EPRIVACY AND NEW EUROPEAN DATA PROTECTION REGIME

Marija Boban
University of Split Faculty of Law, Croatia
marija.boban@pravst.hr

ABSTRACT

The new EU General Data Protection Regulation (GDPR) ensures that personal data can only be gathered under strict conditions and for legitimate purposes. Organisations that collect and manage personal data must also protect it from misuse and respect certain rights.

From this point of view, the GDPR presents an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market in European union. In order to establish the digital single market, one of the important steps to develop the strategy, is the review of the ePrivacy Directive in order to provide the legal framework to ensure digital privacy for EU citizens.

The ePrivacy Directive builds on the EU telecoms and data protection frameworks to ensure that all communications over public networks maintain respect for fundamental rights, in particular a high level of privacy, regardless of the technology used. At this moment, digital privacy of citizens is protected with the ePrivacy Directive (Directive on Privacy and Electronic communications) which was last updated in 2009 to provide clearer rules on customers' rights to privacy.

A revision of the Directive is currently under in the process,in particular, according to the new requirements which were introduced on data such as "cookies" and on personal data breaches. In accordance with that, the author of this paper will give an overview of actualities in the challenges of ePrivacy in surrounding of new data protection regime as well as recommendations for a model of information data governance in order to comply the buisinesses to new legislation regulations set to May 2018 in global market surroundings.

Keywords: *digital privacy, data governance, data protection, digital single market, directive, ePrivacy, General data protection regulation*

1. INTRODUCTION

Information privacy, or data privacy (or data protection), is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. (Boban, 2014.p 116) Privacy, by it's definition, concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, such as genetic material, residence and geographic records, ethnicity, privacy breach, location-based service and geolocation, web surfing behavior or user preferences using persistent cookies. The challenge of data privacy in digital single market is to utilize data while protecting individual's privacy preferences and their personally identifiable information. The fields of computer security, data security and information security design and utilize software, hardware and human resources to address this issue. (Hasty, Nagel, Subjally, 2013)

As the laws and regulations related to Privacy and Data Protection are constantly changing, it is important to keep abreast of any changes in the law and continually reassess compliance with data privacy and security regulations. In this matter, ePrivacy has often been defined as the right of individuals to determine for themselves when, how and to what extent information about themselves is communicated to others. Assuming that the 'E' refers to electronic communication

and thus propose the ePrivacy is widely defined as privacy in the electronic age. (Huie, Laribee, Hogan, 2002), If we accept the above definitions then we have to accept that 'e-privacy' covers a wide range of e-communication which are threatened by electronic devices such as the Internet, mobile phones including email communication, social networking and blog sites, closed circuit television (CCTV) surveillance, phone tapping, hacking, camera phones, etc. (Kotzker, 2003) It is regulated in European Union by Directive 2002/58/EC on Privacy and Electronic Communications, otherwise known as E-Privacy Directive, is an EU directive on data protection and privacy in the digital age. It presents a continuation of earlier efforts, most directly the Data Protection Directive dealing with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies. This Directive has been amended by Directive 2009/136, which introduces several changes, especially in what concerns cookies, that are now subject to prior consent and also the new EU General Data Protection Regulation (GDPR) (GDPR, 2016) ensures that personal data can only be gathered under strict conditions and for legitimate purposes. From this point of view, the GDPR presents an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market in European union. Organisations that collect and manage personal data must also protect it from misuse and respect certain rights and in order to establish the digital single market, one of the important steps to develop the strategy, is the review of the ePrivacy Directive in order to provide the legal framework to ensure digital privacy for EU citizens. (Blackmer, 2016.) This proposed change will be carried on through to the legislation's final approval on 14 April 2016, potentially affecting entities around the world. The Regulation will apply to processing of data outside the EU that relates to the offering of goods or services to data subjects (individuals) in the EU or the monitoring of their behavior but it is questionable whether European supervisory authorities or consumers would actually try to sue US-based operators over violations of the Regulation. (Blackmer, 2016.) Additional changes will include stricter conditions for consent, broader definition of sensitive data, new provisions on protecting children's privacy, and the inclusion of "rights to be forgotten". (GDPR, 2016.)

