Civil claims

The *Law on the Protection of Consumer Rights and Interests (Consumer Protection Law)* of 2014 makes business operators responsible for protecting customers' personal information. However, it remains difficult for consumers to bring lawsuits in cases of violations of personal information, mainly because of the need to provide sufficient evidence and because of the significant lawsuit costs. To date, only few customers have thus chosen to bring civil claims to protect their rights. This section presents a series of civil litigation cases concerning the protection of customers' privacy rights and personal information, organized in three categories: (1) collection and use of personal information; (2) disclosure and release of customers' personal information; (3) illegal transmission of junk short messages.

1. Illegal collection and use of personal information

This category of infringements refers to the collection and use of customers' personal information without their prior consent or in violation of relevant laws and regulations. One example is the case of Zhu Ye v. Baidu, where the defendant operated an online search engine. The claimant realized that when he was looking for terms such as "lose weight, chest enlarge, artificial weight reduction", related advertisements would pop up on some websites he was visiting. The defendant did not inform the claimant in advance that it was using its technology to collect and use the key words for advertising purposes. Therefore the claimant demanded that Baidu discontinue this practice, apologize and offer compensation. The People's Court in the Gulou District of Nanjing held that Baidu was using Internet technologies to record and track the key words used by Zhu Ye and employed personal information associated with his work, hobbies, interests and personal characteristics by showing advertisements on some websites that matched the recorded key words. According to the judgment, personal IDs, addresses, phone numbers, as well as a citizen's private activities form part of the right to privacy.[477]

[477] (2013) No. 238 civil case in Nanjing, final trial http://js.xhby.net/system/2014/10/31/022392631.shtml.

This judgment is of great significance, as in times of modern technology and information people can hardly avoid sharing private information with network service providers when using the Internet.

2. Disclosure and illegal release of customers' personal information

The disclosure and illegal release of customers' personal information is the most frequent type of infringement upon customers' privacy and personal information by business operators. It occurs mainly in three situations: (1) operators provide the customers' information to third parties; (2) operators fail to fulfill their obligation of confidentiality, which leads to the leaking of personal information; (3) operators fail to take measures when the leakage of customers' personal information has occurred or is likely to occur. In accordance with the new *Consumer Protection Law*, operators are obliged to protect customers' personal information that has been collected with customers' consent. As examples from judicial practice, the following cases will be analyzed in further detail: Sun Weiguo v. China United Network Communications Limited Shanghai Branch, and Zheng Yang v. Tianjin Airline Ltd. and Zhejiang Taobao Ltd. are both related to the issue of providing personal information to a third party; Wang Jinlong v. Hanting Hotel Management Co. Ltd. concerns the leakage of personal information; and Yan v. Sina.com and Baidu is related to violations of the right to reputation and operators' failure to adopt necessary measures to prevent such infringements.

Sun Weiguo v. China United Network Communications Limited Shanghai Branch

The case of Sun Weiguo v. China United Network Communications Ltd. Shanghai Branch relates to a dispute on illegally providing personal information to a third party. In 2002, the claimant registered as a mobile phone client at China Unicom Ltd. Shanghai Branch, the predecessor of the defendant (hereafter referred to as Shanghai Unicom). The registration required his personal information (account name, mobile phone number, postal code and contact number). In 2008, the claimant received a call from a service specialist of Shanghai Unicom, offering him free public transportation accident insurance from the AEGON-CNOOC Life Insurance Company. After receiving detailed information about the insurance, he gave his birth date and address and agreed to the service. Later, the claimant received a letter containing a special guarantee of the Financial Management Club of China Unicom Shanghai Branch, in which an insurance certificate listed the claimant's date of birth, ID number, the service phone number of the specialist offering the insurance, and so on. Then, the claimant found out that although Unicom Xinguoxin Communications Co. Ltd. and China United Network Communications Limited were different legal entities, the Unicom Xinguoxin Communications Co. Ltd. Shanghai Branch (hereafter referred to as Xinguoxin Shanghai Branch) and the customer service department offering the insurance service be-

longed to the same group. The People's Court of Pudong New Area held that the right to privacy constitutes a basic personal right and should be included in the category of personal rights protected by law. In order to enjoy privacy, a natural person owns the right to pursue a peaceful life undisturbed by others. Other persons are not allowed to collect, utilize, and disclose private information in violation of the laws and regulations, or without the right holder's permission. Personal information constitutes the major component of the privacy right, including a person's name, gender, occupation, educational background, contact information, family address, marital status, and so on, which are all closely associated with a person and his or her family. In this particular case, the Court held that the defendant had the obligation to assume the responsibility of confidentiality and should neither disclose the information offered by the claimant to any third person or third party, nor exceed the purpose of collection as accepted by the claimant. However, the defendant had provided the abovementioned information to the Xinguoxin Shanghai Branch without prior consent by disclosing the private information it had acquired. According to the Court, this constituted an infringement of the claimant's right to privacy. However, as it did not result in any severe disturbance for the claimant and the confidentiality measures adopted by the defendant meant that the claimant's information was known only to a limited number of persons, the Court rejected the plaintiff's demand for monetary compensation. China United Network Communications Limited Shanghai Branch apologized in written form to the claimant.[478]

Zheng Yang v. Tianjin Airline Ltd. and Zhejiang Taobao Ltd.

In 2014, the claimant bought a flight with Tianjin Airline Ltd. (hereafter referred to as Tianjin Airline) via Tmall, an online shopping platform affiliated with Zhejiang Taobao Ltd. Later he received a message according to which the flight had been cancelled, stating that he should contact the number of Tianjin Airline's customer service department. When he called the customer service department using the number given in the message, he was told that only a refund could be arranged, and that he would have to provide his bank account number. During the conversation, the claimant began to have doubts regarding the authenticity of the flight cancellation. He discovered that no cancellation had actually occurred. The claimant thought that only Taobao and Tianjin Airline knew about his personal information and flight booking, and that one of them had leaked his information. He decided to bring a lawsuit demanding that Taobao and Tianjin Airline apologize to him, compensate him for his losses and cover the litigation costs.

The People's Court of Lidong District in Tianjin held that the claimant had failed to submit the necessary evidence with regard to the defendants' responsibil-

[478] (2009) No. 9737 civil case at the New Pudong Area of Shanghai, first trial.

ity, as, according to the Court, they were not the only institutions that possessed the information. As the claimant had received a message from a stranger who was most likely involved in a fraudulent crime, the Court doubted whether the personal information had indeed been leaked by the defendants.[479]

Wang Jinlong v. Hanting Hotel Management Co. Ltd.

In this case, the claimant was a customer of the Hanting Hotel. When he booked a room at the hotel in 2012, he provided his personal information (ID card and mobile phone number) according to the hotel's requirements. In 2013, WooYun.org, a domestic third-party loophole report platform, published the customer check-in records of several hotels, revealing that the hotel wireless authentication portal system developed by the Huida Network Company had systematic loopholes, causing the leakage of customer information. Shortly afterwards, a data package including 20 million check-in records and a website for browsing the check-in records of customers based on the data package appeared on the Internet. The claimant downloaded the package and found his own name, ID card number, birth date, address, mobile phone number, date of check-in, and so on. Later, the claimant also discovered that the same information was accessible via search key on the website. When the claimant received unsolicited promotion advertisements and junk messages, he lodged a lawsuit before the People's Court of Pudong New Area, claiming that his personal information was leaked by Hanting Hotel.

The People's Court of Pudong New Area had to decide firstly whether the 20 million check-in records contained the information that the claimant used when he was booking the room at the Hanting Hotel, and secondly whether the defendant had leaked the personal information of the accuser, thereby infringing upon his right to privacy. With regard to the first issue, the Court compared the check-in information package with the information recorded by the Hanting Hotel Management System and Membership Management System. Although the claimant's name, gender, ID card number and date of birth were identical in the two sources, the check-in date, accuser's mobile phone number and address were different. Due to the inconsistencies regarding the information registered by the hotel and the personal information leaked, the Court held with regard to the second question that the claimant could not prove that the hotel was the origin of the leaked information. Therefore the Court rejected the claim.[480]

[479] (2014) No. 1720 civil case at Dongli district of Tianjin, first trial.
[480] (2014) No. 501 civil case at the New Pudong Area of Shanghai, first trial.

Yan v. Sina and Baidu

Two unknown bloggers published an article related to the claimant's privacy on the Sina and Baidu blogs. Baidu, after receiving notification of the defendant's wish to have the article deleted, took the article off the blog. Sina did not do so. The claimant sued the two companies for the alleged violation of his right to privacy. In addition, he demanded that the Sina blog disclose the bloggers' identity. The People's Court of Haidian District in Beijing held that Sina had failed to fulfill its obligation to offer the claimant the option of having the article deleted and its obligation to provide effective complaint channels, while Baidu had provided complaint mechanisms for the claimant. With regard to the plaintiff's demand to be given the bloggers' IP addresses and registration information, including their name, address and contact information, the Court took into consideration the content of the article published by the two bloggers and the claimant's right of personality and right to be informed of the personal information of the two bloggers in order to act against them. Therefore the Court held that Sina should disclose the associated information concerning the aforesaid two bloggers within the scope of its technological capability in order to maintain and protect the accuser's lawful right to protect himself. [481]

These cases show that customers have begun to take judicial action to protect their right to privacy. However, due to insufficient knowledge of the relevant laws and regulations, obstacles continue to hamper the protection of consumers' right to privacy and personal information. The success of Sun Weiguo in suing China United Network Communications Limited Shanghai Branch seems fortunate, as the two defendants, Shanghai Unicom and Xinguoxin Shanghai Branch, used the same customer service telephone number, which allowed the claimant to prove that the defendants were illegally disclosing his personal information. As regards the cases of Zheng Yang v. Tianjin Airline Ltd. and Zhejiang Taobao Ltd. and Wang Jinlong v. Hanting Hotel Management Co. Ltd., these cases show that customers' difficulty in finding evidence is one of the biggest obstacles to the protection of their right to privacy. In these two cases, the burden of proof rested on the customers. The cases show the following difficulties: first, the customers have to prove that the leaked information is identical to that shared with the business operator; second, they have to prove the uniqueness and exclusiveness of the channels through which the information is leaked, that is, they must prove that no other possible leakage channels exist; third, customers have to prove that they have indeed suffered losses due to the information leakage. Regardless of the amount of money, technology and energy invested, the customer is undoubtedly at a disadvantage. Therefore, most customers choose to remain silent when they find out that their personal information has been leaked. The case of Mr. Yan v.

[481] http://www.chinacourt.org/article/detail/2014/10/id/1456192.shtml.

Sina and Baidu related to the infringement of rights to reputation and privacy, clearly defining the business operator's responsibility for the protection of customers' personal information. In particular, it emphasizes how important it is for business operators to take necessary action in the event of a possible personal information leakage or infringement upon the privacy of customers.

3. Sending electronic advertisements without customers' prior consent

In the case of Li Meijia v. China Telecom Corporation Limited Leshan Branch (hereinafter referred to as China Telecom Leshan Branch), the claimant became a mobile phone client of the defendant in 2011. Between March and April 2013, the defendant sent ten short messages about its products via its customer service phone number, which is the SMS platform and direct gateway channel of China Telecom Leshan Branch. It is only possible to send short messages to the mobile terminals operated by Leshan Branch and belonging to the value-added telecom service. From May to August 2013, the defendant sent 18 short messages about the opening of mobile phone shops and product promotions to the claimant's mobile phone. Therefore the claimant brought an action before a court, asking the court to declare that China Telecom Leshan Branch had violated his right to health, privacy and property.

The judgment of the Court of first instance, which was affirmed by the appellate Court,[482] held that the right of privacy relates to the right of personality, which includes a natural person's right to control his or her own personal information, private activities and private sphere, including the right to enjoy a peaceful life, the right to the freedom of controlling his or her private activities, and the right to protect his or her private sphere from interference. In the view of the Court, when mobile phone users choose to use the short message service, they have no way of controlling the transmission of the short messages, but can only choose to view or not to view them. Each time a user's mobile phone receives a short message, the phone will inform them in one way or another, for example by ringing or vibrating, which is likely to impact upon users' everyday life and work. Failure to delete them in a timely manner will clutter the mailbox with messages, thus disturbing the normal sending and receiving of messages. Although receiving short messages is totally free, the incessant sending of commercial advertisements in a short period of time by China Telecom Leshan Branch to the claimant's mobile phone affected his well-being and right to privacy to a certain extent, that is, his right to enjoy a peaceful life, freedom to control his own personal activities and protect his private sphere from disturbance.

However, the Court disagreed with the argument that the claimant had suffered any loss of property or severe mental damage. With regard to the alleged violation of the right to property, the Court held that even though the acts of

[482] (2013) No. 1109 civil case in Leshan, Sichuan province, final trial.

receiving, clicking, viewing and cancelling those undesired short messages to some extent consume the mobile phone's resources, the mobile phone short message service also includes the notifications of other businesses and private short messages, and the resources and electricity of mobile phones will also be consumed in the standby mode, no matter whether the user is receiving messages or not. Based on this consideration, the Court rejected the plaintiff's claim that the defendant had violated his right of property. The Court did not support the alleged violation of the claimant's right to health due to lack of evidence. With regard to the claimant's demand for RMB 0.5 compensation for mental damage, Article 8 of the *Judicial Interpretations of Several Questions on Mental Damage Compensation in Civil Infringement Cases* issued by the Supreme People's Court stipulates that "the victim's demand for the compensation of mental damage caused by infringement but not resulting in serious consequences is not supported." Therefore, the Court did not endorse the claimant's demand for compensation. The Chinese laws and regulations have clearly pointed out that only in the case of grave consequences can a victim request compensation for mental damage. However, this view might cause problems for legal claims and discourage individuals from bringing lawsuits to protect their lawful rights. Finally, the Court also ordered the defendant to immediately stop sending short messages containing commercial advertisements to the claimant.

