Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Fiona deals with personal data

An Introduction to Data Privacy

Contents

Glossary

BCR:
Binding Corporate Rules.

Data Controller:
Company which determines the purposes and means of the processing.

Data Processor:
Company which processes personal data on behalf of the Data Controller.

Data Protection Directive:
The EU Data Privacy directive.

Data Protection Laws:
The set of laws and regulations applicable to the processing of Personal Data. Depending on the country, the terms **"Data Privacy Laws"** may also be used.

DPA:
Data Protection Authority.

DPO:
Data Protection Officer or Data Privacy Officer.

Data Subject:
A person to whom the personal data relates.

EEA:
European Economic Area (all of the EU countries as well as Norway, Iceland and Liechtenstein).

EU:
European Union (Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom).

ICA:
Intercompany Agreement.

Personal Data:
Information relating to an indentified or identifiable person.

PET:
Privacy Enhancing Technology.

Sub-Processor:
Company which processes Personal Data at the request of a Data Processor for the benefit and under the control of the Data Controller.

Introduction

About this Booklet

This booklet has been written by the Capgemini Legal Department and is meant to be for you, whether you work in Sales, Delivery, HR, Finance, IT, Procurement or any other community.

All references to Capgemini in this booklet are also meant to refer to Sogeti as well as any other entity of the Group trading under a name other than Capgemini (e.g., Prosodie, CPM Braxis, etc...).

As Data Protection is becoming more and more important, we invite you to read the booklet in order to understand the different issues which you may come across in your daily work.

You should also be aware that the protection of Personal Data is a rule of behavior embedded in Capgemini's Code of Business Ethics that everyone at Capgemini is expected to follow.

With this booklet we aim to raise the legal awareness of the Capgemini employees so that everyone understands why it is important for Capgemini to take care of Personal Data.

In this booklet you will meet Fiona, who works within the delivery organization of Capgemini. In her role, Fiona has to deal with Personal Data belonging to clients of Capgemini. Together with Fiona we will discuss topics such as: What is Personal Data? Can you transfer Personal Data to another country on request of a colleague? What is the difference between a Data Controller and a Data Processor and why is that important? How should we deal with the Personal Data of our clients? What about data security?

Keep in mind that this booklet is just a summary of the most common and important Data Privacy issues. For more complete information and legal assistance, or if you have any questions about the booklet or a specific topic, please contact the Legal Department.

Note that, although this booklet is EU oriented, it applies to all Capgemini employees, even if you are located outside the EU. The reasons for the EU oriented approach are that the EU maintains the strictest privacy rules and that Capgemini headquarters are located in the EU.

About the Legal Department

The mission of the Legal Department is to participate in the Group's development by facilitating profitable business through professional, responsive and pragmatic legal support for all the Group's activities. The Legal Department provides guidance and review regarding applicable laws and internal regulations and policies. Furthermore, the Legal Department provides advice and support to Capgemini business units in public tenders, in the negotiation of contractual terms with clients, in contract management and in disputes. The Legal Department also advises the Group in queries and disputes relating to terms of employment. However, the Legal Department does not deal with personal questions of Capgemini employees.

Highlights

As you will notice in the booklet, each chapter ends with a Fiona's lesson learned. Please find below the highlights of this booklet, which consists of Fiona's lessons learned. You will also find a reference to the chapter which deals with the specific Fiona's lesson learned so that you easily find the right chapter.

- Personal Data means information relating to an identified or identifiable person. Be aware if you are dealing with Personal Data that you need to comply with Data Protection Laws **(chapter 1)**.
- Be sure that you understand whether the company is acting as a Data Controller or Data Processor, in order to know what obligations it must meet and because the responsibilities are different in each role **(chapter 2)**.
- Transfer of Personal Data to other countries may be restricted and is heavily regulated. In most cases, it is the responsibility of the Data Controller to meet the requirements, if any **(chapter 3)**.
- Be aware that transfer of Personal Data within the Capgemini Group is also considered as an international transfer of data and therefore needs to comply with the Privacy Laws **(chapter 3)**.
- Capgemini needs to process certain Personal Data of job applicants, its employees and former employees under the employee-employer relationship. Capgemini stores, uses and processes Personal Data in accordance with applicable Data Protection Laws **(chapter 4)**.
- It is important to obtain the client's consent on the sub-contracting of services to enable the processing of Personal Data by a Sub-Processor **(chapter 5)**.
- If any transfer of Personal Data abroad is contemplated, it is important to inform the client at the earliest and to obtain its consent **(chapter 5)**.
- Personal Data breach incidents can derive from an internal or external source **(chapter 6)**.
- In some countries, there is a legal obligation to report the data breaches to the DPA and to the Data Subjects, failure to do so could result in fines and/or criminal sanctions for Capgemini **(chapter 6)**.
- Liaise with the Legal Department to ensure that you address the Personal Data breach efficiently **(chapter 6)**.
- Always check with the Legal Department if a DPO has been appointed and refer data protection matters to him/her. If no DPO has been appointed, refer the matters to the local Legal Department **(chapter 7)**.
- Privacy by Design and Privacy Enhancing Technologies are to be taken into account as good options for (further) protecting our own as well as our client's Personal Data. Moreover, they provide excellent opportunities for selling extra software functionality **(chapter 8)**.
- Because of the international transfer of Personal Data, privacy is a core issue that needs to be considered carefully in cloud offerings. Security and portability of the data are important subjects which need to be tackled as well **(chapter 9)**.