2. THE RIGHT TO PRIVACY

The right to privacy is a highly developed area of law in Europe. All the member states of the European Union (EU) are also signatories of the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions.(Boban, 2012, p 577) The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence. Since the mid-1970s, the Organization for Economic Cooperation and Development (OECD) has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. In an effort to create a comprehensive data protection system throughout Europe, OECD in the year 1980, issued its first version of "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data".(OECD, 1980) The seven principles governing the OECD's recommendations for protection of personal data were:

- Notice—data subjects should be given notice when their data is being collected;
- Purpose—data should only be used for the purpose stated and not for any other purposes;
- Consent—data should not be disclosed without the data subject's consent;
- Security—collected data should be kept secure from any potential abuses;
- Disclosure—data subjects should be informed as to who is collecting their data;
- Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and

- Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles. (OECD, 1980)

The OECD Guidelines, however, were nonbinding, and data privacy laws still varied widely across Europe. The United States, meanwhile, while endorsing the OECD's recommendations, did nothing to implement them within the United States. However, all seven principles were incorporated into the EU Directive. (Shimanek, 2001, p 462).

The cornerstone of OECD work on privacy is its newly revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data named OECD 2013. Privacy Guidelines (OECD Privacy framework). (OECD, 2013) These new Guidelines constitute the first update of the original 1980 version that served as the first internationally agreed upon set of privacy principles. Actually, two themes run through the updated Guidelines:

- A focus on the practical implementation of privacy protection through an approach grounded in risk management, and
- The need to address the global dimension of privacy through improved interoperability.

The expert group also produced a report which identifies a number of issues that were raised but not fully addressed as part of the review process and which could be considered by candidates for possible future study. Also, a number of new concepts are introduced, including:

- National privacy strategies. While effective laws are essential, the strategic importance of privacy today also requires a multifaceted national strategy co-ordinated at the highest levels of government.
- Privacy management programmes. These serve as the core operational mechanism through which organisations implement privacy protection.
- Data security breach notification. This provision covers both notice to an authority and notice to an individual affected by a security breach affecting personal data. (OECD, 2013)

Also, it is important to note that in 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was negotiated within the Council of Europe. This convention obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did. The European Commission realised that diverging data protection legislation amongst EU member states impeded the free flow of data within the EU and accordingly proposed the Data Protection Directive.

3. DATA PROTECTION AND DIGITAL SINGEL MARKET

The General Data Protection Regulation, as one of the greates challenges of digital single market and strategy Digital Agenda for Europe, is adopted in April 2016, will supersede the Data Protection Directive and be enforceable starting on 25 May 2018. (GDPR, 2016) The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data – furhter DPD) was a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law. The directive was regulating the processing of personal data regardless of whether such processing is automated or not. Alhough GDPR regulation will supersede the Data Protection Directive and be enforceable starting on 25 May 2018 the most important legal definitions of personal data are still in force:

Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2 a DPD, 1995) This definition is meant to be very broad. Data are "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this

link. Some examples of "personal data" are: address, credit card number, bank statements, criminal record, etc.
The notion *processing* means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;" (art. 2 b DPD, 1995).
The *responsibility for compliance* rests on the shoulders of the "controller", meaning the natural or artificial person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; (art. 2 d, DPD, 1995)
The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data. (art. 4 DPD, 1995) Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation. In principle, any online business trading with EU residents would process some personal data and would be using equipment in the EU to process the data (i.e. the customer's computer). As a consequence, the website operator would have to comply with the European data protection rules. The directive was written before the breakthrough of the Internet, and to date there is little jurisprudence on this subject. (DPD, 1995)
The data subject has the right to be informed when his personal data is being processed. The controller must provide his name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. (art. 10 and 11 DPD, 1995)
Data may be processed only if at least one of the following is true (art. 7): when the data subject has given his consent; when the processing is necessary for the performance of or the entering into a contract; when processing is necessary for compliance with a legal obligation;
when processing is necessary in order to protect the vital interests of the data subject; 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; 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.
The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (art. 12, DPD, 1995)
The above given definitions were given by Data Protection Directive which has been a ground for doing business until April 2016 and adoption of GDPR. The European Comission has set a compliance date of 25 May 2018, giving resonable period for legal adoption into the national legislation as well as to business sector to prepare for new legal ePrivacy framework.