4. The boundaries of the legal protection of privacy

In the case of Wang Weining v. Yunnan Telecom Group Kunming Branch (hereinafter referred to as Kunming Branch), the claimant signed a contract on the provision of telecommunication services with the defendant. Later, the defendant used the claimant's phone number for his caller ID service without his permission. Therefore, after attempts to resolve the dispute between the parties had failed, the claimant lodged a complaint requesting that a court determine that the claimant had the exclusive right to use and control the phone number. The People's Court of Panlong District in Kunming, Yunnan Province, held that the right to privacy fell into the category of a personal right. It argued that Chinese law does not establish the right to privacy separately and that the protection of citizens' personal rights is limited to four categories (the right to one's name, the right of one's own portrait, the right to reputation and the right of honor). However, according to the judicial interpretations of the Supreme People's Court, the right to privacy can be subsumed under the right of honor, which is violated in cases of publishing other people's private information verbally or nonverbally, defaming them or damaging their reputation. However, with regard to the present case, the Court considered that the claimant had failed to submit sufficient evidence to prove that the defendant's behavior had caused him damage. The appellate Court reasoned that the right to privacy includes the right to enjoy a peaceful life and to keep personal information and communications secret, referring to the Chinese constitution

which protects citizens' freedom of correspondence and privacy of correspondence. Therefore, in the view of the appellate Court, personal phone numbers form part of personal privacy. The current laws, regulations and judicial interpretations related to the protection of privacy provide for the right of reputation. However, although the right to privacy is related, it goes beyond the right to reputation, right of portrait, right to one's name. Under certain circumstances, the infringement upon the right to privacy may implicate a violation of victims' reputation, but differences between these two rights remain. The Court considered that the laws and regulations concerning the protection of the right to privacy contain certain limitations. With regard to the dispute, the Court held that the telecommunications operator contacted a huge group of telecom users, and thus could not know in advance which users wanted the caller ID service and which ones wanted their phone number to be shielded. Both parties established a relationship of communication in which their rights and obligations were not equal. Hence, the use of the caller ID service did not constitute an infringement of the right to privacy.

II. Criminal justice

In accordance with Article 253 of the Chinese *Criminal Law*, the criminal offences involving infringements upon personal information can be divided into two categories: the crime of selling and illegally providing the personal information of citizens, and the crime of acquiring citizens' personal information through illegal methods. These crimes can be analyzed according to four different aspects: (1) acquiring personal information; (2) selling and providing citizens' personal information; (3) criminal means of illegally acquiring citizens' personal information; (4) the existence of aggravated circumstances.

1. Acquiring personal information

The Case of Lai Illegally Acquiring the Personal Information of Others

Between March 2006 and June 2009, Lai dedicated himself to debt collection, tracking and searching for evidence on extramarital affairs, and other activities relating to acquiring the personal information of others. For this purpose, he repeatedly bought personal information from Zheng Xiangjun, a junior officer in the security department of Jinshan District in Shanghai, as well as information concerning occupied hotel rooms. The People's Court of Pudong New Area in Shanghai held that citizens' personal information includes their name, occupation, title, age, marital status, educational background, work experience, family address, telephone number, credit card number, fingerprints, login account number and password, medical records, and personal records, as well as information on their

movements (e.g. information concerning checkins and checkouts in hotels). Information indicating the whereabouts of a citizen is more related to citizens' privacy and personal safety than names, family addresses, telephone numbers, and so on. The Court sentenced the defendant to one year's imprisonment and a fine of RMB 20,000.[483]

The Case of Zhang 1 and Zhang Illegally Acquiring Mobile Phone Position Information

From June 2011 onwards, Zhang 1 and Zhang, the two defendants, had acquired other people's mobile phone position information by paying the upstream seller, and then sold the information to interested persons. The People's Court of Sihong County in Jiangsu province dealt with two issues in this case: firstly, whether the mobile phone location information falls under the personal information protected by the *Criminal Law*; and secondly, the aggravated circumstances of illegally acquiring citizens' personal information. With regard to the first issue, the Court argued that the mobile phone location information is closely related to citizens' personal information and therefore within the scope of protection of the *Criminal Law of the People's Republic of China*. As to the second issue, the Court considered as aggravated circumstances of the case the following elements: to acquire the information of more than one person and repeatedly; to cause serious economic damage to or severe impact upon the citizens' everyday lives; to negatively impact upon national security and social livelihood; to use the acquired personal information for criminal activities. The Court sentenced Zhang to one years' imprisonment and two years' probation and a fine of RMB 12,000, and Zhang to nine months' imprisonment and one year's probation and a fine of RMB 10,000.[484]

The Case of Xu Zeru Illegally Providing Citizens' Personal Information

Xu Zeru, one of the defendants and Deputy Director of the Office of Teaching Affairs at Wansheng High School, illegally sold the personal information of 301 students registered for the college entrance examination, including their names, registration numbers, ID card numbers, telephone numbers, examination results, and so on to Li Wensong, the second defendant. The People's Court of Dongpo District in Meishan held that personal information refers to all information capable of identifying persons, including their names, occupations, titles, ages, marital status, nationality, educational background, academic degrees, professional qualifications, work experience, addresses, telephone numbers, Internet login names and passwords, ID card numbers, electronic signatures, fingerprints, and so on. Ac-

[483] (2009) No. 2728 criminal case in Pudong district, Shanghai, first trial.
[484] (2012) No. 0506 criminal case in Sihong county, Jiangsu province, final trial.

cording to the *Regulations on the Affairs of the Uniform National Examinations for the Colleges and Universities in 2012*, the examination information includes the student information, examination districts, examination sites, examination room arrangements, test information, evaluation, examination results, honesty, and so forth. The examination information is published only by the Ministry of Education or the provincial student recruitment and examination institutions, and organizations or individuals are not allowed to publish or leak such information. Therefore, the Court argued that the examination results of students, their ID card numbers, examination card numbers, telephone numbers, selected schools, and so on were personal information protected by the *Criminal Law*, and condemned Xu Zeru to eight months' imprisonment and a fine of RMB 5000 for the crime of illegally selling citizens' personal information, and Li Wensong to eight months of imprisonment and a fine of RMB 5000 for the crime of illegally acquiring citizens' personal information.[485]

The Case of Tan Haodong Illegally Acquiring Citizens' Personal Information

In 2012, Tan Haodong, the defendant, learnt from Huang Xi, another defendant, how to download and operate software to steal flight information, and used this to acquire citizens' personal information and sell it. The People's Court of Yizhang County in Hunan province held that the defendant Tan Haodong played a leading role and should be viewed as the author of the crime, while defendant Huang Xi, by teaching Tan the method of committing this crime, but without participating actively in it, should be considered as an accessory and therefore given a lighter sentence. Accordingly, the Court condemned Tan Haodong and Huang Xi to one year's and to seven months' imprisonment respectively, as well as to a fine of RMB 30,000 for illegally acquiring citizens' personal information.[486]

Analysis and Conclusion of Cases

These four typical cases show that case law defines personal information mainly by taking into consideration the following criteria: (1) the information refers to the specific characteristics of a citizen to identify his or her personal status; (2) citizens are usually unwilling to make this information publicly accessible; (3) the information is valuable enough to be protected by citizens, and the leakage can cause damage to the rights of the citizens; (4) the information is related to citizens' privacy, personal safety and social stability.

[485] (2012) No. 303 criminal case of Dongpo district, Meidong, first trial.
[486] (2013) No. 111 criminal case in Yizhang county, Hunan province, first trial.

2. Selling and illegally providing citizens' personal information

According to Article 253 of the *Criminal Law*, the crime of selling and illegally providing citizens' personal information can be committed, in particular, by the staff of government agencies and by employees of financial, telecommunication, transportation, educational and medical institutions. The interpretation of this offence is not really controversial. For example, in the case of Hang selling citizens' personal information,[487] Hang took advantage of his post as administrator of the electronic archives in the Shanghai Administration of Industry and Commerce Minhang Branch to sell information related to the company and citizens' personal information; in the case of Deng selling citizens' personal information,[488] Deng used his job in a telecommunications company to illegally acquire a detailed call list of users and their ID registrations, sending it to other people; in another case involving Wang Shijie selling citizens' personal information,[489] Wang was a member of the Passenger Transport and Marketing Committee of China Eastern Airlines; he downloaded and sold over six million pieces of Eastern Miles customer information without authorization. In the case of Zhou selling citizens' personal information,[490] Zhou took advantage of his job as statistical clerk at the Airport Shuttle Bus Joint Management Office of Beijing Civil Aviation, and sold the personal information of 2060 persons who applied for airport shuttle bus boarding cards; in the case of Xie Xinchong selling citizens' personal information,[491] Xie used his position within the mobile phone location business endowed by China Mobile Beijing Ltd. to provide information to other people on various occasions; and finally, in the case of Xu Zeru illegally providing citizens' personal information,[492] Xu provided the students' personal information to other people.

However, the question of whether the acts of employees in organizations other than those mentioned in Article 253 of the *Criminal Law* should be considered as constituting the crime of illegally acquiring citizens' personal information or selling and illegally offering citizens' personal information has been treated differently by courts, as the following three examples will show.

[487] (2013) No. 1123 criminal case at Minxing district, Shanghai, first trial.
[488] (2011) No. 672 criminal case at Changning district of Shanghai, first trial.
[489] (2013) No. 860 criminal case at Changning district of Shanghai, first trial.
[490] (2010) No. 496 criminal case at Chaoyang district of Beijing, first trial.
[491] (2011) No. 487 criminal case in Shanghai, final trial.
[492] (2012) No. 303 criminal case in Dongpo district of Meidong, first trial.

The Case of Zhong Donghang Illegally Acquiring Citizens' Personal Information

Defendant Zhong Donghang, an employee of the Guihai Dongmeng store of Beijing BHG Supermarket in Fangchenggang and responsible for the maintenance of Internet technologies, used his position to log into the internal network of Beijing BHG Supermarket and copy more than 300,000 pieces of private information of users in the northern areas of Guangxi to his own PC, and subsequently sold part of this information to another person. The People's Court of Gangkou District of Fangchenggang, Guangxi Zhuang Autonomous Region, qualified Zhong Donghang's act as illegally acquiring citizens' personal information.[493]

The Case of Wang Selling Citizens' Personal Information

In May 2011, defendant Wang joined a company in Huizhou; his job was to fill in freight notes. In June, Wang met Zhu through online chatting, and agreed to sell the freight note information to Zhu at the price of RMB 20 for each note. From June to July 2011, Wang sold over 750 pieces of freight note information (including the number of the respective freight note, names, addresses, recipients' contact information, names and prices of goods) to Zhu by QQ (an online chatting platform) and Fetion (mobile phone service) and was paid over RMB 15,000. The People's Court of Huangpu District in Shanghai held that defendant Wang had committed the crime of selling citizens' personal information and gave him a suspended sentence of one year and two months and fined him RMB 2000.[494]

The Case of Chen Selling Citizens' Personal Information

Defendant Chen, director of the sales department of Grand Byland Residential Area in Wujiang District, Suzhou, used his position to acquire and copy the personal information of owners in this residential area (names, room numbers, contact information, and so on). Afterwards, Chen sold the information to Bai Xiangyang, who was working for the Wujiang Branch of Guangzhou Yingtai Decoration Co. Ltd. The People's Court of Wujiang District in Suzhou held that defendant Chen, as an employee of a real-estate company, had committed the crime of illegally selling citizens' personal information. With regard to the argument that the defendant's act did not constitute the key component of the crime and that his behavior moreover did not reach the level of a grave circumstance, the Court considered that the organizations or their employees selling the information acquired about citizens' privacy to other people are characteristic of the offence of

[493] (2013) Now. 149 criminal case in Gangkou district of Fangchenggang, Guangxi province, first trial.

[494] (2012) No. 1177 criminal case in Huangpu district of Shanghai, first trial.

selling citizens' personal information. In addition to the state agencies or financial, telecommunication, transportation, education or medical institutions, the subjects of the crime also included the employees of other enterprises and public institutions who had the opportunity to acquire citizens' personal information. As to whether the circumstance of selling citizens' personal information was serious or not, the Court took into account several factors, such as the number of acts, quantity of information, and means and amount of unjustified benefits. In this case, Chen, the defendant, sold 232 pieces of citizens' personal information (including citizens' names, room numbers and contact information), gained RMB 800, and acquired a large quantity of information, which was made available to and used by other people, thus entailing serious consequences.[495]

Analysis and Conclusion of Cases

These cases show that author of the crime of selling and illegally offering citizens' personal information can be any employee of government agencies or private companies. However, in the case of Zhong Donghang illegally acquiring citizens' personal information, Zhong used his position as the employee of a supermarket, which is not referred to explicitly among the five sectors of organizations listed in Article 253 of the *Criminal Law*. That interpretation is erroneous, as the list of sectors contained in Article 253 is not exhaustive, as the expression "in particular" shows. Therefore, in the two cases of Wang and Chen selling citizens' personal information, the courts extended the interpretation concerning the scope of the subjects of the crime of illegally providing citizens' personal information, and held that all employees of enterprises and public institutions who illegally collect citizens' personal information during their work and service can be authors of the crime of selling and illegally providing citizens' personal information.

3. Criminal means of illegally acquiring citizens' personal information

With regard to the crime of illegally acquiring citizens' personal information, Article 253 of the *Criminal Law of the People's Republic of China* stipulates that the act of stealing or acquiring citizens' personal information by other unlawful means should be deemed as constituting the crime of illegally acquiring citizens' personal information. However, it fails to explicitly and precisely define what is meant by the expression "by other unlawful means". In practice, a variety of means of acquiring citizens' personal information exists, and some means do not seem unlawful as such, such as purchasing citizens' personal information from the Internet. The act of purchasing as such is not illegal, but it is still deemed illegal according to the established case law, as a subjective approach is applied by judicial authori-

[495] (2013) No. 0670 criminal case in Wujiang district of Suzhou, first trial.

ties when determining whether the author's means of acquiring citizens' personal information have violated the laws.

The Case of Zhang and Yang Illegally Acquiring Citizens' Personal Information

Defendants Zhang and Yang rented a floor in a building in Pudong New Area, Shanghai. From March 2013 onwards, they hired employees to operate a health-care products business via telemarketing, for which they purchased over 1000 pieces of citizens' personal information from the Internet in order to acquire customer information. The People's Court of Pudong New Area held that the defendants Zhang and Yang had illegally acquired citizens' personal information and their actions constituted the crime of illegally acquiring citizens' personal information.[496]

The Case of Wen Tao Illegally Acquiring Citizens' Personal Information

Between February and April, 2012, Wen Tao, the defendant, with the support of Wen Xuekun, Song Shifang, Chen Lin, and Lin Xiangfei, took advantage of network technologies and a series of unlawful means such as altering mobile phone numbers and pretending to be the customer service staff of telecommunication companies, to gain access to the passwords and detailed call lists of other people's mobile phones. In this way he obtained the details of 30 mobile phones, which he sold for RMB 86,300. The People's Court of Zixing, Hunan Province, determined that Wen Tao contacted the defendants Wen Xuekun, Song Shifang, Chen Lin and Lin Xiangfei for the purpose of gaining access to other people's mobile phone service passwords, constituting the crime of illegally acquiring citizens' personal information.[497]

The Case of Yang and Xiao Illegally Acquiring Citizens' Personal Information

Between February and March 2014, the defendants Yang and Xiao conspired to attack the examination registration website of a public institution in Shanghai via hacker software in the Honghua District, in Zunyi, Guizhou province. They illegally obtained over 40,000 pieces of examinees' personal information and gained RMB 8,000. Later, defendant Xiao sold the information once more, this time for a higher sum. According to the People's Court of Pudong New Area in Shanghai, the defendants Yang and Xiao had both committed the crime of illegally acquiring citizens' personal information.[498]

[496] (2014) No. 571 criminal case in New Pudong Area District, first trial.
[497] (2012) No. 184 criminal case in Zixing, Hunan province, first trial.
[498] (2014) No. 4078 criminal case in New Pudong Area, Shanghai, first trial.