1 Data Protection Laws – the Basics

Fiona works for Capgemini within the delivery organization. In her work, Fiona has access to the systems of the client. By having access to the systems, Fiona can view certain client data. These data include Personal Data, like the place of residence, email addresses and telephone numbers of the client's employees. In the past, Fiona heard something about Personal Data and the importance of privacy, but she actually does not know what that really means and what she needs to do, or not do. She asks her manager what Data Privacy is all about and what she needs to know in order to comply with the law. Her manager explains the following to her.

Data is stored everywhere and is included in many digital systems and databases. The law defines what is to be considered as Personal Data and how it needs to be protected.

Each country has its own Data Protection Laws and there are differences in the various laws. In the European Union (the "**EU**"), a Data Protection Directive was adopted to serve as the basis for the Data Protection Laws in the EU member states as well as in Norway, Iceland and Liechtenstein (together the European Economic Area, "**EEA**").

Important terms in Data Protection Laws

Note that depending on the country, the terms **"Data Protection"** and **"Data Privacy"** refer to the rules applicable to the processing of Personal Data, including the security measures necessary to protect such Personal Data. The terms are used indifferently in this booklet.

Data Protection Laws apply to the **processing** of **Personal Data**. As long as data is not "personal", the Data Protection Laws do not apply.

Personal Data means information relating to an identified or identifiable person. In most countries this does not include information about legal entities (like corporations), however in a few it does (for example Austria). Examples of Personal Data are name and address, email address, contact data (like a business card), but also date of birth, a photo, a social security number and all other data related to an identified or identifiable person. A date of birth on its own will not be Personal Data but if it is connected to a family name, it is to be considered as Personal Data, as it is identifiable to a person.

Processing has a very broad meaning. Processing includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, and disclosure by transmission, dissemination or otherwise and the alignment or combination, blocking, erasure or destruction of data. The fact that you can view or read the Personal Data on a screen is considered processing as viewing the data puts the copy onto your computer. So processing is just about anything that can be done to data.

Another term in Data Protection Laws which is important is **"Data Subject"**. A **Data Subject** is a person to whom the Personal Data relates. Within Capgemini there are several Data Subjects of which Capgemini processes the Personal Data. Examples are, amongst others, job applicants, employees of Capgemini, employees of Capgemini's suppliers, employees of Capgemini's clients and clients of Capgemini's clients.

Conditions for processing Personal Data

The processing of Personal Data needs to be done in accordance with the law and needs to be fair and accurate. Personal Data may only be processed when it is permitted by law and for a legitimate purpose (for example processing of employees' bank details for payroll management purposes, processing of clients' Personal Data for invoicing purposes). The manner in which Personal Data is processed must be consistent with its purpose.

The processing must be adequate, relevant and not excessive in relation to the purpose of the processing. Personal Data must not be stored longer than needed for the processing.

Note that the uncontrolled creation of temporary files where you extract some Personal Data from a client database and save it on an excel file is generally discouraged as it increases the risk of non-compliance with the law.

Rights of a Data Subject

Being a Data Subject and having your Personal Data stored in a database or used by an application, gives you certain rights.

First of all you have a right to be informed whether an organization (e.g., a private company, an administration, your employer, etc.) is processing your Personal Data, the purposes for which it is being processed, as well as what Personal Data is being processed.

As a Data Subject you can request to have access to your Personal Data and you also have the right to request the Data Controller to add, rectify, block and erase your Personal Data if it is incomplete, inaccurate or if the processing does not comply with the Data Protection Laws (for example, if certain Personal Data is unnecessary to hold for the purpose of processing).

Notification of the processing

In the countries of the EU, each country has a Data Protection Authority ("**DPA**"), which is the national authority in charge of implementing and enforcing Data Protection Laws.

In some countries it is necessary to send a notification or request an authorization from the DPA before any new processing of Personal Data can be lawfully started. The notification may include information such as the purpose of the data processing, the name of the Data Controller, the categories of Personal Data that will be processed and the security measures taken.

The notification may be done by the Legal Department or by the Capgemini Data Protection Officer ("**DPO**"), depending on the countries. Please contact your DPO or local Legal Department as early as possible, when a new application or database which includes Personal Data will be introduced, as the notification may take some time.

Note that more and more countries outside of the EU are also adopting Data Protection Laws to protect Personal Data and prevent security breaches. You should refer to your local Legal Department to inquire about applicable Data Protection Laws in your country and the countries where you do business.

Example

Capgemini Belgium introduces a new application to be used internally to collect and manage information about the persons to contact in companies that are Capgemini Belgium's prospective clients. The application will contain information like name, surname, title and professional contact details and a history of the commercial relationship. As this information is related to an identified or identifiable person, it falls under the qualification of "Personal Data" and is subject to Data Protection Laws.

Because Capgemini Belgium will be working with the application and the data within the application, Personal Data will be processed. As a consequence, it may be necessary, before the processing starts, to notify the local DPA. The purpose of the processing is determined as "prospective client management" and Capgemini Belgium is keen on processing only the needed and relevant data.

Any employee of Capgemini Belgium's client or prospective client whose Personal Data is collected and processed by Capgemini Belgium is a Data Subject and therefore has the right to request that his/her Personal Data be updated if it is incorrect, for example if a prospective client's employee is promoted and changes his/her professional title.

