Deloitte.

Link'n Learn

GDPR from different perspectives

April 2018

neral Data Protection Regulation
April 2018

Welcome
Agenda & Deloitte presenters

Today's agenda

1. Introduction
2. Personal data and personal identifiable data
3. Legislations and other sources of guidance
4. Myths
5. Questions

Presenters

Georges Wantz
Director
Tax and Consulting, Financial Services
Deloitte Luxembourg
gwantz@deloitte.lu

Mohammed Saadi
Manager
Risk Advisory
Deloitte Luxembourg
msaadi@deloitte.lu

Personal data and personal identifiable data

Personal data and personal identifiable data

What is a personal data?

"Any information relating to an identified or identifiable natural person".

Relating

- Content
- Purpose
- Result

Identification

- Direct
- Indirect

Data subject

- Not deceased persons
- Not legal persons

Reference

- Name
- ID number
- Location data
- Online identifier
- Etc.

The vast majority of organizations deal with personal data.

Personal data and personal identifiable data

What is a personal data?

"Any information relating to an identified or identifiable natural person".

Business

- Contract
- Emails
- Performance reviews
- Activity logs

Public

- Facebook profile
- Articles

Private

- Home address
- Memberships

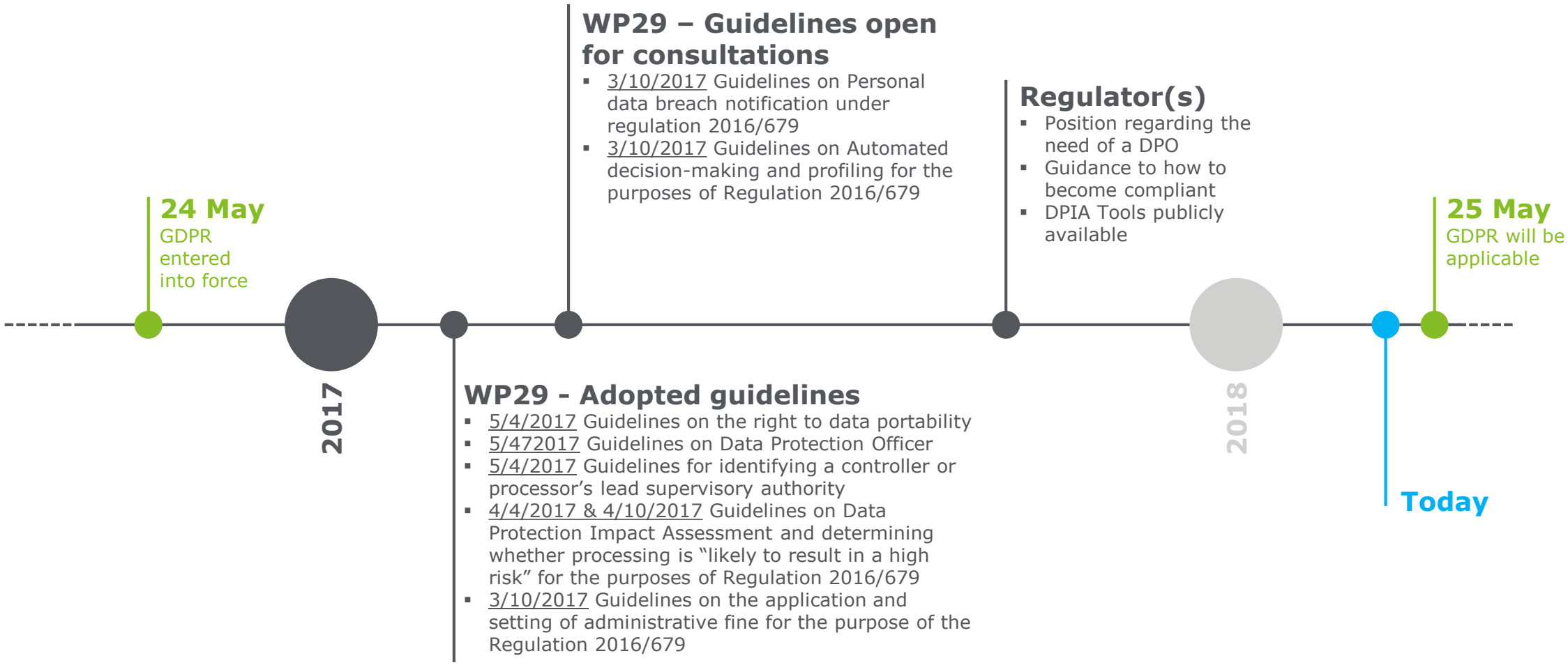
Mixed

- CVs
- Bank transfers
- Call logs

The vast majority of organizations deal with personal data.