4. ELECTRONIC PRIVACY REGULATION

The Electronic Privacy Directive (further EPD) has been drafted specifically to address the requirements of new digital technologies and ease the advance of electronic communications services.[1] The Directive complements the Data Protection Directive and applies to all matters which are not specifically covered by that Directive. In particular, the subject of the Directive is the "right to privacy in the electronic communication sector" and free movement of data, communication equipment and services. (Fromholz, 2000, pp 471-472)
The Directive does not apply to Titles V and VI (Second and Third Pillars constituting the European Union). Likewise, it does not apply to issues concerning public security and defence, state security and criminal law. The interception of data was however covered by the EU Data Retention Directive, prior to its annulment by the Court of Justice of the European Union.

Contrary to the Data Protection Directive, which specifically addresses only individuals, Article 1(2) makes it clear that E-Privacy Directive also applies to legal persons. (art 1(2), EPD, 2009) The EU parliament has been discussing ePrivacy Directive and regulations around people's activities and behaviour being tracked online the past years. On May 25th 2011 it went into force. The new revised version was named the »*EU Cookie Directive*« becuse of it's »cookies« definitio which is amended privacy legislation designed to increase consumer protection. The Directive required websites to obtain informed consent from visitors before they store information on a computer or any web connected device. This is storage is mostly done by cookies, which can then be used for tracking visitors to a site. The previous privacy legislation required websites to give users information on how they could remove or opt-out of cookies, which was commonly placed in privacy policies that went mostly unread. With the EU Cookie Directive the user of a site has been required to opt-in when using a website containing cookies. So the website has to block cookies, until visitors have given their informed consent to their use. On the legal status it is important to note that so called EU Cookie Directive (Directive 2009/136/EC of the European Parliament and of the Council) is an amendment of the Directive 2002/58/EC, which concerns the protection of data and privacy on the web. The most important paragraph in the Directive 2009/136/EC. (EPD, revised, 2009)
The first general obligation in the Directive is to provide security of services (art 29, Data Protection Working Party Opinion, 2/2010) The addressees are providers of electronic communications services. This obligation also includes the duty to inform the subscribers whenever there is a particular risk, such as a virus or other malware attack. (art 29, Data Protection Working Party Opinion, 16/2011) The second general obligation is for the confidentiality of information to be maintained. The addressees are Member States, who should prohibit listening, tapping, storage or other kinds of interception or surveillance of communication and "related traffic", unless the users have given their consent or conditions of Article 15(1) have been fulfilled. The full history of decission making is presented at COM (2000) 385: Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. (COM, 2000)

5. TRANSITION TO THE GENERAL DATA PROTECTION REGULATION

On 25 January 2012, the European Commission (EC) announced it would attempt to unify data protection law across a unified European Union via proposed legislation called the "General Data Protection Regulation." The Objectives Of The European Commission's proposal will give EU companies a competitive advantage globally, as the Regulation would provide for:

- the harmonization of 27 national data protection regulations into one unified regulation;
- the improvement of corporate data transfer rules outside the European Union; and
- the improvement of user control over personal identifying data. (m law group, 2012.)

The package includes a draft "General Data Protection Regulation" (the "Regulation") that will be directly applicable in all member states of the European Union ("EU") replacing the patchwork of different data protection laws currently in force in the different member states. The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for US companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 2 % of worldwide turnover.
Proposed Changes To The Data Protection Law are highlighted in the draft Regulation we find the following remarkable changes to the data protection regime currently in force in Germany and the EU:

a) The EU data protection regulation will also apply for all non-EU companies without any establishment in the EU, provided that the processing of data is directed at EU residents. This may force for example US companies not only to comply with EU law, but also to establish a data protection management, for example by appointing an "European" data protection officer.
b) As a general rule, any processing of personal data will require providing clear and simple information to concerned individuals as well as obtaining specific and explicit consent by such individuals for the processing of their data (Opt-in), other than in cases in which the data protection regime explicitly allows the processing of personal data.
c) The Regulation will make a safe transfer of data outside of the EU (including the procession of data in clouds) easier in the event that the parties involved commit themselves to binding corporate rules.
d) New privacy rights, including data subject's "right of portability" and the "right to be forgotten", will be established in the EU. The "right of portability" will allow a transfer of all data from one provider to another upon request, for example transfer of a social media profile or email, whereas the "right to be forgotten" will allow people to wipe the history clean.
e) The processing of data of individuals under the age of 13 will in general require parental consent, which will make it more difficult for companies to conduct business which is aiming at minors.
f) All companies will be obligated to notify EU data protection authorities as well as the individuals whose data are concerned by any breaches of data protection regulations or data leaks without undue delay, that is within 24 hours.
g) A harsh sanction regime will be established in case of breach of the unified EU data protection law allowing data protection authorities to impose penalties of up to 2 % of a company's worldwide turnover in case of severe data protection breaches. (GDPR, 2016.)
The original proposal also dictated that the legislation would in theory "apply for all non-E.U. companies without any establishment in the E.U., provided that the processing of data is directed at E.U. residents," one of the biggest changes with the new legislation.
The compliance date set for May 2018 is giving businesses around the world a chance to prepare for compliance, review data protection language in contracts, consider transition to international standards, update privacy policies, and review marketing plans.