Applicable sanctions for non compliance with Data Protection Laws

In some countries, the DPA has enforcing powers with regards to compliance with Data Protection Laws. It may conduct investigations and impose financial penalties. It can also publicize information on any non-compliance with the law, which may be very harmful for the company's reputation and client trust. It is therefore necessary to strictly follow all Privacy Laws.

Fiona's lesson learned

Personal Data means information relating to an identified or identifiable person. Be aware if you are dealing with Personal Data that you need to comply with the Data Protection Laws.

2 Data Controller and Data Processor

Now that Fiona knows in general what Data Privacy is about, she feels confident and she discusses this with a colleague. Her colleague is already aware of the basics and asks Fiona whether she knows if Capgemini is a Data Controller or a Data Processor. Fiona is surprised; apparently she is not aware of all important terms yet, so she visits the Legal Department to get a better understanding of another important topic. This is what the Legal Department tells her about the terms Data Controller and Data Processor.

Data Protection Laws distinguish between the **Data Controller** and the **Data Processor**.

The **Data Controller** determines the purposes and means of the processing of Personal Data and decides what data will be collected. Often the Data Controller is the company which originally collected the Personal Data from the individual.

The **Data Processor** processes the Personal Data on behalf of the Data Controller. The company that is carrying out the processing, asked or instructed to by the Data Controller will usually be the Data Processor. For example, in providing outsourcing services to its clients, Capgemini is usually the Data Processor and the client is the Data Controller.

There are instances where the company is at the same time the Data Controller and the Data Processor, for instance when it collects the Personal Data of its employees and processes this data on its own IT systems.

Obligations

There are obligations imposed on the Data Controllers, as well as on the Data Processors depending on the jurisdiction. In many countries, most of the obligations that are specified in the Data Protection Laws are imposed on the Data Controllers, but this depends on the jurisdiction.

Obligations of the Data Controller under the Data Protection Laws are for example:

1. The processing of the Personal Data must be lawful
2. The processing of the Personal Data must be specified, explicit and for legitimate purposes
3. The Personal Data must be accurate and up-to-date
4. The Personal Data must be kept for no longer than necessary
5. Under EU law, Personal Data must not be transferred outside the EEA unless certain conditions are met.

The main obligation for the Data Processor is to act as requested by and agreed with the Data Controller.

In addition, the Data Controller and the Data Processor are under the legal obligation to enter into a contract to define the security measures to be taken by the Data Processor. Since by law Personal Data must be held only for as long as necessary, the contract should provide that upon termination, all the Controller's Personal Data is returned or destroyed by the Data Processor.

When Capgemini acts as a Data Processor at the request of a client who is a Data Controller, it is essential that the contract define the obligations of the parties clearly so that Capgemini does not bear more obligations than what is required by law. In addition, the Data Controller must guarantee to Capgemini that it has complied with all its obligations so as to ensure that Capgemini would not be breaching the law when processing the data at the request of the Data Controller.

Example

Capgemini USA contracts a payroll service provider to manage the Capgemini USA monthly payroll.

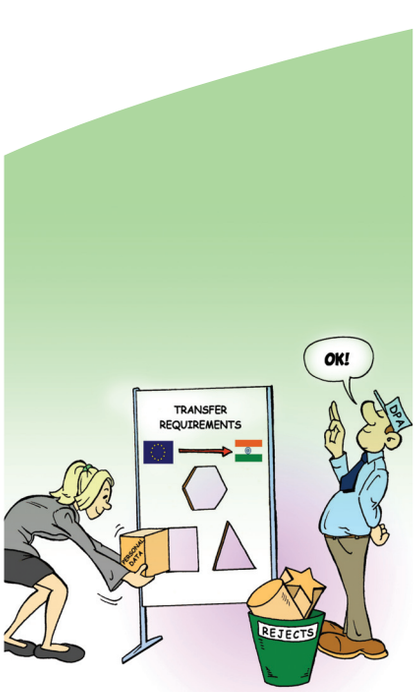
Capgemini USA will be the Data Controller and will give instructions to the payroll service provider on how to manage the payroll. The payroll service provider is the Data Processor. This means that Capgemini USA needs to determine the technical and organizational measures to protect the Personal Data. Capgemini USA also needs a contractual right to audit or review the procedures and practices in place with the service provider. Upon termination or expiration of the contract, Capgemini USA will need to make sure that the Personal Data will be returned (or destroyed) by the payroll service provider.

Fiona's lesson learned

Be sure that you understand whether the company is acting as a Data Controller or Data Processor, in order to know what obligations it must meet and because the responsibilities are different in each role.

3 Transfer of Personal Data to Other Countries

Fiona knows Capgemini uses offshore locations (like India for example) for the delivery of services to clients. Fiona is working for a client where the hosting services will be delivered by a Capgemini office in India. As Fiona just learnt the basics of Data Privacy, she realizes that her colleagues in India are actually processing data. Since they are located in India, it means that the data needs to be transferred /downloaded in India in order for it to be processed. Fiona is not sure whether that is allowed, so she calls a colleague from the Legal Department to help her. Here is what he said.



In many cases, client services will be performed in a country different from the country of the client. If Personal Data is involved, this means that these Personal Data that have been collected in a given country will be transferred to another country. Logging on to a system or having the possibility to view the data already qualifies as a transfer of Personal Data. This cross-border transfer is sometimes restricted.