Analysis and Conclusion of Cases

In the cases of Wen Tao et al., Yang and Xiao illegally acquiring citizens' personal information, the authors made use of cheating and technological means to steal other people's private information. Such means are commonly used in the crime of "illegally acquiring citizens' personal information" and show obvious characteristics of illegality. However, in the cases of Zhang and Yang illegally acquiring citizens' personal information, Zhang and Yang bought citizens' personal information through means of acquisition that did not have obvious illegal features in themselves, but were nevertheless considered illegal by the Court. Therefore, the unlawful acquisition of citizens' personal information is not limited to unlawful means, but can be affirmed under the following conditions: (1) the acquisition of information has violated the true willingness of information owners; (2) the information is required to be within the scope of legal protection; (3) the means of acquisition have violated the prohibitive provisions of laws and disturbed public order and good custom.

4. "Aggravated circumstances"

Article 253 of the *Criminal Law* establishes "grave circumstances" for the crimes of selling and illegally providing citizens' personal information and illegally acquiring citizens' personal information. However, it does not define such grave circumstances specifically. Case law seldom rarely refers to them. In the aforementioned case of Zhang 1 and Zhang illegally acquiring information concerning the location of mobile phones, the Court held that grave circumstances of obtaining personal information of citizens by unlawful means included: acquiring the personal information of several people on many occasions, causing serious economic losses or severely damaging the everyday lives of citizens, exercising a bad social influence, causing a negative impact on national security and people's livelihoods, or using the acquired personal information in criminal activities.[499] In the case of Sun Yindong illegally acquiring citizens' personal information,[500] Judge Ye Shengnan at the People's Court of Cixi, Zhejiang province, argued in favor of applying a mixed approach with both objective and subjective elements concerning the concept of grave circumstances. It should combine a series of factors such as objective danger and subjective malignancy as well as the social harm arising from criminal acts and the personal threat posed by actors. First, the amount of profit should be taken into account, as the reasons for actors illegally acquiring citizens' personal information are mostly of an economic nature. Second, the quantity of information illegally acquired normally consists of hundreds or even thousands of pieces of information, and such information can be resold many times. Third, the

[499] (2012) No. 0506 criminal case in Sihong county, Jiangsu province, first trial
[500] (2012) No. 1580 criminal case in Cixi, Zhejiang province, first trial.

number of infringements should be taken into account. According to the *Criminal Law*, "many times" refers to three times or more; the conviction standard for the crime of Mark Six gambling is accepting other people's bets three times or more. "Many times" as a grave circumstance of infringements upon citizens' personal information should be interpreted as at least three times within a year. Fourth, the impact on victims should be assessed. The act of illegally acquiring citizens' personal information is most likely to affect the victims extremely negatively. For example, the victims' right of reputation and privacy are encroached upon, and it will certainly impair their family and personal life and incur serious economic losses for them. Hence, these cases should be considered grave circumstances. [501]

In the aforementioned case of Xie Xinchong selling and illegally providing citizens' personal information, Mr. Jin Changwei, a judge from the Second Intermediate People's Court of Beijing, considered that the following aspects should be taken into account when determining "grave circumstances":[502]

1. The quantity of information and frequency of infringement. The frequency of criminal behavior is a standard of criminal law used to establish whether a personal is guilty or not and the committed crime is severe or light.

2. The degree of privacy related to the information, which reflects the severity of social harm incurred by criminal acts. Information that could be published according to the laws and regulations and with the prior consent of the data subject has a comparatively lower degree of privacy, and the impact on citizens' personal life is lower in most cases. Personal privacy, by contrast, refers to strongly personal attributes and thus merits a stronger degree of privacy. If viewed only from the perspective of the objective of the crime, the infringement upon personal privacy is more likely to impair a citizen's lawful rights and can lead to more serious social harm, and thus should be dealt with in different ways when determining the grave circumstances.

3. Duration and scale of dissemination of information. When talking about personal information, citizens mainly enjoy a kind of personal privacy right, that is, the right to an undisturbed personal life. The length of time and the scale of the dissemination of citizens' personal information is di-

[501] Shengnan, The Case of Sun Yindong Illegally Acquiring Citizens' Personal Information — Affirmation of Crime of Illegally Acquiring Citizens' Personal Information, Selected Cases of People's Courts, Edition 2, 2013.

[502] Changwei, Affirmation of Grave Circumstances in the Crime of Infringement upon Citizens' Personal Information, China Trial News, Edition 98.

rectly associated with the extent of influence of criminal acts on citizens' personal lives, and reflects the severity of social harm as a very important standard in the determination of grave circumstances. Dissemination of personal information can have negative consequences across large areas and for a very long time, for example information spreading quickly nationwide or even worldwide, or negative long-term consequences, which are difficult to rectify.

4. The immaterial damage and property losses suffered by the victims. As a result of the severe influence upon victims' work and life, they can suffer psychiatric disorders, family break-up, illness or suicide, or serious property losses.

5. The benefits obtained by the criminals. The major purpose of selling and illegally providing or acquiring citizens' personal information is to make profits, apart from invading other people's privacy or threatening them. Grave circumstances are constituted if the amount of illegal income gained by the criminal act is large. It is set at RMB 500 to more than RMB 2000, according to case law.

III. Administrative enforcement of law

The Ministry of Public Security launched three collective operations against criminal activities affecting citizens' personal information in February 2012, December 2012 and February 2013. They led to a total of 4115 detained suspects, the investigation of 4382 cases of selling, illegally providing and acquiring citizens' personal information, and the confiscation of nearly five billion archives containing personal information. The operations were directed against 985 criminal gangs that had acquired citizens' information by unlawful means, and uncovered more than 10,000 cases involving kidnapping, racketeering, debt collection by barbarous ways, telecommunication fraud, illegal investigation, and so on. In August 2013, the Ministry of Public Security once again deployed the public security organizations in a coordinated operation in 20 places including Beijing, Hebei province, and Shanghai.[503]

Within a month of the enactment of the *Consumer Protection Law*, the Hangzhou Administration Bureau for Industry and Commerce applied it for the first time in March 2014 in a case of infringement upon customers' personal information. During the special management and supervision of home decoration and building materials, the law enforcement officer of the Bureau discovered that a home decoration company, in order to promote their business and enhance their performance, had collected the information of owners in some sold residential

[503] http://www.gov.cn/gzdt/2013-08/12/content_2465232.htm.

districts by illegal means and without the owners' prior consent and authorization. The collected information included the owners' names, numbers of building floors, contact information, and so on. As the acts violated the regulations concerning the protection of customers' personal information as indicated in the new *Consumer Protection Law*, the Bureau imposed the administrative penalty of a RMB 15,000 fine.[504] In the same month, a furniture business operator in the Jiangyan district of Taizhou, Jiangsu province, published the private information of more than 100 customers including their names and home addresses, violating the provisions of the *Consumer Protection Law*. After receiving the information from customers, the officers at the local consumer protection association immediately carried out the investigation and transferred the case to the industrial and commercial administrative departments for further clarification.[505] In April 2014, a gas company in Daqing, Heilongjiang province, displayed a client's information on the computer at the receptionist's desk to remind the employees not to provide her with gas as she owed money. The client thought the company had leaked her personal information and made a complaint to the local consumer protection association. After the mediation, the client finally received RMB 3000 in compensation for immaterial damage.[506] In March 2015, the China Consumers' Association officially issued the *2014 Report on the Network Security Situation of Customers' Personal Information*, which analyzed the problems at the administrative supervision and management level with regard to the current consumer information protection practices. The report pointed out that although the new *Consumer Protection Law* had clearly stipulated the principles of protecting customers' personal information against illegal collection by business operators and the civil and administrative liabilities for the infringement upon customers' right of personal information, the current administrative law enforcement system and mechanisms are still insufficient. This is due to the fact that illegal means of infringement are mostly implemented on the Internet in a virtual, technologically fast-developing and secretive way. Local law enforcement officers still require more training in order to respond adequately to the practical difficulties of guaranteeing the protection and network security of customers' personal information.

[504] http://www.315.gov.cn/jnxf/201404/t20140418_144068.html.
[505] http://finance.chinanews.com/it/2015/03-15/7129664.shtml.
[506] http://gsj.zj.gov.cn/zjaic/jrgs/yqjc/201407/t20140715_130084.htm.

C. Current Issues and Case Law Concerning Consumer Data Protection in Germany and Europe (Prof. Dr. Gerald Spindler)

In this part, current issues and case law concerning consumer data protection in Germany and Europe are presented, taking into account some of the latest developments in consumer data protection before German courts and the ECJ. Case law has a direct influence and impact on German legislation and the judicial interpretation of norms. The following issues are dealt with: credit scoring and related databases, data protection in social networks, cloud computing, "big data," the existence of rating platforms on the Internet, profiling, unsolicited e-mails, the role of online search engines, and the right to be forgotten in the jurisprudence of the ECJ, as well as its judgment on data retention.

I. Data protection in social networks

Social networks, particularly Facebook, have raised numerous concerns about data protection as they have collected personal and sometimes highly sensitive data. The ULD in the province of Schleswig-Holstein particularly inaugurated several actions against Facebook.[507] These actions concentrated on so-called fanpages and on plug-ins and "like" buttons that collected data without prior notice to the user. However, the *Oberverwaltungsgericht Schleswig* (Higher Administrative Court) denied the jurisdiction of Schleswig-Holstein, thus rendering it impossible for the supervisory authority to carry on the investigations and actions.[508] The discussion in Germany generally focuses on the privacy policy of Facebook, particularly on the consent which is provided by users. It is argued that transparency is lacking and requests for disclosure of data processing are unanswered.

II. Credit scoring

Credit scoring is a widely used tool for financial institutions in Germany in order to assess the credit reliability of consumers (and other persons). One of the most important credit inquiry agencies is the central organization called "Schufa Holding AG"[509] (Schufa), which operates a database that collects information about persons and their financial reliability, usually transferred to Schufa by enterprises which are connected to the database/Schufa.

---

[507] See the collection of all facts at https://www.datenschutzzentrum.de/facebook/.
[508] OVG Schleswig, decision of 22/04/2013 – 4 MB 10/13, 4 MB 11/13.
[509] www.schufa.de

Section 28a of the BDSG addresses credit inquiry agencies explicitly, specifying the conditions to be met if personal data concerning a claim are transferred to a credit inquiry. The justification of the transfer generally requires that:

> the performance owed has not been rendered on time, the transfer is necessary to protect the justified interests of the controller or a third party.

In addition, the transfer, according to Sec. 28a (1) of the BDSG, depends upon several elements, of which at least one has to be fulfilled, in particular that:

> 1. the claim has been established by a final decision or a decision declared enforceable for the time being, or if an executory title has been issued under Section 794 of the Code of Civil Procedure,
> 2. the claim has been established under Section 178 of the Insolvency Act and has not been disputed by the debtor at the verification meeting,
> 3. the data subject has expressly acknowledged the claim,
> 4. a) the data subject received at least two written reminders after the due date,
> b) at least four weeks elapsed between the first warning and the data transfer,
> c) the controller gave the data subject sufficient notice before transferring the information, or at least informed the data subject of the impending transfer in the first reminder and
> d) the data subject did not dispute the claim, or
> 5. the contractual relationship on which the claim is based can be terminated without prior notice for payment in arrears and the controller has informed the data subject of the impending transfer.

In practice, the express acknowledgment of the transfer (No. 3) seems to be prevailing, as most enterprises, merchants, financial institutions, etc. require their contracting partner (in most cases a consumer) to give their express consent to transfer data and to allow inquiries to a central credit inquiry agency. However, it seems that a lot of information is also being transferred according to Nos. 1 and 4. Moreover, financial institutions are facing even stronger restrictions according to Sec. 28a (2):

> (2) For the future transfer under Section 29 (2), financial institutions may transfer personal data on the creation, orderly execution and termination of a contractual relationship concerning a bank transaction under Section 1 (1) second sentence No. 2, No. 8 or No. 9 of the Banking Act to rating agencies unless the data subject's legitimate interest in excluding such

> transfer obviously outweighs the interest of the credit inquiry agency in the data. The data subject shall be informed of this before the contract has been concluded. The first sentence shall not apply to contracts concerning current accounts without overdraft protection. For the future transfer under Section 29 (2), data concerning the behaviour of data subjects which serve to create market transparency in the context of pre-contractual relationships of trust may not be transferred to credit inquiry agencies even with the data subject's consent.

Based upon this information, credit inquiry agencies and operators of (financial) databases often create financial scores for data subjects, particularly for consumers. In Germany, Schufa acts as one of the most important database operators, offering interested clients, such as banks, financial institutions, credit card enterprises, or telephone companies (to name but a few) a score for any person who intends to conclude a contract with a client.

Concerning scoring, Sec. 28b of the BDSG, stipulates that:

> For the purpose of deciding on the creation, execution or termination of a contractual relationship with the data subject, a probability value for certain future action by the data subject may be calculated or used if
>
> 1. the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure,
>
> 2. in case the probability value is calculated by a credit inquiry agency, the conditions for transferring the data used under Section 29, and in all other cases the conditions of admissible use of data under Section 28 are met,
>
> 3. data in addition to address data are used to calculated the probability value,
>
> 4. in case address data are used, the data subject shall be notified ahead of time of the planned use of these data; this notification shall be documented.

The use of "scientifically recognized mathematic-statistical procedures" (besides other elements of Sec. 28b BDSG)is, thus, crucial to the scoring process.

The existence and structure of those methods had been exactly the focal point of a decision of the German High Federal Court:[510] A data subject had filed an action against the credit inquiry agency/operator of the database Schufa claiming information about scoring procedures which led to a negative score, thus, affecting his ability to conclude contracts.