Legislations and other sources of guidance

Legislations and other sources of guidance



Debunking the GDPR

Debunking the GDPR

From myths to reality : examples of common misconceptions about the regulation

International Exchange
Will the supervisory authorities share information?

Data Subject
Who is under the scope as per the regulation definition?

Personal data
To what extent can data be considered as personal?

Right to be forgotten
Under which circumstances can the right to be forgotten enforced?

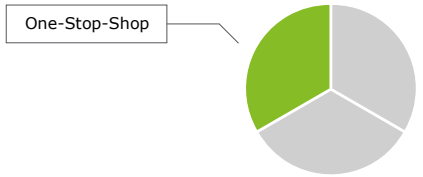
Direct marketing
Under which circumstances direct marketing is allowed?

Legitimate interest vs Consent
What is the right balance between those two lawful grounds?

International transfers
What changed with the GDPR in regards to data transfers?

Data breach
What is considered as a data breach as per the regulation?

Debunking the GDPR
International exchange of information



Myth

Data Protection Authorities (DPAs) will strictly enforce data protection laws at a national level. As such, the entities in Luxemburg will only be controlled by the CNPD.

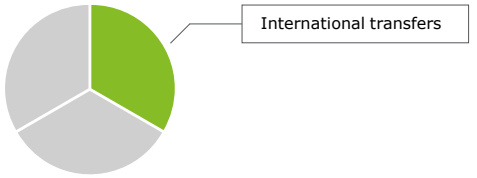
GDPR

While each Member state is required to appoint at least one DPA to implement the Regulation and protect the rights and freedoms of individuals (Recital 117; Article 51), another concept, the "One-stop-shop", has been introduced by the GDPR. It aims at improving the harmonization and ensure a more uniform application of EU data protection law, as an organisation will generally deal with a single lead DPA. (Recitals 124-128; Articles 55, 56; WP29 Lead DPA Guidelines).
In cases in which organisations are under investigation in multiple Member States, lead and concerned DPAs are required to cooperate and provide each other with mutual assistance. They also have formal legal authority to carry out joint operations. (Recital 133, 134; Articles 61, 62).

Implications

As a significant number of entities on the Luxemburgish market process data from citizens outside Luxemburg, they are likely to be investigated by other DPAs on top of the CNPD. Examples : CPVP in Belgium, CNIL in France, etc.

Debunking the GDPR
International transfers and contractual clauses



Myth

It is believed that the GDPR has introduced new restrictions or rules to abide by in order to be compliant with the law in regards to international transfers of personal data.

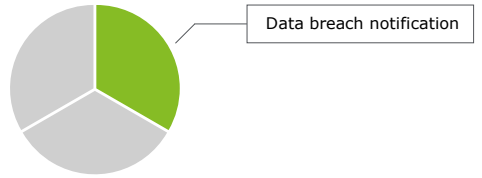
GDPR

The regulation actually prohibits cross-border data transfers if the following requirements aren't met : Cross-Border Data Transfers may only take place if the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). Recitals 101-116; Articles 44, 45.
The Directive (95/46/EC) have essentially similar restrictions : Cross-Border Data Transfers are, without prejudice to compliance with national law, prohibited, unless the transfer is made to an Adequate Jurisdiction or the data exporter has implemented a lawful data transfer mechanism (or an exemption or derogation applies). Recitals 56-57; Article 25, Article 26(1)-(2) of the 954/46/EC Directive.

Implications

An illegal international transfer by GDPR is most probably already illegal today.
If no contractual clauses such as BCRs or SCCs were in place before the GDPR for the international transfers that were taking place from an European country, those were already illegal under the 95/46/EC directive.

Debunking the GDPR
Data breaches as per the regulation



Myth

Data breaches only concern the theft of data by a third party.

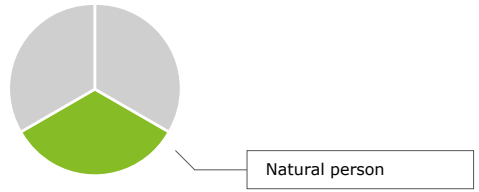
GDPR

The regulation actually defines a personal data breach as such : "means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Article 4(12).
In their guidelines, the WP29 gives the following precision : "What should be clear is that a breach is a type of security incident.
However, as indicated by Article 4(12), the GDPR only applies where there is a breach of personal data. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR".

Implications

The definition of data breach goes therefore way beyond the simple theft of data.
Among other things, it includes the unsolicited or illegal alteration of personal data or even the loss of data due to a fault in a system.

Debunking the GDPR
Scope of data subjects



Myth

It is frequently believed that the GDPR strictly concerns clients personal data, or that the GDPR also encompasses in its definition of the data subjects legal entities.