Applicable law

The law that applies to a transfer of Personal Data, is the law of the country **where the Personal Data was originally processed,** i.e., the law applicable to the Data Controller. Such law defines the conditions that the Data Controller needs to respect in order to lawfully transfer the Personal Data abroad. By imposing conditions on the international transfer of Personal Data, the law applicable to the Data Controller ensures that the necessary level of protection of Personal Data will be applied in the country where the data is sent to.

The rules for the transfer depend on the law applicable to the Data Controller and need to be verified on a case-by-case basis. Note that these rules apply not only when you transfer Personal Data to a third-party entity but also when you transfer Personal Data to an entity of the Capgemini Group located in another country.

Keep in mind that in all cases a contract must be signed between the Data Controller and the Data Processor to organize the transfer of data. Please ask the Legal Department for assistance.

Transfer of Personal Data from a country located in the EU

If you are transferring Personal Data from a country located in the EU, the Data Protection Directive makes an essential distinction based on whether the data collected in an EU country is transferred to a country of the EEA or is sent to a non-EEA country:

1. If you transfer Personal Data from a country located in the EU to another country located within the EEA, such transfer is not regulated at the European level. However, please check whether there are specific obligations in the local law which needs to be met (such as for instance the need to obtain the prior consent of the Data Subject).

2. If you transfer Personal Data from a country located in the EU to a country located outside of the EEA, the applicable rules will vary depending on the level of protection afforded by the laws of the country where the Personal Data is sent:

a. If the entity receiving the data is located in a country that is regarded as having an "adequate level of protection" as defined by the European Commission, the transfer will be possible. The European Commission keeps a list of countries whose level of protection is regarded as "adequate". This list only contains a limited number of countries and will change over time, so please contact the Legal Department to check if the country where you are sending the Personal Data is on that list.

b. If the Personal Data is sent to the United States, you need to check if the legal entity that will receive the Personal Data is registered with the US State Department as being "Safe Harbor" certified. The Safe Harbor privacy principles allow US companies to certify that they comply with the EU data protection requirements, which in turns enables the lawful transfer of Personal Data from countries of the EU to Safe Harbor companies in the US without a specific data transfer agreement. Note that Capgemini in the US is not currently Safe Harbor certified.

c. For transfers to all other countries or if the US entity is not Safe Harbor certified, it will be necessary to enter into a specific data transfer agreement with the entity receiving Personal Data. Such agreement will have to be based on standard contractual clauses drafted by the European Commission so as to ensure that the receiving entity commits to the principles defined in the Data Protection Directive.

Note that if Personal Data is encrypted or in another way secured (like scrambled) so that a person can no longer be identified, the data does not qualify as Personal Data anymore and the Data Protection Laws are no longer applicable in that case.

Transfer of data from a country not located in the EU

If you are transferring Personal Data from a country not located in the EU, it may be the case that local law does not regulate the international transfer of Personal Data. You should always contact the Legal Department in advance of any transfer to verify this point.

In cases where Capgemini provides services to a client, the client is the Data Controller. It is therefore necessary to inform the client at the earliest stage if the service will be performed offshore in order to enable the client to comply with the rules applicable to the international transfer of Personal Data.

Approval Data Protection Authority

In some countries of the EU (for example in France), the law determines that in addition to the conditions imposed by the Data Protection Directive as mentioned above, the Data Controller also needs to obtain approval from the local DPA before Personal Data can be transferred outside of the EEA. Find out the rules applicable to your country by contacting the Legal Department.

Example

Client X in France (Data Controller) is outsourcing its application management to Capgemini in France (Data Processor). Within Capgemini, part of the execution of the services will be delivered by Capgemini India (Sub-Processor). The client's data will be stored on a server to which our employees at Capgemini India have access and will download in order to provide the application management services.

As soon as employees download data from India, the data will be transferred to India. If Personal Data is involved this means that there will be a transfer of Personal Data to India. This is considered to be an international transfer of Personal Data from France to India. As France is part of the EU, and India is not regarded as "adequate" by the European Commission, this transfer will need an approval from the French DPA to be given to Client X, prior to the transfer. In addition, Client X will have to sign a contract based on the standard contractual clauses drafted by the European Commission with Capgemini India to ensure that although not located in the EEA, the Sub-Processor shall be bound by the standard obligations of the Data Protection Directive when processing Personal Data originating from France.

Downloading Personal Data from abroad

Note that if you log on to the system and you download Personal Data while you are abroad there will be a transfer of Personal Data. Please be aware that, depending on the country you are in, there might be restrictions. For example, you are working for Capgemini Germany and you are on a mission in South Africa. Whilst you are there, you need to do some work which requires downloading Personal Data on your laptop.

This action will be restricted under EU law. Contact the Legal Department for more information.

Binding Corporate Rules

Finally, EU law also enables international groups to adopt Binding Corporate Rules (**"BCR"**) that serve as a group internal global privacy policy and that needs to be approved by the DPA of the countries of the EU to certify compliance with EU standards. BCR may be available as an alternative means of transferring data outside of the EEA, but they cover only the international transfer of Personal Data within the same group of companies and apply only to Personal Data in relation to which the company is a Data Controller (e.g., employee and customer databases). BCR do not apply to Personal Data processed by a Data Processor for its clients. Note that Capgemini has not, so far, implemented BCR.

Fiona's lesson learned

Transfer of Personal Data to other countries may be restricted and is heavily regulated. In most cases it is the responsibility of the Data Controller to meet the requirements, if any.