However, the court rejected the claim, arguing that the legislator explicitly restricted the claim to be informed to individual personal data and did not extend this claim (Sec. 34 (2, 4) BDSG) to revealing scoring procedures or benchmark groups.[511] The court deemed information about individual personal data that had been used for scoring and information according to Sec. 34 (2, 4) of the BDSG, such as probability values, as sufficient to cover the needs of data subjects to be informed; any information about the specific scoring procedures are not covered by the request for information.

III. Cloud computing

The main problem with regard to cloud computing concerns the different levels of data processing in the cloud and the unpredictability of where the data will be processed and by whom exactly. Thus, there are problems of international transfer of data[512] and information required for consent.[513] Cloud computing can be qualified as data processing on behalf of the controller who is the user of the cloud.[514] Hence, the user has to ensure that the cloud provider complies with all data protection requirements – which is, in practice, hard to do, as the control of data processing required is not limited to the cloud provider itself, but extended to every level of the cloud.[515] Moreover, concerning consent, it is usually required that the data subject must be informed where and who will process the data –

---

[510] Bundesgerichtshof (German High Federal Court), 28.1.2014 – VI ZR 156/13

[511] *Bundesgerichtshof* 28.1.2014 – VI ZR 156/13 no. 17, 22 and following, in particular 27; *Heinemann/Wäßle*, MMR 2010, 600, 602; *Metz*, VuR 2009, 403, 406;

[512] See *Hon/Millard*, in Millard, Cloud Computing Law, p. 254 ff.; *Brennscheidt*, Cloud Computing und Datenschutz, p. 181 ff.; *Heckmann*, in jurisPK-Internetrecht, Kap. 9, Recital 624 ff.

[513] *Cimato (ed.)*, D31.1 – Risk assessment and current legal status on data protection, p. 41 ff., available at http://www.practice-project.eu/downloads/publications/D31.1-Risk-assessment-legal-status-PU-M12.pdf; *Hon/Millard*, in Millard, Cloud Computing Law, p. 261 f; *Spindler/Nink*, in Spindler/Schuster, Recht der elektronischen Medien, Para. 4a BDSG, Recital 15 f.

[514] C.f. *Mell/Grance*, US NIST SP 800-145, 2011, The NIST Definition of Cloud Computing, p. 6, available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; *Hon/Millard*, in Millard, Cloud Computing Law, p. 3 ff.; various other definitions at *Giedke*, Cloud Computing, p. 36 ff.

[515] Bräutigam/*Thalhofer*, in Bräutigam, IT-Outsourcing und Cloud Computing, Teil 14, Recital 49 ff.; *Brennscheidt*, Cloud Computing und Datenschutz, p. 87 ff.; *Giedke*, Cloud Computing, p. 229 ff.; *Art. 29 Working Party*, Opinion 05/2012, WP 196, 8 f.

which is also hard to comply with.[516] Finally, the rules for transfer of data in third countries cannot be fulfilled as – again – the location of data processing is unknown before the cloud computing process starts.[517] Thus, it is hard to tell in advance if an adequate level of data protection is guaranteed in the third county where the cloud computing will take place.[518] Because of this, only "European" clouds are allowed from a strictly legal perspective.[519]

IV. "Big data"

"Big data," as a new way to recombine data, raises a lot of unresolved questions.[520] As "big data" technologies enable the filtering of data in new ways and creating profiles out of data existing already, even non-identifiable data may be arranged in such a way that a person is again identifiable.[521] In other words, formerly anonymous data now becomes personal data, as algorithms may relate data to a person.[522] Moreover, a given consent refers to a specific purpose of data processing[523] – it does not (and cannot) take into account other purposes for data processing which arise later.[524] However, this change of data use (and purposes) are typical for "big data." Hence, consent may not work out as a legitimation for "big data" processing.[525] Moreover, information that has to be provided for the data subject cannot be given at the time of "big data" processing, as it is unclear who is really affected until the final result of "big data" processing.[526] Nevertheless, according to Sec. 28 (1) of the BDSG, controllers can use personal data if needed to create, carry out or terminate a legal obligation with the data subject (in principle, contractual obligations) or in so far as data processing is necessary to

---

516 *Bräutigam/Thalhofer*, in Bräutigam, IT-Outsourcing und Cloud Computing, Teil 14, Recital 65; *Brennscheidt*, Cloud Computing und Datenschutz, p. 151.

517 Regarding the transfer of data in third countries, see *Cimato (ed.)*, D31.1 – Risk assessment and current legal status on data protection, p. 44 ff.; *Bräutigam/Thalhofer*, in Bräutigam, IT-Outsourcing und Cloud Computing, Teil 14, Recital 66 ff.; *Weichert*, DuD 2010, 679 (686 f.).

518 *Gabel*, in Taeger/Gabel, BDSG, Para. 4b, Recital 23; *Simitis*, in Simitis, BDSG; Para. 4b, Recital 79.

519 Regarding the deficits in data protection in the USA and the access to data of US American authorities, see *Heckmann*, in jurisPK-Internetrecht, Kap. 9, Recital 626, 630 ff.; *Rath/Rothe*, K&R 2013, 623 (628); *Spies*, ZD 2013, 535 (536 ff.).

520 For an overview of the legal challenges concerning "big data," see *Ohrtmann/Schwiering*, NJW 2014, 2984 (2984 ff.); *Weichert*, ZD 2013, 251 (251 ff.).

521 *Katko/Babaei-Beigi*, MMR 2014, 360 (361 f.).

522 *Koch*, ITRB 2015, 13 (18); Weichert, ZD 2013, 251 (257).

523 District Court (Landgericht) of Berlin, decision of 30/04/2013 – 15 O 92/12 – NJW 2013, 2605 (2606); *Art. 29 Working Party*, Opinion 03/2013, WP 203, 15 ff.; *Helbing*, K&R 2015, 145 (146 ff.); *Taeger*, in Taeger/Gabel, BDSG, Para. 4a, Recital 30.

524 *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 4a, Recital 32; *Katko/Babaei-Beigi*, MMR 2014, 360 (362); *Simitis*, in Simitis, BDSG, Para. 4a, Recital 27 ff., 70; *Spindler/Nink*, in Spindler/Schuster, Recht der elektronischen Medien, Para. 4a BDSG, Recital 9.

525 *Koch*, ITRB 2015, 13 (17).

526 *Weichert*, ZD 2013, 251 (256).

safeguard the justified interests of the controller. If the data is generally accessible (Sec. 28 (1), sentence 1 No. 3 BDSG), e.g. on web pages[527] or in social networks,[528] "big data" applications may be justified if the interests of data controllers outweigh the interests of individuals.[529] Moreover, "big data" does not infringe data protection provisions if data is being anonymized or at least pseudonymized so that the data loses its reference to specific persons.[530] However, the general principles of purpose binding, of data avoidance and data minimization (also see Art. 8 (2) of the Charter of Fundamental Rights of the European Union) may render the use of "big data" impossible.[531] Moreover, the prohibition of automated individual person-related decisions (see Sec. 6a BDSG) creates another legal hurdle concerning "big data" analytics.[532] Article 20 of the GDPR Proposal provides every natural person the right to object to profiling, in particular to profiling that has the effect of discrimination.[533] Finally, Art. 33 (1) of the GDPR obliges the controller to carry out an assessment of the impact of the envisaged processing operations on the rights and freedoms of the data subjects, which will most likely have to be done regarding "big data" processing.[534] This highlights just a few problems related to "big data," and the traditional justifications of the DPD for data processing do not allow for these new instruments.[535]

V. Profiling

Profiling is a widespread tool to combine different data so that a personal "profile" for a user can be created which allows the operator of the profile to tailor actions according to the profile of the person, such as personalized advertisements or messages which are related to the location of the person. Every kind of decision taking or action could be based upon such a profile, even concerning criminal

527 As long as the access to the information is open to everyone, e.g. via search engines, see *Gola/Klug/Körffer*, in Gola/Schomerus, BDSG, Para. 28, Recital 33a; *Oberwetter*, BB 2008, 1562 (1564); *Weichert*, ZD 2013, 251 (257).

528 For this very controversial question, see *Wittek*, Soziale Netzwerke im Arbeitsrecht, p. 56 ff.

529 *Bitter/Buchmüller/Uecker*, in Hoeren, Big Data und Recht, p. 78 f.; *Weichert*, ZD 2013, 251 (257).

530 Nevertheless, the possibility of re-individualizing of data is an existing risk, c.f. *Baeriswyl*, in Weber/Thouvenin, Big Data und Datenschutz, p. 50 ff.; *Bitter/Buchmüller/Uecker*, in Hoeren, Big Data und Recht, p. 79 f.

531 *Koch*, ITRB 2015, 13 (17); *Ohrtmann/Schwiering*, NJW 2014, 2984 (2987); *Weichert*, ZD 2013, 251 (256).

532 *Ohrtmann/Schwiering*, NJW 2014, 2984 (2987 f.).

533 C.f. *Koch*, ITRB 2015, 13 (20); Scholz, in Simitis, BDSG, Para. 6a, Recital 8a.

534 *Koch*, ITRB 2015, 13 (20).

535 C.f. *Koch*, ITRB 2015, 13 (16 ff.).

prosecution.[536] Hence, dangers for privacy are evident if any available data can be combined in such a way that profiles are created.[537]

With the exception of Sec. 15 (3) of the German Telemedia Act,[538] the BDSG and the European DPD do not provide specific norms on profiling. By contrast, profiling is dealt with in Sec. 6a of the BDSG (based upon Art. 15 and Art. 12 a) DPD), which generally prohibits decision taking by automatic procedures and using personal profiles. However, Sec. 6a (2) allows for some exceptions:

> 2) This shall not apply if
>
> 1. the decision is made in connection with the conclusion or fulfilment of a contract or any other legal relationship and the data subject's request has been met or
>
> 2. if there are appropriate measures to protect the legitimate interests of the data subject and the controller informs the data subject that a decision as referred to in sub-Section 1 has been made and, upon request, explains the main reasons for this decision.

The prohibition of Sec. 6a depends upon the consequences of an automated decision: Only if the automated decision entangles legal consequences or is of substantial harm for the data subject does Sec. 6a (1) step in.[539] Even though personalized advertisements are one of the most relevant cases, the prevailing opinion upholds the position that the amount of marketing, content of the advertisement and other circumstances are decisive to assess the harm to the data subject.[540] Thus, using profiles for marketing purposes is not generally prohibited.

The proposals of the GDPR are far more specific on profiling:

First, Art. 4 (12a)[541] defines profiling as:

> "profiling" means any form of automated processing of personal data consisting of using those data to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements.

---

536 Cf. the famous science fiction movie "Minority Report," which deals with profiles created by the police in order to determine future criminal behavior of persons.

537 We do not deal with the specific problems of cookies as addressed by Art. 5 (3) of the ePrivacy Directive. For a detailled analysis, see the working paper No. 171 of the Art. 29 Working Party, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.

538 See below.

539 Gola/Schomerus, § 6a BDSG No. 10.

540 *Scholz* in Simitis, BDSG, § 6a No. 28; Gola/Schomerus, § 6a BDSG No. 10.

541 Council Proposal.

According to Art. 4 (1) (h),[542] the data controller has to inform the data subject about

> the existence of automated decision making including profiling referred to in Article 20(1) and (3) and information concerning (…) the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Article 20 of the envisaged GDPR does not, in priniciple, change the approach chosen by the DPD (and Sec. 6a BDSG). However, (in the Council's proposal) Art. 20 (1a) (c) also allows profiling in the case of an explicit consent and (b) in the case of member state allowances if the member state requires "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." More precisely than before, the GDPR requires:

> 1b. In cases referred to in paragraph 1a (a) and (c) the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

However, proposals to prohibit profiling of minors did not find their way into the latest proposals of the Council. Thus, profiling will be regulated in more or less the same way as before if the Council's proposal prevails.

Whereas all these provisions concern the decision taking based upon generated profiles and do not explicitly deal with the collection of data aiming at establishing profiles,[543] Sec. 15 (3) of the German Telemedia Act allows the collection of user data (concerning their behavior) for purposes of marketing, designing the telemedia or marketing research only if pseudonyms are used and only if users do not object to the use of their data. Thus, profiling is handled in a very restrictive way concerning telemedia; in contrast to Sec. 6a of the BDSG and the prevailing opinion, pseudonyms are required even in cases of unsubstantial harm. Moreover, even in the case of pseudonyms, profiles may not be used for other purposes than those mentioned in Sec. 15 (3) of the German Telemedia Act [544] – as long as telemedia services are concerned.[545]

---

[542] Council Proposal.

[543] Cf. The criticism of Härting CR 2014, 528 (532 ss.).

[544] Cf. also Zeidler/Brüggemann CR 2015, 248 (254).

[545] Note that most services concern both the German Telemedia Act and the BDSG, such as online banking.

VI. Unsolicited e-mails

Unsolicited e-mails (Spam) are one of the main nuisances of Internet communication. These mails are generally used for purposes of (unsolicited) marketing and advertisement. Thus, it is evident that they are, in principal, dealt with by provisions of the unfair competition law (*Gesetz gegen den unlauteren Wettbewerb*:). Section 7 (2) (No. 3) of the UWG, in particular, requires the explicit consent of the individual to whom the e-mail is being sent.[546] However, the use of an e-mail address also implies, in most cases, the use of personal data, as the e-mail address is linked to a person who can be identified by means of the address.[547] Thus, data protection law also applies to the use of e-mail addresses in advertising and marketing.[548] Whereas the treatment of unsolicited e-mails according to the UWG falls outside the scope of this analysis, it is worthwhile taking a closer look at the data protection requirements. According to the general principles, only the explicit consent of the data subject or a legal justification will permit the use of personal data in the e-mail address. Regarding the explicit consent, the general principles for the consent apply, particularly that the consent has to be declared explicitly and voluntarily. However, whether minors can also declare their consent is still disputed; some authors contend that minors are able to assess the implications of their consent to receiving unsolicited e-mails.[549] Whereas this differentiation between general contract law (and law of declarations) and consent is doubtful, the forthcoming GDPR states this view (as mentioned already) by fixing the age for minors to declare their consent at 13. Moreover, the frequent use of general terms and conditions raise some problems concerning their relationship to consent: The German High Federal Court declared a clause in general terms and conditions of contract as void which was designed as an "opt-out clause" and combined with other declarations of the client.[550] Thus, the court generally requires a specific "opt-in" declaration, usually by an individual signature or a separate click-box. However, the court[551] deemed a clause as legitimate which explicitly restricted the consent in the general terms and conditions to e-mails if the clause highlighted the consent. The court also required that the client declares his/her consent to the general terms and conditions; thus, pre-formulated click-boxes ("tickle-away") are not permitted.[552]

---

546 For more details, see Schirmbacher/Schätzle WRP 2014, 1143.

547 E.g. in the case of *Oberverwaltungsgericht Berlin-Brandenburg*, 31.7.2015 – OVG 12 N 71.14.

548 *Gola/Schomerus* BDSG, § 3 Rn. 10a; Rudolph CR 2010, 257 (260); Schirmbacher/Schätzle WRP 2014, 114.