6. INSTEAD OF CONCLUSION: PROPOSAL OF MODEL OF INFORMATION GOVERNANCE

The goal of European legislators was to harmonise the current legal framework, which is fragmented across Member States. A 'Regulation' (unlike a Directive) is directly applicable and has consistent effect in all Member States, and GDPR was intended to increase legal certainty, reduce the administrative burden and cost of compliance for organisations that are active in multiple EU Member States, and enhance consumer confidence in the single digital marketplace. (Boban, 2016)
Establishing an effective information governance framework across the organization presents the best way of preparing for compliance and managing risk. Ideally this framework should adopt compliance 'building blocks' that reflect the key features of the Regulation, in order to comply the business preparation for the GDPR, as shown on diagram 1.

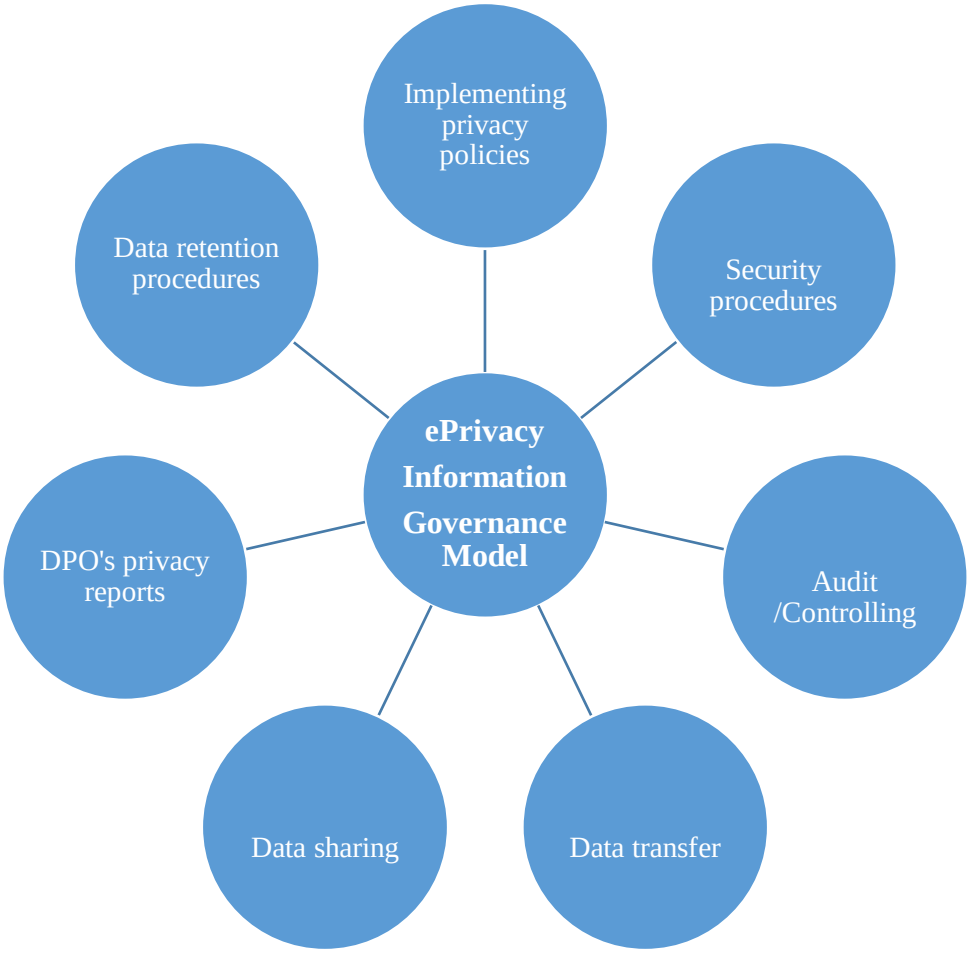

Diagram 1: Proposal of ePrivacy Information Governance Model based on GDPR

The main idea of the ePrivacy Information Governance Model is that GDPR is build on grounds of ePrivacy and data protection policies and strategies with compliance from the start of any new project - ensuring that privacy risk is identified and managed from the very earliest design-phase when creating new products and services. All procedures should include privacy impact assessments as a matter of routine, especially when considering new arrangements that may involve handling sensitive data fields, or large volumes of personal data following new GDPR regulations.

LITERATURE:

1. Blackmer, W.S. (2016). "GDPR: Getting Ready for the New EU General Data Protection Regulation", Information Law Group, InfoLawGroup LLP. (Retrieved 22 September 2016.)
2. Boban, M. (2012), Right to privacy and freedom of information in the modern information society. Proceedings of the Faculty of Law, Split.Vol 49 (2012), No 3 (105); pp 576-577
3. Boban, M. (2015), Covergence of technological innovation, global media, culture and economics in information society, Global Media and Socially Responsible Business, Collection of Scientific Papers of International Scientific Conference Media and Economy, pp 114 – 129
4. Boban, M., Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world", Proceedings of 16th International Scientific Conference ESD 2016., „The legal challenges of modern world", Split, 2016.
5. Data Protection Working Party Opinion (16/2011), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf ((Retrived 22 September 2016)