Be aware that transfer of Personal Data within the Capgemini Group is also considered as an international transfer of data and therefore needs to comply with the Privacy Laws.

4 Data Privacy and HR Data within Capgemini

In her work Fiona deals with a lot of data. She has insight into all different kinds of personal client data.

Thinking about that, Fiona realized that her own Personal Data are also in databases and used by applications within Capgemini, for example her contact details, but also financial data and her CV. She wonders how Capgemini deals with her own data and so gives the HR department a ring. This is what HR tells her.

HR data

Capgemini holds various information about employees and former employees, as well as applicants and other third-parties working on the Group's behalf. This information may include information such as contact, salary, bank details and recruitment information. Much of this information has been collected directly from the employees.

Purpose

As mentioned before, in order to process Personal Data you need to have a legitimate purpose. Generally, Capgemini collects this type of information where there is a clear and foreseeable purpose which is connected with Capgemini's business activities. Typically, these purposes will be work-related. Capgemini will store, use and otherwise process the Personal Data in a manner compatible with the purpose(s) for which it was originally collected.

Storage and access

Storage of Personal Data will be done in compliance with the applicable laws and regulations. For example, Personal Data cannot be stored for an unlimited period of time, so the local law will determine a retention period for data, after which the Personal Data needs to be destroyed. Moreover, Personal Data of employees cannot be accessed by just anyone within Capgemini. Only those employees who have a need to know, for business, HR or legal reasons can have access to this data.

Example

The Capgemini Group introduces a new application with regard to performance management. It is an internal application which will be used by the HR department. In the application there is data like name, date of birth, date of employment and data related to performance. As this data is related to an identified or identifiable person, it falls under the qualification of "Personal Data" and is subject to Data Protection Laws. The application will collect and store the Personal Data and Capgemini will work with the application, which means that Personal Data will be processed. This means that it may be necessary, before the processing starts, to notify the local DPA. The purpose of the processing is determined as "performance management" and Capgemini is keen on processing only the needed and relevant data.

As Fiona is an employee of Capgemini, her Personal Data will also be processed. Fiona is a Data Subject and has therefore the right to request that her Personal Data be updated if, for example, she changes her name after getting married.

Rights of employees

Current employees or former employees of Capgemini, who have had their Personal Data processed, have certain rights. For instance, they are entitled to be informed whether Capgemini is processing their Personal Data, as well as the purpose for which it is being processed and which Personal Data is processed. They also have the right to request to add or correct data which is incomplete or inaccurate.

Offshoring

As Capgemini has data centers in various countries, the Personal Data of employees and former employees may be stored, processed and accessed by Capgemini anywhere in the world. Capgemini has ensured that the Personal Data of employees and former employees are stored, processed and transferred everywhere in accordance with the applicable laws of the country where the Controller of such Personal Data is located and that access is limited only to the employees who have a need to know.

Works Council

The International Works Council and the local Works Councils are consulted, when required by law, on the processing and international transfer of Personal Data of Capgemini employees.

Fiona's lesson learned

Capgemini needs to process certain Personal Data of job applicants, its employees and former employees under the employee/employer relationship. Capgemini stores, uses and processes Personal Data in accordance with applicable Data Protection Laws.

5 Data Privacy when Capgemini is Supplier

While executing a project for, or providing maintenance to a client, Capgemini acts as a supplier. An IT supplier such as Capgemini often deals with Personal Data of the client's employees, suppliers or customers. Fiona wonders whether an additional Data Processor may be used in this process. Fiona knows that Capgemini is the Data Processor but is not familiar with the fact that there also can be an additional Data Processor. She asks her manager who explains how this works.

In a client negotiation it is important to be clear about which entity is the Data Controller and which entity is the Data Processor, as the obligations and liabilities are different. The Data Processer is processing Personal Data under the direction of the Data Controller.

In general, where Capgemini provides services to its client, Capgemini will be a Data Processor for the client's data because Capgemini processes the data for the benefit and under the control of the client (the Data Controller). This means that the client gives instructions to Capgemini on how to process the Personal Data. The contract between the client and Capgemini needs to clearly define the obligations of each party.

Sub-processing

Capgemini will often want to use a sub-contractor for the provision of some of the services. In this situation, the Capgemini entity which signed the contract with the client is to be qualified as the "**Prime Contractor**". In such cases, Capgemini needs first to verify that the client authorizes the sub-contracting of part of the services to another entity.

The Prime Contractor can subcontract part of the services to a "**Sub-Contractor**" which can be another Capgemini entity, like the Capgemini entities in India, or an unrelated third party. In both cases the Prime Contractor is still the Data Processor. The Sub-Contractor, whether a Capgemini entity or a third party, is an additional Data Processor, i.e., a "**Sub-Processor**".

Example

Capgemini UK closed a BPO contract with a bank in the UK, where the bank will outsource the human resources, finance and accounting processes. In the deal, the parties agreed that the client - the bank - determines the guidelines on how the business processes will need to be handled by Capgemini UK. As the data will be processed by Capgemini UK under the client's instructions, Capgemini UK is the Prime Contractor (Data Processor). The client is the Data Controller. In order to be competitive in terms of price, Capgemini UK offered that the services will be partly delivered by Capgemini India. Capgemini India is therefore a Sub-Contractor and as far as data protection is concerned is also qualified as a Sub-Processor. Capgemini India will process the data for the benefit of the client. As the client is the Data Controller and is located within the EU, it is the client's obligation to make sure that the transfer of Personal Data to India meets the requirements of UK Data Protection Laws.