549 In particular Schirmbacher/Schätzle WRP 2014, 1143 (1144 s.).

550 German High Federal Court (BGH), 16. 07. 2008 – VIII ZR 348/06, WRP 2009, 56 – Payback.

551 German High Federal Court (BGH), 16. 07. 2008 – VIII ZR 348/06, WRP 2009, 56 – Payback.

552 German High Federal Court (BGH), 10. 02. 2011 – I ZR 164/09, WRP 2011, 1153 – Double-Opt-in-Verfahren; more details at Schirmbacher/Schätzle WRP 2014, 1143 (1145 s.), in particular discussing a deviating decision of *Oberlandesgericht München* 27. 09. 2012 – 29 U 1682/12, WRP 2013, 111; see also *Ernst* , WRP 2013, 160.

In practice, the so-called "double opt-in" procedure is widely used: Here the operator of the website sends the user an e-mail asking him to confirm by a specific link that he/she really was the one who has given his/her consent to advertisements and receiving newsletters.[553]

Even though these requirements have been developed mainly for unfair competition law, they can also be applied to data protection law.[554] Interpretations may differ only in one (sometimes, however, crucial) detail: Some of the authors dealing with consent in unfair competition law, in particular Sec. 7 (2) of the UWG, contend that an "explicit" or "specific" consent still encompass the implied consent.[555] Without going into more details, this interpretation seems to be doubtful in the light of the wording of the directives. However, the general principle in data protection law applies that the consent has to be given explicitly, as the Art. 29 Working Party stated, in order to avoid circumventions of the right of self-determination by interpreting a data subject's behavior.

Regarding legal justifications, Sec. 28 (1) and (3a) of the BDSG, in principle, provide for some privileges of marketing and advertisement actions, in particular the so-called "list-privilege;" however, this privilege does not apply to e-mails. Moreover, Sec. 7 (2) (No. 3) of the UWG would be potentially overridden by these justifications, so that even though these justifications may apply from the general perspective of data protection law, they cannot put aside the specific requirements of the UWG. Thus, the explicit consent is still needed.[556]

Finally, Sec. 6 (2) of the Telemedia Act prohibits the concealment of the commercial character of the e-mail or the identity of the sender, particularly regarding the header of the e-mail.

VII. Rating platforms

The famous case of the rating platform "spickmich.de" concerned a rating system for teachers.[557] This rating platform offered a rating system addressed to students and pupils in order to evaluate their teachers, using the full names of the teachers and of the school where they were engaged. Access to the platform was available to everyone, however, users had to register themselves, but without any identity

[553] However, some authors have cast doubt upon the legitimacy of the double opt-in procedure, as the first mail of the merchant (requiring a confirmation) could already been qualified as an unsolicited e-mail, cf. Möller WRP 2010, 321 (327 s.); see also *Oberlandesgericht München*, op. cit.

[554] Note, however, that the German High Federal Court contended that consent in data protection law has to be interpreted differently in contrast to unfair competition law – even though both provisions were intended to implement the ePrivacy Directive, see German High Federal Court (BGH), 16. 07. 2008 – VIII ZR 348/06, WRP 2009, 56 – Payback; similar Rudolph CR 2010, 257 (260); criticized by Möller WRP 2010, 321 (332).

[555] See, for example, Rudolph CR 2010, 257 (259).

[556] Also see Rudolph CR 2010, 257 (261).

[557] German High Federal Court (BGH) – decision of 23.06.2009 – VI ZR 196/08.

check – only an e-mail address was required. The platform offered typical social network functions to users, such as building up friendships and clubs, and evaluation forms of their school including rating factors, such as "party factor" or "flirt factor." Concerning the teachers, their full names and identity could be related to evaluations using school notes for the quality of their teaching, as well as their personal characteristics, such as "coolness." Moreover, a generic field allowed for free text in order to cite anecdotal stories about a teacher. Finally, the system allowed for a complaint mechanism for users. One teacher complained about her rating of a "4" (sufficient) related to her full name and the name of the school – however, all this personal data had been available at the public website of the school, accessible to everyone. The teacher filed a civil action against the platform operator requiring the deletion of the evaluations as well as stopping any kind of similar evaluation in the future.

The German High Federal Court denied the actions claimed in arguing that the BDSG does not prohibit these activities of the platform operator. Whereas the court acknowledged that the evaluations had to be qualified as personal data, the court stated that the transmission and storage of the data had been justified according to Sec. 29 of the BDSG. The courts struck a balance between the interests of the public to be informed (as well as of the students to free speech) and the interests of the teacher not to be identified. From the court's standpoint, the freedom of speech of the students and the public interest to access information and to discuss those ratings outweighed the interests of the teacher. The court applied the same criteria as, in general, civil law concerning personality rights, however, in the realm of the BDSG concerning the balance of interests.[558] The court stressed the fact that the evaluations could not be accessed by a search engine; registration was necessary in order to read the information and evaluations[559] – thus, distinguishing the case from the later decision of the ECJ in Google Spain. Moreover, the court upheld that free speech involves anonymity, so any kind of identification requirements may lead to a chilling of free speech.[560] The Court denied the application of the so-called media privilege (Sec. 41 BDSG) for the platform operator, as this privilege is restricted to traditional mass media, such as press publications or broadcasters. In contrast to traditional mass media (even electronic press, etc.), the court emphasized the fact that such rating platforms do not contribute, in principle, to public discourses (characteristic for democratic processes) which are covered by the German Constitution.[561]

[558] Cf. German High Federal Court, op. cit. No. 30 – 35.
[559] German High Federal Court, op. cit. No 37.
[560] German High Federal Court, op cit. No. 38.
[561] German High Federal Court, op. cit. No. 20 – 22.

VIII. The right to be forgotten

The famous case of the ECJ concerning the so-called "right to be forgotten" (Google Spain)[562] referred to information available at an online-archive about a Spanish journal, La Vanguardia, freely accessible on the Internet. The complaint was based on the fact that when an Internet user entered the name of the claimant in the search engine of the Google group ("Google Search"), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González's name appeared for a real estate auction relating to attachment proceedings for the recovery of social security debts. The claimant requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia.

The court stated that even though the information was publicly available and not altered by the search engine, the DPD was still applicable, as Google "multiplicated" the impact of distributing personal data on the person affected.

Moreover, concerning the quality of Google as the search engine operator, the court did not see any reason why such a search engine could not be assessed as the data controller.[563]

Even though the publisher (the journal) is the original source of information and can determine the extent to which search engines may access the data, the ECJ upheld the view that this does not change the fact that the search engine operator can at least be qualified as a joint controller.[564]

Moreover, the court pushed aside the arguments of Google (and implicitly of the national courts) that the DPD shall not be applicable if data processing is done outside of the EU; i.e. that the DPD shall not be applied if a subsidiary just carries out marketing activities.[565] Hence, the court emphasized not only that the marketing activities are linked to the data processing, but stressed the importance of protecting fundamental rights of data subjects.

Another essential element of this landmark decision refers to the emphasis on the role of fundamental rights based upon the EU Charter of Fundamental Rights. Thus, the ECJ established a constitutionally grounded framework for data

[562] ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález.

[563] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 33 – 37.

[564] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 39 – 40.

[565] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 54 – 58.

protection.[566] On the grounds of this interpretation, the ECJ balanced the interests and rights of Google as the data controller with the rights of the data subject.[567]

Moreover, the ECJ pushed aside the argument that firstly an erasure of data should be obtained by the publisher. Hence, the ECJ denied any subsidiarity principle evoked by Google, referring explicitly once again to the effectiveness of data protection in the EU.[568] Even though the first data controller (here, the publisher) benefits from exemptions of the DPD, the second data controller (here, the search engine) may not claim the same exemptions.[569]

Furthermore, the ECJ pointed out that the impact of published data (or linked personal data) on the data subject's rights may change over time. Even though the original linking to the publication of personal data has been justified, the interests of the public may diminish over time, thus, changing the balance of interests.[570] However, the ECJ still keeps a door open for overriding public interests, particularly of a data subject in public life.[571]

IX. Data Retention

Another prominent case with relevance for most states concerns the EU Data Retention Directive. Similar to the German Constitutional Court,[572] the ECJ declared the existing directive void by citing principles of transparency, clarity and proportionality regarding the fundamental rights of data subjects.[573] The decision has had a strong impact on the evolution of data protection at an EU level, as it carved out clearly the individual rights based on the EU Charter of Fundamental Rights.

The case concerned a mobile phone which had been registered on 3 June 2006 and had been used since that date. Directive 2006/24 required telephone communications service providers to retain traffic and location data relating to those providers for a specified period, in order to prevent, detect, investigate, and prosecute

---

[566] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 68 – 70.

[567] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 80 – 82.

[568] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 84.

[569] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 85 – 87.

[570] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 93 – 94.

[571] *Cfr.* ECJ, decision of 13/05/2014 – C-131/12 – Google Spain SL a. Google Inc./Agencia Española de Protección de Datos [AEPD] a. Mario Costeja Conzález, Para. 97.

[572] German Federal Constitutional Court (Bundesverfassungsgericht), decision of 02/03/2010 – 1 BvR 256/08 – BVerfGE 125, 260 (retention of data).

[573] ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others).

crime and safeguard the security of the state. These data include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration, and type of communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, *inter alia*, of the name and address of the subscriber or registered user, the calling telephone number, the number called, and an IP address for Internet services. Those data make it particularly possible to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication and the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

The ECJ first stressed the fact that those

> 27. […] data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[574]

The court submitted the directive to a thorough test based on the fundamental rights of the EU Charter.[575] Hence, any interference has to be justified, particularly with regard to the basic principles enshrined in the EU Charter, such as transparency, clarity and proportionality.[576] The ECJ emphasized that the tests to be passed are even stricter if automatic processing is at stake.[577]

Moreover, the court stressed the fact that the directive applied to nearly everyone, even without evidence that the data subject is linked to any crime.[578] One of the crucial failures of the directive had been the "general absence of limits":

60. Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to

[574] ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 27.

[575] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 29, 34 – 35, 37.

[576] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 38, 45 – 48, 54.

[577] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 55.

[578] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 56 – 59.

determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.[579]

The court deplored the fact that the directive provided no safeguards to protect the personal data and, in particular, no principles for the purpose and subsequent use of the data.[580] Moreover, the directive provided for no distinctions concerning the data retention period.[581] Finally, the ECJ demanded safeguards concerning the effective protection of data retained.[582] The court particularly required that the data retained must stay in the EU in order to ensure adequate data protection.[583]

D. Challenges of New Technologies for Consumer Data Protection
(Privacy International with Consumers International)

Since the 1960s and the expansion of information technology capabilities, business and government organisations have been storing personal information in databases. Databases can be searched, edited, cross-referenced and data can be shared with other organisations and across the world. Once the collection and processing of data became widespread, people started asking questions about what happened to their information once it was turned over. Who had the right to access the information? Was it kept accurately? Was it being collected and disseminated without their knowledge? Could it be used to discriminate or abuse other fundamental rights? From all this, and growing public concern, data protection principles were devised through numerous national and international consulta-

[579] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 60.
[580] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Par. 61 – 62.
[581] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 64 – 65.
[582] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 66 – 67.
[583] *Cfr.* ECJ, decision of 08/04/2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Recourses and others), Para. 68.

tions. Today, over 100 countries have data protection laws, and organisations, public or private, that collect and use personal information have the obligation to handle this data according to the data protection law.

But technologies can also play a strong role in ensuring data protection rules are followed. Through technological means and careful design it is possible to limit data collection to mathematically restrict further data processing and to assuredly limit unnecessary access, among other privacy measures. Laws can influence and compel such developments when necessary. However, the adoption of these measures has been slow as data collectors are resistant to limit their future capabilities or aspirations to mine personal information, even when they are legally supposed to.

Nevertheless, it is also possible to see how modern technology developments are challenging some of our existing rights, as well as how we conceptualise human autonomy. There are a variety of these technologies used nowadays that will be outlined in the following paragraphs.

I. Cloud Storage

The goal of Cloud Storage is to leverage the internet to provide large and reliable data storage accessible from anywhere. The costs of computer storage have decreased year on year, meaning that now up to 50GB of free storage can be offered to users.. Accessing files can generally be done through a browser or a device such as a mobile phone or laptop. In all cases, the files can be stored in many locations simultaneously so that if one copy gets destroyed or corrupted another copy is available.

Cloud storage providers generally get access to individuals' data in two ways:

1. Metadata: the IP address of the users and the times at which they make changes to files.
2. Content: the contents of all files are generally available to the cloud storage providers' employees.

The benefit of this technology is that individuals and businesses have the peace of mind that their data is stored in a reliable location, off-site and readily available. The downside to this is that the information is viewable by others as well as the metadata revealing much of the lifestyle of the user. These downsides make it unsuitable for professions with a responsibility for keeping privileged information confidential. Some platforms, such as SpiderOak, do offer encrypted storage but the metadata problem still exists.

Importantly, this information may reside in another jurisdiction where data protection laws are weaker, or even non-existent, providing even greater hurdles to the individual who is seeking to protect their data.

II. Cloud Computing

Cloud Computing builds on cloud storage to perform complex and time consuming operations that would be impossible or impractical on a user's computer. A user can upload the data and software to powerful computers that can perform the computations. The user only pays for the computation used rather than the actual hardware, making it a cost effective way to do analytics. Similar problems arise as with Cloud Storage, because the service provider will be able to view the data to be processed as well as the results sent back to the user.

Examples of cloud computing have emerged even in the consumer space. Office 365 and many image and video editing systems allow users to upload their data, not solely for storage, but for further processing. This can include video editing and complex analytics on accounts in a database or spreadsheet. Ownership of the data uploaded and the results provided can vary from provider to provider and so too can applicable law in relation to access to this information.

III. Big data

Big data is a term used to describe the application of analytical techniques to search, aggregate, and cross-reference large data sets in order to develop intelligence and insights. While data mining and the application of analytics to data is not new, the ambition of 'big data' is that these methods can be applied to very large data sets for the first time. These large data sets can range from publicly available data sets, to national data sets, all search requests on a search engine, to internal customer datasets held by a particular company.

