GDPR - Implications for Financial Institutions

ING-DiBa AG

Harborth, Leila / Data Management & Protection

Frankfurt ▪ 8th of June 2021

About me

- My name is **Leila Harborth**
- I am working at **ING Germany, CoE Data Management & Protection** for GDPR related projects
- Before, I worked among others at:
  - EY
  - Commerzbank
  - BHF-Bank
  - Goethe University, E-Finance Lab
- Education:
  - Goethe University - Master in Finance & Information Management
  - Goethe University - Bachelor in Business Administration & Economics
  - San Diego State University – Study Abroad - Economics

Agenda

What is GDPR about (focus on specific topics)?

What rights do you have?

ING`s business model

What are possible implications when implementing GDPR compliant processes?

GDPR – Introduction (1/2)

- The topic of data protection is becoming **increasingly important** and is now very present. In times of increasing digitalization, a reform and standardization of data protection within the EU became necessary.
- The GDPR is valid since the **25th May 2018** and concerns also the ING.
- Data protection has long been a topic for ING, but the rules of the game have changed.
- The principles of the GDPR are represented in the following.

GDPR – Introduction (2/2)

The central intention of the GDPR is to ensure the protection of personal data. But what does that mean exactly and what are personal data at all?

- The handling of personal data is part of our daily business and therefore unavoidable.
- At the bank, we work with a wide range of personal data, in particular with that of our clients.
- Personal data is more than just the client's name. It can be e-mail addresses, IP addresses, account numbers and much more.
- The more information is available about a person, the more conclusions can be drawn about that person.
- In the following you will find more insights regarding personal data.

GDPR – Personal Data

- The GDPR defines personal data as well as special categories of personal data.
- The second needs to be protected even more:

Personal Data

- General personal data - e.g. name, address, e-mail, telephone number, place of birth
- Bank details - e.g. account numbers, credit information, account balances
- Online data - e.g. IP address, location data
- Identification numbers - e.g. personnel number
- And much more

Special Categories of Personal Data

- Health data - e.g. diseases, taking medication, genetics
- Biometric data - e.g. voice, fingerprints
- Beliefs - e.g. political, religious or ideological
- Background - e.g. cultural, ethnic
- Membership to trade union

GDPR – Processing of Personal Data

- When processing personal data, many of us think of the active use of data, such as creating reports or analyzing data.
- But processing is much more than that.
- It's every process we do with personal information - **both active and passive.**

Examples		
Collection of data	Retention of data	Storing of data
Adaption or modification of data	Reading of data	Organizing of data
Capturing of data	Sorting of data	Etc.

GDPR – Principles

The GDPR defines principles for the processing of personal data …

- … the data must be used in a **lawfully** and transparent manner.
- … the data may only be used if there is a fixed **clear purpose** for it.
- … it may only be processed as much data as is **necessary** for the defined purpose.
- … the data must always be updated to a new and **correct** state.
- … the storage of data must be **limited**. We may store data only then and only as long as it is necessary for the defined purpose.
- … during the processing of the data an adequate **security** of the personal data must be guaranteed.

GDPR – Security (1/2)

- Art. 32 GDPR requires - among others – the implementation of "**appropriate technical and organisational measures to ensure a level of security appropriate to the risk**".
- Sufficient data security is necessary for effective data protection. Data security has the goal to protect data to a sufficient degree against loss, manipulation and other threats.
- **Examples of measures:**
  - Pseudonymization or encryption of data
  - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
  - A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

GDPR – Security (2/2)

What does confidentiality, integrity, availability and resilience stand for?

Confidentiality
Protection against unauthorized disclosure of information

Integrity
Maintenance of data accuracy

Availability
Data should be available when needed

Resilience
Ability of systems to recover quickly in the event of a failure

GDPR – Data Subject Rights

1. Right to access
2. Right to rectification
3. Right to erasure/ to be forgotten
4. Right to data portability
5. Right to object
6. Right to restriction of processing

ING´s Business Model
Our Goal: to be the leading Digital Bank in Germany

Digital Leadership

1. **We want to be the primary financial partner for our customers.**

2. **We want to be digital leader of the finance sector.**

Many customers carry the branch of the future anytime and anywhere in their pockets: **the smartphone**

ING

ING´s Business Model
Digital services for easy and stress-free banking - Examples

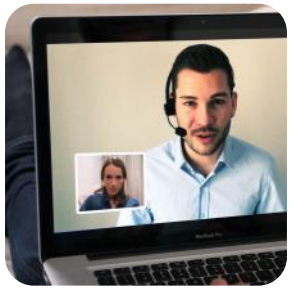
Photo transfer

Capture data from a printed invoice

Fingerprint

Fingerprint instead of TAN

Video



Convenient identification from home

Mobile Payment

Simply pay by mobile phone

Let´s deep dive into three practical use cases...

Use Case – Data Breach

ING is required to report data protection violations to the supervisory authority immediately, at the latest within 72 hours of becoming aware of the incident.

1. Perform a research on what the GDPR demands if such an incident happens. Summarize what the law describes.
2. Think about what a potential data incident might be. Describe a scenario.
3. Imagine that you are the data protection officer at ING. Please develop a strategy to manage the incident. The following questions might help you:
   - Which process steps do you need to introduce in order to manage this data incident?
   - Do you need information from other departments? What information do you need?
   - Do you have to inform the affected person? Do you have to inform the supervisory authority in this case?
   - What challenges do you face?

Use Case – Right to be Forgotten

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing.

1. Perform a research on what the GDPR demands. Summarize what the law describes.
2. Think about a scenario where a person wants to make use of his/her right to be forgotten. Describe the scenario.
3. Imagine that you are the data protection officer at ING. Please develop a strategy to manage the request. The following questions might help you:

   - Which process steps do you need to introduce in order to be able to react according to the law?
   - Do you need information from other departments? What information do you need in this case?
   - How many time do you have to respond to the request?
   - How long can data be kept under GDPR?

Use Case – Privacy Impact Assessment

If a processing of personal data is likely to result in high risks to the rights and freedoms of natural persons, a privacy impact assessment needs to be carried out.

1. Perform a research on what the GDPR demands. Summarize what the law describes.

2. Imagine one scenario within the financial sector where a privacy impact assessment would need to be performed. The following questions might help you:

   - In which context is processing taking place?
   - Which type of data is processed, e.g. is it also personal data such as customer data or employee data?
   - Is sensitive data processed (special categories of personal data)?
   - How much data is being processed?

Thank you!

Leila Harborth
Data Management and Protection

ING Germany
Theodor-Heuss-Allee 2
D-60486 Frankfurt am Main

Telefon +49 / 69 / 27 222699 48
Mobil +49 / 172 / 382 89 28
Leila.Harborth@ing.de

www.ing.de

Facebook.com/ING.Deutschland

@ING_Deutschland

Instagram.com/ING.Deutschland

YouTube.com/ingdiba