This Sub-Processor is processing data for the Prime Contractor but the processing is done for the benefit and under the control of the client.

Note that the Prime Contractor remains responsible for the overall proper protection of the data towards the client. As the Prime Contractor (Data Processor) is responsible for the acts of the Sub-Contractor (Sub-Processor), the contractual issues with the Sub-Contractor must be arranged in a good way to ensure that the Sub-Contractor complies with all the provisions contained in the original contract signed between the client and the Prime Contractor (so that there is no potential additional liability for the Prime Contractor).

When services are subcontracted to a Capgemini entity, intercompany agreements **("ICA")** ensure the flow-down of all contractual conditions to the Sub-Processor. In some instances, it will be necessary for the client and the Sub-Processor to sign a specific agreement based on the standard contractual clauses of the European Commission.

In the event the Sub-Contractor is located in another country, be aware that there might be conditions which need to be met regarding the transfer of Personal Data prior to processing. For further details see chapter 3 of this booklet about transfer of Personal Data to other countries.

For countries within the EEA, the client should always be made aware, at an early stage, that some part of the services may be provided from outside the EEA and that some filings may be required by the local DPAs. This is critical as the inability for Capgemini to transfer the Personal Data to off-shore sites will have significant impact on the price of services offered to the client.

Entities	Legal qualification	Data Protection qualification
Bank	Client	Data Controller
Capgemini UK	Prime Contractor	Data Processor
Capgemini India	Sub-Contractor	Sub-Processor

Fiona's lesson learned

It is important to obtain the client's consent on the sub-contracting of services to enable the processing of Personal Data by a Sub-Processor.

If any transfer of Personal Data abroad is contemplated, it is important to inform the client at the earliest and to obtain its consent.

6 Personal Data Breach Notification

Fiona is currently managing a contract where Capgemini is providing cloud services to several clients of the banking, the insurance and the defense sector. Capgemini is also hosting client's data on its servers. There is a rumor that a month ago the Capgemini servers were accessed by unauthorized third parties. However, no one reported the incident to her. She is concerned about the implications that this may have on Capgemini. She then decides to consult the Data Privacy booklet to know more about data breach notification and how to address the incident efficiently.

What constitutes a Personal Data breach?

A Personal Data breach is a security incident in which Personal Data is copied, transmitted, viewed, lost, stolen or used by a third party who is not authorized to do so.

Data security breaches can happen for a number of reasons: loss or theft of data or equipment on which data is stored (including your own PC or other mobile devices), inappropriate access controls allowing unauthorized use, equipment failure, human error, unforeseen circumstances such as a fire or flood, hacking attack, blogging offences where information is obtained by deceiving the organization that holds it, etc.

Data breach notification

In some countries, there is a legal obligation to report data security breaches. Within the EU for instance, there is a compulsory notification requirement for internet service providers and telecommunication operators for any breach of security leading to the loss, destruction or unauthorized disclosure of Personal Data (a Personal Data breach).

Personal Data breach notification is the procedure followed by a company when reporting a breach to a DPA and informing the Data Subjects whose data is concerned by the breach. The data breach notification attempts to mitigate any damage caused by a data breach.

There might be a similar procedure which is provided by the law in your country. Please check with the Legal

Example

Capgemini France provides BPO services to a French telecom operator (the Data Controller). In performing the services, Capgemini France (the Data Processor) will be processing Personal Data of the telecom operator's clients (the Data Subjects). The contract between the telecom operator and Capgemini France determines that the Data Controller must immediately be informed of any security incident to ensure compliance with data breach notification obligations applicable under French law. Following an equipment failure that led to the loss of data, Capgemini France must immediately notify the Data Controller, which in turn will have to notify the French DPA of the security breach. If the security breach leads to the unauthorized disclosure of Personal Data and therefore potentially harms the privacy of the Data Subjects, the latter will also have to be informed of the data breach by their telecom operator.

Department if this there is such an obligation in your country.
Failure to comply with such laws could expose Capgemini to a fine and/or to criminal sanctions.

In any event, Capgemini has to ensure its clients and suppliers that it takes appropriate and proportionate security measures against unauthorized or unlawful processing and against accidental loss, destruction or damage to Personal Data.

The importance of managing data breach incident for Capgemini

Whether the breach is minor or serious (e.g., sensitive data accessed, high volume of data hacked, real risk of individuals suffering some harm), a data breach has to be handled carefully. Where reporting to the DPA is required by law, it should be performed immediately. In other cases, the potential harm to individuals whose data is lost is the overriding consideration when deciding whether a data breach should be reported to the DPA or communicated externally. Overall, bad management of a data breach could seriously damage Capgemini's reputation in the market and could result in a loss of business opportunities and clients.

Fiona's lesson learned

Personal Data breach incidents can derive from an internal or external source.

In some countries, there is a legal obligation to report the data breaches to the DPA and to the Data Subjects, failure to do so could result in fines and/or criminal sanctions for Capgemini.

Liaise with the Legal Department to ensure that you address the Personal Data breach efficiently.