Big data can pick out patterns in data that would be impossible to do manually. However, the patterns it picks out are limited to the quality and scope of the input data and the algorithm. Accordingly the results can be of poor quality and potentially incorporate unlawful factors (such as race) in the models for decision making that it produces. Big data does show promise in understanding risk factors for certain medical conditions but the collection of medical data is problematic from a privacy perspective in the first place.

Big data analytics often involves a secondary use of the data. Data is very rarely generated for the purpose of data mining, rather data that was intended for another purpose is mined in order to get other useful information from it. The party performing the mining may not be the one who provided the original service and they may even sell the results of their mining venture back to the original owner of the data store. This raises the issue of whether the person who created the data is aware that it is being mined. Legally this gives rise to conflict with data protection law.

IV. Social Media

Social media has seen an explosion in popularity over the past decade. It allows users to upload information on their lives, including photos, friendships and thoughts. The services are typically provided for free as advertisers pay for screen real estate. With advertisers involved, there is a push to have more and more information shared on the platform so that it can be used to "improve" the relevance of ads to the user. In some cases, information about the user can be sent to these third parties themselves for them to decide which ads to present.

Who can have access to this information, in what circumstances and in what jurisdiction are big questions that social media providers often have difficulty providing answers to. Aside from the technical flow of data and metadata for operational reasons, users' locations may change and that may give rise to an additional factor that must be taken into consideration when data is accessed.

V. Internet of Things

Internet of Things (IoT) is a term that is used to articulate a paradigm shift from computers with screens connected to the internet to the connectivity of objects directly to the Internet. These objects can provide rich sensing and actuation capabilities in the physical world. The promise of the Internet of Things is an environment that senses and adapts to us without significant explicit interaction with the system.

There are many issues with the Internet of Things, including security of the system. Additionally, it is unclear how the system will resolve conflicts in delivering conflicting performance goals for different people or groups of people. Finally, having a world that senses everything you do poses massive privacy issues, including how the data about you is processed and transferred to third parties, as well as government access to sensitive information about entire populations.

VI. Smart Cities, Buildings and People

Building on top of the IoT infrastructure are the notions of smart cities and buildings as well as personal environments that are constantly sensing and adapting. We are seeing heart rate monitors incorporated into watches that connect to the internet via the users' phones and even medical devices that are online. All of the problems associated with IoT translate into these types of systems and are beginning to become more ubiquitous with each new gadget released on the market.

When we extend the use of sensors across areas and regions, the sensors are no longer limited to an individual but an entire population of a city. Smart meters are already emerging to monitor household consumption, but smart grids can monitor the consumption data and habits of a city, nation, and beyond. Smart cities will be able to monitor the movement of individuals and vehicles and help the city make decisions accordingly. It is also extending to smart policing where

data sets and machine learning will be used to identify activities for the police to pursue.

VII. Privacy friendly technologies

In face of different abusive usages of consumer data, there is a growing awareness of the need to protect data and demand higher levels of protection and transparency from companies dealing with consumer data in our everyday lives. Many new products and technologies have emerged or have been increasingly used to satisfy this demand. These are just some:

VIII. Disk encryption

Many device manufacturers are now switching on encryption by default on their devices, including mobile phones. This technology makes it difficult, if not impossible, to read the contents of the device when powered off or locked. It means that anyone who has access to the device itself must have the means to transform the data on the disk into an intelligible form — decryption therefore should, by design, be challenging to do without access to secrets known and/or held only by the user.

IX. Browse configurations and Ad-blocks

Cookies allow websites to store information in your machine. They are used for a series of purposes, including: to let websites determine how many visitors they have through installing a unique ID for every visitor (your computer); to store your preferences; and to enable functions such as "quick checkouts". Therefore, your unique ID can be used to associate your computer to pages you have viewed from the site, information you have given to the site in online forms, things you have selected, etc. Tracking cookies is commonly used to compile records of users browsing. This set of data can be used for a variety of purposes, such as advertisement and profiling of consumers. Therefore, cookies can have important implications for protecting privacy and anonymity while browsing. Most browsers support cookies by default, but also allow users to disable then.

Advertising companies use third-party cookies to track a consumer across multiple sites they visit, particularly those where it has placed advertising. This kind of knowledge about pages visited allows them to target advertisements according to a consumers presumed preferences. This presumption becomes more and more accurate with the increased amount of people being profiled. Besides setting up browser configurations to disable cookies, there are also browser plug-ins or extensions that block and filter advertisement. However, filtering doesn't mean that you are not being tracked, so disabling cookies might still be needed.

X. HTTPS/TLS

Hyper Text Transfer Protocol Secure and Transport Layer Security are protocols that enable secure communications between devices. The HTTPS/TLS protocols are used, as a rule, when you want to keep the information transmitted between the client and the server from being viewed by third parties, as in the case of online shopping. That is because it allows for data to be encrypted while transmitting and requests authenticity of the server and the client by checking digital certificates. That means that, using complex mathematical properties, large secret numbers are negotiated that are then used to scramble data as it moves between the two endpoints. The mathematics used by the algorithms means that an adversary who can observe all communications before the actual data is transmitted will not be able to determine how to decode the subsequent information.

The existence of a padlock in the address bar of your browser demonstrates that the page is certified and the use of the HTTPS protocol and the communication between the browser and the server will occur safely. Users can double click on the padlock to view the certificate and verify the identity of the server. HTTPS/TLS protocols are used for webpages and email but are now being increasingly deployed for software updates. Nevertheless, many websites still do not support encryption over HTTPS/TLS, but there are browser extensions and plugins that enable it by default. Finally, these technologies do not address the metadata problem or data on the devices themselves.

XI. Virtual Private Networks (VPNs)

Like HTTPS, VPNs secure communications in transit and they also aim to partially address the metadata problem. The connection between a device and the internet is mediated by a third party, the VPN provider, who will provide an encrypted channel for the communication to its servers. The VPN provider then becomes the conduit for the connection to the internet. However, given that the VPN provider will now have access to the metadata of users of its service rather than the user telecommunication provider, the problem is simply shifted to a different party rather than solved.

XII. The Onion Router (TOR)

TOR aims to address the metadata problem by routing packets through many locations with no one location knowing the source and destination of the communication. It also partially addresses communication security using encryption but if the two parties are not using encryption then potentially these communications will be accessible at the entry and exit nodes of the TOR network. Using end to end encryption such as PGP, HTTPS or TLS would prevent this sort of exposure while using TOR.

XIII. Off the Record (OTR)

OTR messaging, when implemented properly, generates a new and independent key for each communication in a session. The aim of this system is that an adversary would have to acquire all communications and both initial private keys to crack the communications. If a session key is compromised then only a small portion of the communications will be vulnerable. It also provides a degree of deniability to the parties to the communication session. However, some implementations do not generate and negotiate new keys for each communication to provide the requisite. Instead, repeated computations are performed on the initial secret key depending on the number of messages sent.

Chapter 4
Comparative Thematic Issues of Consumer Data Protection

This chapter offers an overview of the central thematic and legal issues concerning consumer data protection in Germany, China and Brazil, to show similarities and differences of the legal regimes and the institutional architecture in the three countries, which can be useful for further discussions on how to improve consumer data protection and cooperation between the countries.

I. Fundamentals and the existing legal framework

Although the economic and social situations in Brazil, China and Germany are highly diverse, they do have one constant development in common: The increase of Internet penetration throughout the population and the growth in the use of personal and corporate data of all kinds, transmitted and stored for public and private interests. As data and traces of data arise from any step or operation taken within the digital world, regardless of its originator or the technology used, the amount of data is very difficult to assess.

As a result, the growing markets of the Internet-based economy in every conceivable sector, as well as the collection and processing of data by public bodies,

are developments of vast economic importance. At the same time, these developments also highlight risks related to the personal data of natural persons as well as for business data.

Thus, Brazil, China and Germany find themselves in the middle of the global development of increasing interconnectedness in almost every sector of private and public life. Brazil, despite having no general data protection law, regulates data protection within the specific sectorial legislation (e.g. the financial sector) with regard to the special regulatory needs of each sector. Nonetheless, consumers' rights are protected through various provisions. The CDC contains provisions for the rights of individuals concerning protection of their personal data (privacy). This is also acknowledged as a constitutional matter, whereas the right of access to collected personal data derives from the Brazilian Constitution itself, specified within the *Habeas Data* writ.

The situation in China is comparable. While also lacking uniform law on personal information protection, the Chinese legislation contains provisions concerning consumer data protection in the relatively new Consumer Protection Law of 2014. Additional legislation on consumer protection, data protection and Internet services includes provisions deriving from various acts, decisions, notices, and guidelines. Despite this rather dispersed legislation, Chinese law on private consumer information protection derives from the historical unitary concept of private affairs (Yin Si, 隐私). This evolved towards the concept of privacy, which has now been replaced by the broader and more definable concept of personal information protection.

The German legislation, on the other hand, consists of a general data protection act regulating public and private processing of personal (and not corporate) data without limitation to the data subject being a consumer. The general law is supplemented by various sectoral provisions, especially in the telecommunications and financial sectors. German data protection law is based and reliant on European provisions and, therefore, currently represents the legislative parameters of the European Data Protection Directive (DPD). As this is being reviewed and is expected to be replaced by a new European General Data Protection Regulation (GDPR), German law is also about to encounter various changes.

II. Applicability of data protection acts

Concerning applicability of data protection acts, we have to distinguish between the international (cross-border) level (i.e. conflict of laws) and the national level, in particular how a data protection act may be applied to a specific case, for instance, in financial sectors.

1. Applicability to cross-border cases

Concerning the international scope of data protection regulation, two different approaches can be distinguished which are applied in most countries, in particular China, Brazil and Germany:

- A *market-based approach*, which focuses on how a service/data processing activity is addressed to a data subject in a country. Hence, the actual location (e.g. management headquarters, registration) of the data processor is irrelevant to the application of data protection law, which emphasizes the protection of the individual's data. Exemplarily, even if a data processor is based in the US, the fact that its services are addressed to individuals living in the relevant country suffices for a regulation to be applicable. This approach is largely being adopted by the new proposal of the GDPR in the EU and, thus, could also be the future law in Germany. Brazil seems to have also adopted this approach by applying Brazilian law in any case where services are addressed to a Brazilian audience, according to Art. 11 of the Internet Civil Rights Framework.

- In contrast, a *territorial approach* focuses on the headquarters and real seat of a data processor, sometimes also (or only) on the place where the data processing is taking place. Thus, it will be irrelevant if people outside the state where the data processor is being located are addressed by the services of the data processor; a territorial approach restricts the application of data protection law to those data processors which are based in the relevant state. One main argument of this approach is strongly related to the sovereignty of a state: As data protection law is, to some extent, part of public law and can only be enforced within a state, application of these provisions often follow the territoriality principle. It seems that this approach is dominant in China, where provisions on Protection of Personal Information of Telecommunication and Internet Users promulgated by MIIT restrict the application of data protection to those processing acts which take place in China. However, the Anti-Terrorism Law discussed requires that "those providing telecommunications and Internet services within the territory of China shall keep relevant facilities and domestic user data within China and shall not provide such services within the territory of China if refusing to do so" (Para. 3, Art. 15). Hence, here it seems to be sufficient that services are offered within China, forcing data processors to establish facilities and keep the data in China.

Moreover, the Data Protection Directive in the EU originally took the same stance by requiring a subsidiary or similar establishment to carry out the data processing in the EU. However, the European Court of Justice recently extended that scope in the "Google Spain" decision to any kind of ancillary activities of a data processor in the EU. As a result of this, even marketing activities will be sufficient for declaring the Data Protection Directive applicable. Hence, the EU currently has a mixed approach, somehow coming close to the market-based approach, but still relying upon some sort of foothold of the data processor inside of the EU.

2. Applicability on the national level

Concerning the applicability of data protection provisions on the national level, we have to distinguish between general data protection acts (such as the *Bundesdatenschutzgesetz* in Germany) and specific provisions regulating certain industrial sectors or services. Similarly, in Brazil, the *Habeas Data* writ seems to apply to most databases containing personal information. Regarding these general acts, their applicability depends mostly on personal data which is being processed outside the private or family sphere, Art. 3 (2) Data Protection Directive. On the other hand, both Germany and Brazil apply data protection provisions to private entities as well as to state authorities.

However, the existence of a multitude of specific regulations renders the task to assess legal requirements complex and difficult. In Germany, telecommunication acts as well as telemedia acts (referring to Internet communication) contain their "own" data protection provisions. The situation seems to be the same in Brazil regarding the Internet Civil Rights Framework. The general data protection act is subsidiary to those specific provisions. The same is true for consumer-related provisions, such as in Brazil, or for specific industrial sectors, such as financial regulations and social insurance.

III. Personal data

The definition of personal data is crucial for the application of the European Data Protection Directive (as well as the planned GDPR). The EU and German provisions are not linked to the notion of the consumer, but rather to that of the individual. Enterprises and legal persons are outside of the scope of the provisions. If data is being anonymized or pseudonymized, the data protection provisions no longer apply. The notion of personal data refers to any possibility to identify the individual related to the data; however, it remains unclear what effort has to be undertaken in order to declare data identifiable.

The EU data protection law distinguishes between "normal" personal data and highly sensitive personal data. The latter, according to Art. 8 of the European Data Protection Directive, includes references to racial or ethnic origin, political

opinions, religious or philosophical beliefs, trade union membership, and health or sex life. The proposed GDPR (LIBE) maintains this approach in Art. 9, even extending it to the processing of genetic or biometric data and data concerning administrative sanctions, judgments, criminal or suspected offences, convictions, or related security measures.

In contrast to the European situation, China and Brazil seem to concentrate more on the definition of "consumers" as part of the applicability of data protection. In general, a "consumer" is a natural person with regard to the needs of daily use (China). China does not yet have a definition of "highly sensitive information." Instead, it refers to a special treatment of specific kinds of data, such as in Art. 14 of the "Administrative Regulations on the Credit Reporting Industry" concerning credit reporting agencies which are prohibited from gathering information regarding religious belief, genes, fingerprints, blood type, and disease and medical history of an individual, and any other prohibited information.

By contrast, Brazil uses a broader definition of "the consumer" which is not restricted to contractual relations; corporate entities may be qualified as consumers if they are the final users. Finally, consumers are all persons being exposed to commercial practice or suffering from the damages of commercial activities. Concerning personal data, Brazilian law contains one definition in the Freedom of Information Law (Law No. 12.527 of 2011) which refers to information of identifiable natural persons. Additionally, Brazilian law acknowledges some specific sensitive data, such as in the Credit Information Law (Law No. 12.414 of 2011), however, this is restricted to loans. By contrast, the Internet Civil Rights Framework (*Marco Civil da Internet*) specifies basic information as a set of personal information in order to identify a citizen, such as their profession, address and parents' names.