GDPR

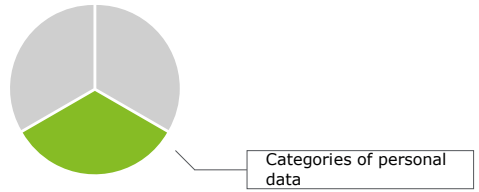
The regulation actually refers to data subject as such :

- "… identified or identifiable natural person … ". Article 4(1).
- "… personal data of data subjects who are in the Union … ". Article 3(2).
- Recitals 23 & 24 define the scope under which personal data of data subjects are concerned.

Implications

Following the definition provided by the regulation, a data subject also refers to employees, company representatives and more generally any natural person whose data are processed one way or another by a controller and/or a processor.
The definition of a data subject does not include data from legal entities.

Debunking the GDPR
Extent of personal data



Myth

Personal data only concerns data that identifies directly the data subject such as his name, his address, his phone number, etc.
Also, data available publicly and data that are related to employment ("Professional data") are not personal data.
Alternatively, it is believed that sensitive personal data cannot be processed under any circumstances.

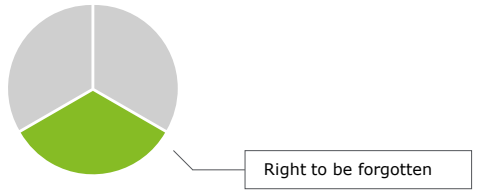
GDPR

The regulation actually defines a personal data as such : "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Article 4(1).

Implications

Following that definition, personal data includes all data directly or indirectly linkable to a data subject with a proportionate effort.
For example, if data such as preferences, GPS coordinates, list of purchases or professional data are linkable to a data subject, they are therefore considered as personal data as per the regulation.
Some data have been defined, as per the regulation, as sensitive. Those data (e.g. health, racial or ethnic) can be processed by a controller and/or a processor but under very strict rules.

Debunking the GDPR
Enforcement of the right to be forgotten



Myth

All personal data under the control of a processor or a controller are susceptible to be erased on the spot following the request of a data subject.

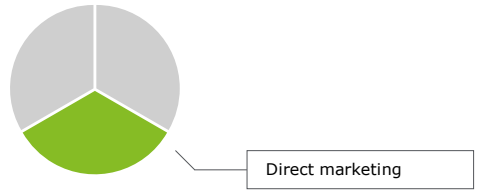
GDPR

The regulation actually refers to the right to be forgotten as such : "A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject … However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller … ". Recital 65.

Implications

The right to be forgotten is not absolute and most probably cannot concern all data you process.
For example, should the right to be forgotten be exercised, it should not impact negatively other data subjects.
Also, this right to be forgotten does not have to be exercised by the controller if as a consequence, it was preventing legal actions to be pursued.

Debunking the GDPR
Direct marketing, allowed or forbidden



Myth

The regulation prevents some processing activities to be performed such as direct marketing.

GDPR

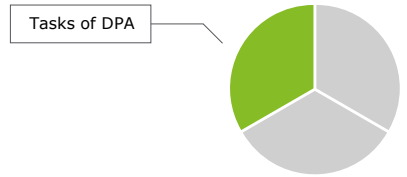
The regulation actually refers to direct marketing as such :

- "Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing". Article 21(2)**.**
- "Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.". Article 21(3)**.**

Implications

This is actually false. Unless the activity in its current state is assessed as highly risky and does not implement the appropriate safeguards required by the regulation, the GDPR does not prevent to do direct marketing. The regulation only gives a legal framework under which this activity is permitted. In the recitals, direct marketing is recognized as a processing activity for which controllers and/or processors have a legitimate interest (lawful ground) to perform.

Debunking the GDPR
Compliance support tool provided by the CNPD



Myth

It is mandatory for Luxemburgish entities to demonstrate their compliance with the compliance support tool developed by the CNPD.

GDPR / Opinion

The obligation to use this tool is neither mentioned in the GDPR nor in any opinion stated by the CNPD. Data Protection Authorities (DPAs) are responsible for enforcing data protection laws and providing guidance on the interpretation of the laws. Among those responsibilities, we have : monitor and enforce the application of the GDPR, promote awareness, advise national and governmental institutions, etc. Recitals 122, 123; Articles 55, 57.

Implications

This tool, accessible for free on the CNPD portal since end of December, enables users to check the level of coverage of their organizations against the GDPR. It will allow them to maintain a record of processing activities, including their related documents, and to monitor the evolution of the level of coverage.

The aim of the tool is to help organizations in their task of integration of the GDPR requirements, in particular to demonstrate their accountability by centralizing all the information required by the regulation. In that regard, this tool can be seen as an accelerator, but in no circumstance can be considered as mandatory.

Q&A

5. Q&A

Next Link'n'Learn
Date: Thursday 26th April 2018
Topic: MiFID II and Corporate Governance

Deloitte.