7 Data Protection Officer

Fiona realizes that Data Privacy issues are present everywhere all across the company's internal or external activities. Given the complexity of Data Protection Laws and the fact that processing of Personal Data is at the core of Capgemini's activities, Fiona wonders if it would not be easier to have a single point of contact for all Data Privacy related issues. Could it be that privacy is such a big issue that a specific department within the company be in charge of it? She goes to the Legal Department to further inquire about this. This is what she learns.

In certain countries, the law imposes on companies the obligation to appoint a Data Protection Officer (**"DPO"**) to ensure compliance with Data Protection Laws. In Germany, for example, companies with more than 9 employees who are permanently employed in the automated processing of Personal Data have the obligation to appoint a DPO and face administrative fines if they fail to do so. As a consequence, Capgemini in Germany has appointed several DPOs.

In some other countries, like in France, for example, the companies are merely encouraged to appoint a DPO to ensure compliance with the law and facilitate the relationship with the French DPA. As a consequence, Capgemini in France has appointed three DPOs who keep official registers of all data processing performed in France and liaise regularly with the French DPA (the "CNIL").

Under current EU law, there is no obligation for companies to appoint a DPO. However, a January 2012 EU draft Data Protection Regulation would make it compulsory for companies processing Personal Data (as part of their business activities or as a core activity) and employing more than 250 employees to appoint a DPO. Such DPO would be in charge of all data protection related issues within the Group and would advise on applicable law, monitor the implementation of data protection policies, perform trainings and audits, perform appropriate notifications in case of Personal Data breaches and serve as a central point of contact with the DPAs.

Example

Capgemini Germany has won a deal to provide BPO services to a bank. During the negotiation of the contract, the bank requests Capgemini Germany to certify that it has appointed a DPO as such is required under German law. The bank also requests the name of Capgemini Germany DPO so as to refer all questions related to Data Protection to him/her.

In addition to cases where appointment of a DPO is required by law, in some particular instances, Capgemini has voluntarily appointed DPOs in specific businesses or countries to respond to market demand.

The FS GBU for example has appointed a FS GBU global security and compliance officer (and the corresponding function at a country level) who plays the role of a DPO for Data Privacy matters by implementing Data Privacy policies, performing training, ensuring Capgemini compliance to industry standards and client requirements and handling incident reporting and coordination in case of data breaches.

In the US, the compliance and regulatory department has appointed a Privacy Lead to implement a privacy program and in particular to ensure compliance with the data breach notification requirements of the various state regulations.

Fiona's lesson learned

Always check with the Legal Department if a DPO has been appointed and refer data protection matters to him/her.

If no DPO has been appointed, refer the matters to the local Legal Department.

8 Privacy Enhancing Technology and Privacy by Design

Fiona thinks that complying with all these Privacy Laws and regulations, although fascinating, may also be something of a burden for any organization. On the other hand, it occurs to her that a smart use of technology may contribute to managing any organization's privacy concerns. And … Eureka!

Isn't Capgemini in the technology business? So, all these privacy worries may also provide excellent new business opportunities! Capgemini could sell technological solutions that will help clients protect their data, and be compliant at the same time! Promptly, she goes to see her friend at the business development practice, to find out if she is really the first one to have this revolutionary idea.

Privacy Enhancing Technology

Actually, Fiona was not the first with this brilliant idea. In 1995, in a joint report by the Dutch and Canadian DPAs, the term Privacy Enhancing Technology (**"PET"**) was first used and described. There are various definitions of PET but the recurring elements of these definitions are that a PET:

- minimizes the amount of Personal Data held by a Data Controller at all times;
- empowers individuals to retain control of information about themselves;
- reduces or eliminates the risk of contravening Data Protection Laws.

Privacy by Design

Later on, the concept of "Privacy by Design" was introduced. This means that privacy should be embedded as core functionality into the design of systems. In that way, instead of having to find fixes for privacy breaches as they occur, such breaches can be prevented from happening and/or their impact will be a lot less severe. Especially now that we are moving at great speed into the cloud, one single data breach may lead to Personal Data being copied million fold in no time, retrievable anywhere, for any purpose. PETs are therefore important elements for designing systems with privacy in mind.

Example

A hospital may protect patient Personal Data by using encryption (a PET) for storage and communication. Computer screens at the counters are equipped with privacy screen filters (a PET, making the data on the screen readable only if the reader is right in front of it). Data access is protected by username and password (a PET) and is logged (a PET, but the logging and logs themselves also bring about new privacy risks which have to be addressed) in order to be able to respond to unwanted actions. Furthermore, a patient file will be segmented (by design) as to make medical data available to the medical staff only, whereas the accounting department will only have access to anonymized – or pseudonymized – financial data.

The design allows high-quality data to be used for scientific research or statistics and management information, but only in an aggregate, anonymized form. Medical, financial and/or administrative patient data are combined only to the extent needed, e.g., for printing (or mailing) invoices or providing information to the patient himself. And in these cases, it is easy to take additional measures (such as using machine processed envelopes for printed invoices, which reduce the risk of fraud) to even better protect the patient's privacy.

Apart from the legal consequences of privacy breaches (damages, penalties), data leaks also mean bad publicity. Fixing data leaks or potential data leaks in a system that was not designed to protect data is costly and sometimes hardly possible.

Having privacy built in is better than having it bolted on. Privacy by Design may provide for added value to many of Capgemini's offerings and proposals. And, last but not least, Privacy by Design has been incorporated as one of the principles of the revised EU 2012 Draft Data Protection Regulation.