6. Data Protection Working Party Opinion (2/2010), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf ((Retrived 22 September 2016)
7. European communities - Electronic communications networks and services - privacy and electronic communications regulations (ECNS), (2011), available at https://www.dataprotection.ie/documents/legal/SI336of2011.pdf (Retrived 23 September 2016)
8. Fromholz, J.M. (2000), The European Union Data Privacy Directive, 15 Berkeley Tech. L.J., pp 471-472
9. General Data Protection Regulation- GDPR, (2016), OJ L 119, 4.5.2016, p. 1–88 (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, retrived 10. 08. 2016. from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
10. Harvey, D.W., White, A.(2002), The Impact of Computer Security Regulation on American Companies, 8 Tex. Wesleyan L. Rev. 505
11. Hasty, R., Nagel, T.W., Subjally, M. (2013), Data Protection Law in the USA. (Advocates for International Development, Available at http://a4id.org/sites/default/files/user/Data%20Protection%20Law%20in%20the%20USA_0.pdf (Retrived 22 September 2016)
12. Huie, M.C., Laribee, S.F., Hogan, S.D. (2002), »The Right to Privacy and Person Data: The EU Prods the U.S. and Controversy Continues, Comp. & Int'l L., Tulsa, pp 391-441
13. Kotzker, J., (2003), »The Great Cookie Caper: Internet Privacy and Target Marketing at Home and Abroad«, 15 St. Thomas L. Rev., pp 727-748
14. m law group, »New draft European data protection regime also to apply to all US companies processing data of European residents«, 2012., pdf available at http://mlawgroup.de/news/publications/pdf/2012_02_01-EU_data_protection.pdf (Retrieved 25 September 2016.)
15. Moshell, R.,...And Then There was one: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection, 37 Tex. Tech. L. Rev. 357, 358;
16. Procedure 2000/0189/COD, COM (2000), 385: Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, available at http://eur-lex.europa.eu/procedure/EN/158278, (Retrived 25 September 2016)
17. Shimanek, A.E. (2001). "Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles". Journal of Corporation Law. 26 (2), pp 462–463.
18. The Organization for Economic Co-Operation and Development- OECD Privacy framework (2013), available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Retrived 23 September 2016.)
19. The Organization for Economic Co-Operation and Development, OECD (1980) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Retrived 25 September 2016.)
20. Zaidi, K.(2003), Harmonizing U.S.-EU Online Privacy Law: Toward a U.S. Comprehensive Regime For the Protection of Personal Data, 12 Mich.St. J. Int'l L. 169