IV. General guiding principles

The general guiding principles on data protection in the three countries show similarities in a number of areas.

In Germany, the Federal Data Protection Act lists seven basic principles of data protection:

1) the *legality principle* (the collection, processing and use of personal data is strictly prohibited, unless permitted by law or with the consent of the data subject);

2) the *principle of immediacy* (personal data has to be collected directly from the person concerned);

3) *priority of special laws* (as far as other federal laws concerning personal information including their publication are applicable, these enjoy priority);

4) the *principles of adequacy, necessity and proportionality* (the laws and procedures of data protection must be appropriate, necessary and must balance the rights and interests at stake proportionally);

5) the *principles of data avoidance and data economy* (data collection must be limited to the necessary minimum);

6) the *principle of transparency* (the data subject must be informed about the purposes of the collection, processing or use); and

7) the *specific purpose principle* (data can only be collected for a particular purpose; the use for a new purpose requires a law or consent).

The European Data Protection Directive explicitly sets out three categories of data protection principles:

1) the *principle of transparency* (data subject has the right to be informed when their personal data is being processed);

2) the *principle of legitimate purpose* (personal data can only be processed for specified, explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes); and

3) the *proportionality principle* (personal data processing must be adequate, relevant and not excessive in relation to the purposes of data collection).

In China, the "Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Network," and the Consumer Protection Law contain general data protection principles, among them:

1) the *principle of legality*,

2) the *principle of rationality* and

3) the *principle of necessity* of data collection, use and storage.

4) The *purpose, manner and scope* of collecting and using information must be indicated, and

5) the *prior consent* of data subjects is necessary, unless otherwise provided by law.

Additional principles are

6) the *transparency and public notification principle* (enterprises shall publish their rules of collection and use of data);

7) the *confidentiality principle* (enterprises shall keep personal information strictly confidential and not divulge, alter, damage, sell, or illegally provide personal data to others);

8) the *security principle* (to take technical and other necessary measures to ensure information security and prevent electronic personal information of citizens gathered during their business activities being leaked, damaged or lost); and

9) the *quality assurance principle* (to strengthen the management of information published by their users, immediately stop transmission of information prohibited by laws or regulations, take measures to remove the effects, keep the relevant records, and report to competent authorities).

Finally, the *Guideline for Personal Information Protection* contains the most comprehensive provisions and specifies eight principles for personal information protection:

1) *explicit purpose* (the processing of personal information shall have a specific, explicit and rational purpose, shall not expand the scope of usage and not change the purpose without notification of the data subject);

2) *minimal sufficiency* (only the minimal amount of information relevant to the purposes shall be processed; once the purposes are achieved, the said information shall be deleted as quickly as possible);

3) *public notification* (business operators shall inform, explain and alert the data subjects, and use clear and appropriate means to truthfully inform the data subjects about the purposes of information processing, the scopes of personal information collection and usage, measures for personal information protection, etc.);

4) *personal consent* (personal information shall be processed only after the consent of the data subjects has been obtained);

5) *quality assurance* (it shall be ensured that personal information is confidential, complete, usable, and updated in the course of processing);

6) *security assurance principle* (proper measures and technical means to prevent the possibility and the extent of personal information damage so as to ensure the security of personal information and prevent unauthorized search, disclosure, loss, leak, damage, and tampering);

7) *good faith principle* (processing of personal information shall occur in good faith and be stopped once the stated purpose has been achieved); and

8) *accountability principle* (to take proper measures to ensure the accountability for personal information processing and record the process for later track-back).

In Brazil, similar principles can be found in the CDC, the Credit Information Law and the Internet Civil Rights Framework, which make reference to the following principles:

1) the *specific purpose principle* (personal data shall be obtained only for specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes);

2) the *security principle* (appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data);

3) the *quality assurance principle (*consumer data must be objective, clear, truthful, and easily understood);

4) the *publicity principle* (publicity and clarity of any terms and conditions of the Internet connection providers and Internet applications providers shall be guaranteed);

5) the *transparency principle* (clear and complete information on the collection, use, storage, processing, and protection of users' personal data);

6) the *confidentiality principle* (nondisclosure to third parties of users' personal data);

7) the *consent principle*; and

8) the *good faith principle* (to eliminate personal data provided to a certain Internet application, at the request of the users, at the end of the relationship between the parties).

V. Restrictions to the collection, processing and transfer of (consumer) data

As personal data may result from any activity within online and offline data-networks, its handling (in the sense of collecting, processing and transfer) is subject to several restrictions. The Brazilian, Chinese and German restrictions, however, differ in various ways.

Brazilian law does not contain a general approach to the justification of collecting, processing and transfer of data. Lacking a general data protection law, rules for the handling of data can only be drawn from sectorial legislation. The Credit Information Law requires consent prior to any collection of the so-called "positive financial data." Additionally, the Internet Civil Rights Framework, requires a *provision of the law* or the user's *express, free and informed* consent prior to a transfer of data to third parties.

Chinese law, on the other hand, stipulates general rules. Network service providers and other enterprises and institutions are authorized to collect data if the prior informed consent of the user affected is given and if the enterprises adhere to the principles of legality, rationality and necessity, and state the purposes, manners and scopes of collecting and using information explicitly. Apart from that, specific sector rules may apply prohibiting institutions from collecting sensitive information. Depending on these sector provisions, explicit or mutual consent shall be given. However, the distinction between these two forms of consent remains ambiguous in Chinese law. In addition, credit reporting agencies may collect sensitive financial data if the user has been informed explicitly and has consented in writing. The collection of data is, thus, unjustified and regarded as illegal if obtained without prior consent or if the method of collecting or the use of personal data is not in line with the relevant general or specific sector laws and regulations. This would result in an infringement of the user's right of privacy. Apart from minor variations, the same preconditions apply with regard to processing and transferring data. A user needs to be informed explicitly before a data transfer can take place.

According to the European DPD and the German data protection act, processing may be justified by the user's consent, or by explicit allowances deriving from data protection or other specific acts. In addition, personal data should not be processed at all unless the data processing operator complies with certain requirements which are comparable to the Chinese requirements shown: transparency, legitimate purposes and proportionality. Moreover, the DPD allows member states to provide for exceptions for reasons of significant public interest.

The GDPR tightens the requirements for specific sensitive personal data given in the DPD and also includes other permissions for processing as exceptions to the continued approach of general prohibition of data processing. Consent of the user constitutes an exception, and the GDPR provides five other explicit exceptions: in the case where the processing is necessary for the performance of a con-

tract to which the user is party; for compliance with a legal obligation to which the controller is subject; in order to protect the vital interests of the user; for the performance of a task carried out in the public interest or in the exercise of official authority; or for the purposes of the legitimate interests pursued by the controller. With regard to the last exception, mere financial benefits for the user do not suffice to justify processing.

Apart from that, the challenges arising from new technologies, such as Big Data, are also being discussed within the framework of the GDPR. The traditional justifications for data processing of the DPD would not allow these new instruments as there are no explicit rules for it and an informed consent may not work out as a legitimation for Big Data processing.

VI. Approaches towards the principle of consent

Brazilian, German and Chinese law consider consent as one of the major justifications for data collection, processing, storing, and transfer. Nevertheless, the regulations of these countries are not entirely comparable in this respect.

In Brazil, there is no general approach to consent to the general handling of personal data. Nevertheless, the Internet Civil Rights Framework requires consent for processing personal data in cases of data processing via Internet connections. It obliges the provider to obtain the user's express free and informed consent. Thus, providers have to supply the user with enough information in order for them to know the context and the consequences of leaving data with the provider and the consent needs to correspond to the actual will of the user. Providers are, therefore, obliged to act in a transparent way when informing users and asking for their consent.

Chinese law, on the other hand, stipulates the general need for the user's prior consent to justify data collection. According to the Consumer Protection Law as well as various other sector and subsequent provisions, network service providers, enterprises and institutions shall, prior to gathering and using electronic personal information of citizens, obtain voluntary consent from whomever information is collected. Thus, collectors must give a prior statement in respect of their purposes, manners and scopes to obtain an effective consent of users and may not use standard terms and technical means to compel consumers to give consent. In case of a violation of these provisions, operators will be deemed as not having obtained the consent and shall bear legal liability.

Nevertheless, Chinese Law differentiates between implicit and explicit consent with regards to general and sensitive personal information. For general personal information, implicit consent is regarded as sufficient. However, in the case of a user's explicit objection to this collection, operators need to stop collecting or even delete the information in question. On the other hand, when sensitive personal information is collected, explicit consent from the data subject is required and, as a further protection mechanism, sensitive personal information may not be

collected from persons under 16 years of age or others with limited to no capacity to give informed consent. Unfortunately, these clear rules are undermined by the rather sketchy differentiation between general personal information and sensitive personal information. The latter's content depends on the user's will and, at the same time, on business-specific features in every single case. Sensitive personal information may, therefore, include ID number, telephone number, ethnic group, political views, religious beliefs, genetic information, fingerprints, and the like, whereas general personal information refers to any information other than sensitive personal information. Furthermore, disclosure of personal information to third parties without express consent of the data subject is prohibited as well as the transfer of personal information to foreign recipients, whereas such a transfer may be possible if explicit provision or approval of the relevant authorities is given.

Consent is of primary importance in European and German law. Most services can only be used if the individual affected gives their consent prior to personal data processing. This applies to the current as well as to the expected legislative situation. Both the DPD and the GDPR require the controller to obtain effective consent. This means informed consent given freely and unambiguously. A user is informed if they are given a set of certain information defined by DPD and significantly extended by the provisions of the GDPR. In this respect, the GDPR extends the scope of information which needs to be given and, unlike the DPD which requires information prior to the processing of data, obliges the controller to provide all relevant information prior to the collection of any data. Consent needs to be given freely, which means there can be no intimidation or other means of coercion undermining the user's freedom of choice. Consent also has to be unambiguous. In contrast to the situation in China, implicit consent as well as pre-ticked boxes shall not count as consent in order to protect the users from being influenced by the provider. Current and expected European and German law, thus, require explicit consent. Additionally, the new GDPR requires data controllers to provide standardized and easily legible information which has to be specified according to the individual circumstances of the data subject.

VII. Transparency

Any processing, storage and transfer of data happens either manually or, most probably, automatically and within digital data structures, such as servers. Thus, the vast majority of relevant processes involved in any of these processes are invisible to users, even though their personal data might be subject to these processes. With regard to the protective approach of the consumer and personal data protection regulations in question, service providers, controllers or processors are asked to provide transparency for users and partly also for the general public. Transparency is undoubtedly one of the main pillars of data protection regula-

tions. However, the approaches of Brazil, China and Germany towards transparency prior to, during and after the use of data are not entirely comparable.

In Germany, Art. 10 and 11 of the DPD and the German data protection act, request controllers to provide information about their identity, the purpose of processing, the recipient(s) of the data and, if necessary, further information to guarantee fair processing. The GDPR envisaged, on the other hand, is expected to extend this approach in different ways. According to the draft, controllers need to provide more detailed, standardized and easily legible information specific to the individual circumstances of the data subject even before personal data is collected. This would include the collection of data based on an explicit legal permission. Thus, the GDPR might demand much more from a controller and may have to be audited with regard to viability.

The situation in China, even though it is not as strict, is comparable to aspects of current and expected regulations in the EU and Germany, as service providers shall not collect or use (process) information in violation of laws, regulations or the agreement between user and provider. According to the "Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks" and subsequent relevant legislations, providers shall publish their collecting practices and also provide information stating the purpose, manner and scope of information collection and use prior to the collection of data.

In contrast to Germany and China, Brazilian provisions on information prior to data collection derive from consumers' legislation or specific sector laws: The CDC of Brazil, which applies to the treatment of personal data of consumers, also refers to the principles of transparency and information, as Art. 6, Para. 3 of this act requests "adequate and clear information about (...) services, with correct specifications for quantity, characteristics, composition, quality and price, as well as any risks involved" and, thus, considers information as a basic consumer right. Apart from this rather vague provision, the Credit Information Law also contains transparency rules. Nevertheless, these only apply to financial consumer data and are equally general in content, as they request the service provider to provide the consumer with enough information in order to know the context and consequences of their choice before processing and transferring financial data.

On the other hand, Brazilian law provides explicitly for the right to access and correct stored data. Deriving from the *Habeas Data* writ and, therefore, directly from the Brazilian Constitution, citizens are provided with a tool to access and correct their personal information stored by public bodies. As this procedure is restricted to public bodies and is relatively costly, slow and impractical for citizens, Brazilian law also provides access within the CDC and sector legislation, particularly in financial legislation. According to those, the consumers' files need to be accessible upon inquiry and must be objective, clear, truthful, and easily understandable.

Similar regulations can be found in Chinese legislation. Upon inquiry from the data subject, the information administrator shall notify whether it possesses this information, the content and status of such information, and shall provide this truthfully and free of charge.

The current European and German legislation also concentrates on the right to access and rectify stored data, and offers more precise provisions for users to obtain information about the data processed, stored and transferred by a controller or its representative. The expected GDPR, however, aims to extend these provisions by providing various additional kinds of data and information which need to be delivered. Furthermore, it will introduce an explicit right for data portability to obtain a copy of the stored personal data in an electronic and interoperable format which is commonly used and allows further use by the data subject. Currently, there are no similar provisions on data portability in Germany, Brazil or China.

Brazil has no regulation regarding notification of data breaches as yet. Any incident involving data breaches can be addressed by means of the ordinary civil liability if a data subject individually notices them or is informed by others.

Chinese law, on the other hand, usually requires the publication of violations, whereas the consumer law and diverse sector law requests comparable measures. However, the only provision that requires timely notification of the data subjects affected is the "Guideline for Personal Information Protection."

Neither the current legislation nor the GDPR require a public report on data protection. Instead, Art. 21 of the DPD requires member states to establish a register of processing operations which is kept by the supervisory authority and can be inspected by any person. The GDPR, however, extends European and German legislation with regard to transparency in all cases of personal data breaches. Breaches in data security shall be reported to the supervisory authorities or, should the breach occur at the processor, to the controller. Furthermore, the GDPR extends the general information obligations towards the user affected, who needs to be specifically informed of a personal data breach.

VIII. Responsibility

Since any collecting, processing or storing of data is of an inherent technical and organizational complexity (e.g. cloud services), the same complexity applies to the systems of responsibilities to ensure data security and protection in Brazil, China and Germany.