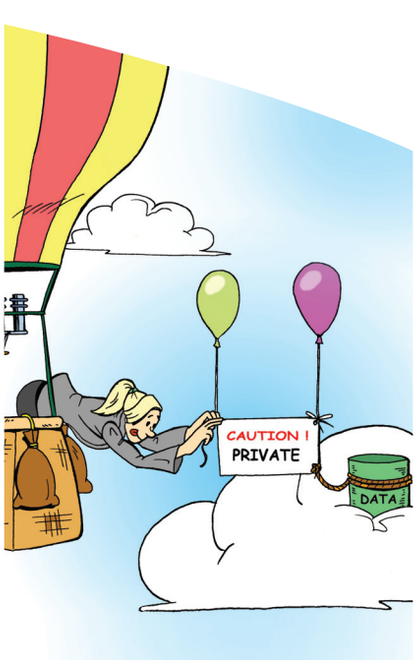
Fiona's lesson learned

Privacy by Design and Privacy Enhancing Technologies are to be taken into account as good options for (further) protecting our own as well as our client's Personal Data.

Moreover, they provide excellent opportunities for selling extra software functionality!

9 Privacy in the Cloud

Fiona noticed that Cloud Computing is the new trend, where IT services will be provided as a service from "the cloud". She is aware that Capgemini provides cloud services to its clients, but also from a procurement side Capgemini purchases services that are provided from the cloud. As "the cloud" is something intangible, Fiona wonders whether Personal Data is safe in the cloud. As you do not always know where the cloud is, you do not know where the Personal Data is stored and that will raise all kind of privacy questions. Fiona comes to the conclusion that privacy in the cloud is an important issue that needs to be taken care of. She is curious how this can be dealt with in practice and visits the Legal Department.



Nowadays cloud computing is used more and more, which means that clients get IT services as a service/utility. Cloud computing provides flexibility, scalability and location-independent access to computer resources. Compared to normal outsourcing services, cloud services do not differ that much. Clearly the Privacy Laws apply, which means that if Capgemini is the provider, the client is the Data Controller and needs to comply with the Privacy Laws.

As the services will be provided from "the cloud", you often do not know where the data is stored. Typically, a service provider stores all the data in different data centers around the world. Bearing in mind the restrictions of the transfer of Personal Data to other countries and the regulatory constraints (see chapter 3), this may have an impact and needs to be considered.

Capgemini is both a client and a provider of cloud services. We can be a client of the cloud provider in procurement cases when we purchase software as a service, and we can be the cloud provider when offering IT infrastructure services to our clients.

In both instances privacy will be an important issue, as the Personal Data will be stored in the cloud and therefore Data Protection Laws remain fully applicable (e.g., Data Subjects' rights, international transfer of data, notification of data breaches…).

Being the client you do not have control over the data as in the "traditional way" and if Personal Data is involved, this will be an important issue to consider when choosing a cloud offering.

Example

Capgemini Italy wishes to move its CRM database to the cloud. Such database contains the names and contact details of the IT procurement and sourcing managers of Capgemini Italy's clients which are qualified as Personal Data. Capgemini Italy is the Data Controller and the cloud provider would be the Data Processor. When choosing its cloud provider, Capgemini Italy will have to perform a privacy risk assessment to ensure that all Personal Data of the CRM database to be moved to the cloud will be processed in accordance with Italian and EU Data Protection Laws, especially if the cloud provider has data centers located outside of the EEA. If the data is moved outside the EEA, the Data Controller may have to perform filings with the DPA and depending on the country concerned, EU standard contractual clauses may need to be signed with the cloud provider.

Being the cloud provider, protection of Personal Data is important to take care of. With this regard, security is an important subject in order to secure the data protection.

Security

The security requirements, the level of security and the way to control this, are important issues within cloud computing. Often, the cloud providers do not allow audits in their data centers, but they offer guarantees through the supply of certificates related to security. These need to be investigated every time in order to review whether they are acceptable in the specific case. Similarly, if Capgemini provides cloud offerings, clients are keen on having certifications as well.

Data Portability

Another key element regarding privacy in cloud solutions is the portability of the data. As the data is stored somewhere in the cloud, when acting as a client, Capgemini needs to make sure that the moment the services are no longer provided (for example if Capgemini chooses to terminate the contract and to move the data to a different provider), the cloud provider ensures full access and retrieval of the data in a readable format (also called the right to data portability). It is therefore important to agree to a proper exit arrangement.

Fiona's lesson learned

Because of the international transfer of Personal Data, privacy is a core issue that needs to be considered carefully in cloud offerings.

Security and portability of the data are important subjects which need to be tackled as well.

10 Conclusion

Fiona was very satisfied to have learned so much on Data Privacy. Not only did she understand the legal implications of collecting, storing and transferring personal data, but she also realized that Data Privacy Laws must be taken into account in all her daily professional activities. She was also happy to have identified two communities - the DPO community and the Legal Department - that could support her to help ensure Capgemini's compliance with Data Protection Laws.

For more information:
Legal Department Web Page and List of Privacy Lawyers and DPOs:
http://talent.capgemini.com/Infocenter/global_functions/leg/

About Capgemini

With around 120,000 people in 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2011 global revenues of EUR 9.7 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at
www.capgemini.com

Author: Legal Department
Illustrations: René Lauffer
March 2012

IN/01-017.12

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

www.capgemini.com

Capgemini
11 rue de Tilsitt
75017 Paris
France