European and, thus, German law distinguishes between responsible entities, on the one hand, and processing entities, on the other hand. Whoever (alone or jointly) determines the purposes and essential means of data processing is regarded as a controller and, thus, responsible, whereas processors are legal entities processing the data on behalf of the controller. Therefore, the differentiation between controllers and processors is crucial. Whereas the definition of a controller

applies to the current (DPD) as well as to the expected legislation (GDPR), the ambiguity of the status of each entity within a more complex construction of data processing is problematic and may be subject to possible changes.

Furthermore, the responsibilities and measures to be taken by controllers are expected to become more differentiated. According to the DPD, single and joint controllers are required to comply with all provisions stated within the DPD and are, thus, responsible for informing the user and taking appropriate technical and organizational measures in order to avoid data leaks, data losses and illegal forms of personal data processing. In addition, all data processing by the processor is considered as done by the controller, whose responsibility is, therefore, not limited by outsourcing this processing of data. Consequently, all possible fees and court rulings will apply to the controller, regardless of their role (single/joint controller), as long as their responsibility for the processing of data can be established. The GDPR also asks controllers to inform users and adopt policies and implement technical and organizational measures to ensure that the processing of personal data is performed in compliance with these (partly new) regulations. This implies contractual as well as factual measures, such as examinations by the controller, which are explicitly laid down within the GDPR. If a processor conflicts with the instructions of the controller or if they become the determining party in relation to the data processing, they shall be considered to be a controller in respect of that processing, and will be subject to the rules on joint controllers and bear responsibility within these rules.

Similar to the German legislation, the "Decision on Strengthening Information Protection on Networks" of the National People´s Congress and the Chinese Consumer Protection Code require enterprises and institutions, when gathering and using the electronic personal information of citizens, to comply with the principles of legality, rationality and necessity, explicitly state the purposes, manners and scopes of collecting and using information, and obtain the consent of those from whom information is collected. Additionally, data administrators are required to take technical and other necessary measures to ensure data security and prevent leaks, damage or loss of citizens' data. Furthermore, administrators are responsible for promptly taking corrective measures in case of actual or possible data leaks, damages or losses. Regarding security measures, data security policies and procedures need to be followed. Anyone engaging in Internet information services shall entertain sound procedures to ensure network and information security, including procedures to ensure website security, a system to manage the security and confidentiality of information, and a system to manage the security of subscriber information. Moreover, telecommunications operators and Internet information service providers are required to take more specific actions to ensure data security and shall entertain self-inspections regarding the performance of user data protection at least once every year, record the results and timely remove potential security problems thus identified. Network service providers and other

enterprises shall, on the one hand, prevent the electronic personal information of citizens from being divulged, damaged or lost. On the other hand, they are asked to "strengthen the management of information" published by their users and shall immediately stop transmission if any information prohibited by laws or regulations is transmitted, and are required to take measures to remove the effects, keep the relevant records and report to the competent authorities. Generally speaking, legal responsibilities lie within the scope of factual responsibilities. Nevertheless, responsibilities of intermediate platforms and providers may be extended to third parties' content. If an Internet service provider fails to take necessary measures with regard to third parties' content which violates the rights of others, it shall be jointly and individually liable with the said third party. Furthermore, Consumer Protection Law requires online platform providers to be liable if they fail to provide the true name, address and valid contact method of the seller or service provider. If the Internet service provider is or should be aware that the seller or service provider is using their platform to harm legitimate consumer rights and interests, but fails to adopt the requisite measures, they shall bear joint and several liability.

Brazilian law does not distinguish between data controllers and data processors. However, the Internet Civil Rights Framework does distinguish between Internet connection providers and Internet application providers. All actors within the supplier's chain are subject to consumer law, which also applies to providing services in connection with data processing, and are, thus, responsible for ensuring consumers' rights within their services.

Whereas Brazilian consumer law approaches security as a consumer's right, data security as a responsibility is not stated explicitly. Nevertheless, the Internet Civil Rights Framework provides rules and responsibilities for the storage and processing of personal data. The storage of connection and application logs, which are considered personal data as well as communications data, shall comply with the protection of privacy of all parties directly or indirectly involved. Measures and procedures shall be published in a comprehensible way by each service provider, and are supposed to meet specific standards, set in a regulation of the Federal Government. Unfortunately, there is no such regulation to date. Therefore, the security standards have yet to be decided, which implies insecurity for users.

The issue of intermediary liability of Internet services is specifically regulated within the Internet Civil Rights Framework. Whereas Internet connection providers shall not be liable for civil damages resulting from content generated by third parties, Internet application providers may be held liable. Nevertheless, this liability is strictly limited to cases in which the application provider refrains from following a specific court order regarding content that was identified as being unlawful (e.g. blocking the content) or unjustified (e.g. refraining from removing con-

tent of a sexual nature after being informed of the unauthorized publication by the person affected).

IX. International transfer of data

Regarding the transfer of data across borders (in the case of the EU: to states outside the EU), the EU has established an elaborate scheme to ensure the same level of data protection as in the EU, whilst offering a set of tools in order to achieve that goal. Among these tools are standard contract clauses approved by the EU, binding corporate rules (also approved by supervisory authorities) and rules on the explicit consent of individuals to having their data transferred to third party countries. One of the most crucial exceptions, the so-called Safe Harbour Regime for US American-based enterprises, has come under serious attack in recent years. Thus, most cloud applications which are not restricted to EU servers are seriously affected. This approach is not being modified by the proposal of the GDPR.

By contrast, neither China nor Brazil have specific provisions in place to regulate cross-border data flow. It seems that China favors keeping data inside China as much as possible, such as stipulated by Art. 11, Para. 2 of the Law on Banking Regulation and Supervision and Art. 24 of the Administrative Regulations on the Credit Reporting Industry. Brazil does not seem to have any provisions regarding cross-border dataflow – despite the fact that some efforts had been undertaken to develop such a legal framework in the early 1970s.

X. Data retention

Regulations of data retention differ significantly in Germany, on the one hand, and China and Brazil, on the other hand.

In Europe and Germany, provisions on data retention contained in the European Directive on Data Retention and the German Telecommunication Act have been declared void by the European Court of Justice and the German Constitutional Court, respectively. The main arguments of the decisions of both courts referred to the unspecified powers for state prosecutors and the police to process data, as the relevant provisions did not implement necessary precautions (such as judicial control) for the individuals addressed. Moreover, both courts stated that there were no precautionary rules concerning the safety of retained data and controls of how the data could be used by third parties.

With regard to the judgment of the European Court of Justice, which is analyzed in further detail in the study, the court held that the retention of telephone communications meta-data concerning date, time, location, and type of communication for the purpose of preventing, detecting, investigating, and prosecuting crimes and safeguarding the security of the state severely interferes with the right to privacy. Therefore, its justification must comply with a high standard, especially

in the case of automatic data processing. The court criticized several shortcomings of the directive which affect the right to privacy in a disproportionate manner. Firstly, the directive allowed for data retention without requiring a specific relationship or linkage of the affected data subject to specific crimes, which were not sufficiently defined in the directive. Secondly, the directive did not specify the objective criteria regarding limits of access of national authorities to the data and their subsequent use. Thirdly, access to data was not subject to a prior review of a court or an independent administrative body. Finally, the time limits for the retention of data were formulated in a rather broad and unspecific manner. While the European Commission currently has no plans to adapt the data retention directive, the German government just recently presented a new proposal for a (national) data retention act.

In China, several sectorial regulations concerning telecommunication and the Internet, among them the "Telecommunications Regulations," the "Administrative Measures for Internet Information Services," the "Regulations on the Administration of Internet Access Service Business Sites," and the "Administrative Measures for Online Trading," deal with data retention. The regulations establish that operators of Internet access services shall register the users' IDs and record their Internet access information, keeping the records for 60 days and present them in case of inquiries by the culture administration departments or public security organs. Operators of third-party online platforms shall record commodity and service information released via the platform, online business operator's business licenses and personal identity, and transaction records for at least two years.

In Brazil, there is no general demand that data must be retained only for the time necessary to fulfill its purposes. Several laws, among them the CDC and the Internet Civil Rights Framework, determine that data concerning telecommunication, the financial situation of the consumer and the access logs to Internet applications can be retained for up to five years. Telecommunication enterprises must retain the logs (metadata) of telephones for one year. The CDC allows retention of relevant financial consumer data for up to five years. The Internet Civil Rights Framework establishes a mandatory minimal data retention period of one year for logs of access to Internet connection providers and six months for commercial Internet applications providers. The information subject to mandatory data retention includes the date, time, duration, beginning and end of the connection, as well as the IP address used for sending and receiving data packages. The data retention period can be extended upon request by the judicial authorities. In such cases, no time limit is envisaged.

XI. Enforcement

Enforcement measures can be of a civil, criminal or administrative character. Only Germany has created a Data Protection Officer who shall guarantee data protection in private corporations with more than nine employees and in public authori-

ties. In addition, the federal states have assigned federal data protection commissioners to monitor and supervise private and public bodies. The data protection officers enjoy independence and a special dismissal protection, but owe certain duties to the data protection supervisory authorities, e.g. cooperation and information duties. The European Data Protection Directive requires that its enforcement (and its implementation in national laws) is in the hands of independent supervisory authorities.

China has a highly decentralized structure for the administrative enforcement of personal information protection, as various administrative departments, e.g. the industrial and commercial administration departments, enforce such protection in their respective sectors or areas. There is no uniform and specialized agency for personal information protection.

In Brazil, the administrative departments that can address issues related to consumer privacy are part of the National System of Consumer Protection, a pool of public state and municipal bodies that can apply consumer protection legislation in order to protect consumers' data. A total of 786 public bodies exist currently, which are known by the name "Ombudsman for Consumer Protection and Defense." They are all autonomous in the application of consumer law to protect a consumer's privacy. Consumers can lodge a complaint before the governmental supervisory authorities, which can impose fines and determine that certain activities which infringe consumers' rights must be omitted.

With regard to civil enforcement, the European Directive contains a general liability rule for civil claims concerning damages suffered by the person affected, combined with a reversal of the burden of proof concerning the responsibility of the controller, stating that the controller may be exempted from this liability, in whole or in part, if they prove that they are not responsible for the event giving rise to the damage. The GDPR extends liability to processors. Even though the German Federal Data Protection Act offers a direct basis to claim compensation for violations, the bulk of civil court decisions referring to the violation of "personality rights" are based upon sec. 823 of the German Civil Code.

In China, the Tort Liability Law and the Consumer Protection Law contain liability clauses which offer compensation for violations of the right to personal information. In Brazil, a general liability rule can be found in the Civil Code, but the protection of consumer privacy is directly addressed by the CDC. It establishes various mechanisms and instruments for the effective judicial protection of the consumers, such as the "reversal of the burden of proof," "strict sense liability," and "indemnification of patrimonial and moral damages," among others.

Concerning criminal law, there are few provisions related to data protection, in particular sec. 44 of the German Data Protection Law. However, only a very few final convictions have been reported so far. The European Data Protection Directive does not enshrine such provisions, as the EU has no competence in criminal law. The lack of enforcement is one of the most important concerns of the cur-

rent data protection legislation. By contrast, the GDPR will oblige member states to introduce "penalties" which have to be "effective, proportionate and dissuasive" and provides for sanctions which are similar to antitrust fines.

In China, serious infringements of rights to privacy, reputation and personal information are sanctioned through several provisions of the Criminal Law and the Consumer Protection Law. The *Notice on Legally Punishing Criminal Activities Infringing upon the Personal Information of Citizens'* issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security in 2013 offers guidance on how to interpret and apply criminal sanctions. The criminal provisions have been applied in several cases concerning the illegal acquisition, selling and providing of personal information, but a uniform interpretation has still to be established.

The CDC of Brazil criminalizes some types of conduct directed against the consumer and their rights to adequate information. However, in practice, these conducts are rarely, if ever, sanctioned by courts.

XII. Self-regulation and co-regulation

Self-regulation takes place in the EU (and Germany), China, and Brazil, however, in different forms and with different legal frameworks.

In the EU, the Data Protection Directive encourages the adoption of codes of conduct in Art. 27. These codes of conduct have to be authorized by the supervisory authority in order to check their compliance with legal provisions. However, neither the directive nor the German data protection act provide for any legal obligation to enact these codes of conduct. The GDPR pursues this approach by encouraging codes of conduct according to Art. 38 (1), specifying the requirements for accreditation and monitoring of codes of conduct.
In Germany, the Association for Self-regulating the Internet (*Verein zur Selbstregulierung der Internetwirtschaft*) has developed such a code, in particular concerning geolocation services. However, in reality, hardly any codes are being enforced.

Regarding China, there seem to be a lot of industry regulations in place, such as the "Interim Measures for the Administration of Members' Credit Archives" ("Interim Measures"), issued by the Chinese Institute of Certified Public Accountants as the first systematic provision on members' credit information ever released (in 2004). Also, self-regulations can be found in some regions, such as the "Rules of Personal Information Protection for Software and Information Service Industry in Dalian (for trial implementation)" issued in 2006 by the Dalian Software Industry Association concerning personal information protection.

Moreover, Art. 21 of the "Provisions on Protection of Personal Information of Telecommunication and Internet Users" encourages telecommunications and Internet industry associations to formulate self-regulatory provisions on personal

information protection in accordance with the law, to guide members to strengthen self-regulation and to improve the level of user data protection.

By contrast, there are few self-regulation efforts in Brazil. The "E-mail Marketing Auto Regulation Code" (*Código de Autorregulamentação para a Prática de E-mail Marketing*) in 2009 forms an exception. Although, in a formal sense, the blocking of "door 25" by most of Brazilian providers cannot be assessed as self-regulation (lacking formal procedure, etc.), it still constitutes a significant effort to bundle resources in order to combat spam. Finally, attention is being paid in the upcoming bill on data protection to self-regulation as a standard market practice.

The rapid development of new information and communication technologies has changed people's everyday life and consumption patterns significantly. The worldwide spread of those technologies provides many innovations for consumers, but it can also bear risks, such as the indiscriminate collection, storage and cross-border flow of personal data, illegal spying on Internet activities, dissemination of personal information, and abuse of user passwords. The study deals with the current state of consumer data protection law in Brazil, China and Germany from a comparative perspective. It covers the main legal issues of consumer privacy and data protection in these countries and seeks to explain current issues and case law concerning consumer data protection from a practical perspective.

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

ISBN: 978-3-86395-236-5

Universitätsverlag Göttingen