

Hello and welcome everybody!

Have you already heard about the GDPR? If yes, what can you say about it?



The aim of this course is:

- to understand the ins and outs of the protection of personal data
- and to think about how data is processed and protected in our company.

### Better protected!

GDPR offers everyone better protection of their data.



### GDPR, what is it?

---

#### General Data Protection Regulation

- European regulation
- Data protection
- Personal and sensitive nature
- Standardisation
- Reinforcement

3

The General Data Protection Regulation is a European regulation that protects data with a personal and sensitive nature, by standardising its processing and reinforcing its security.

## Everyone is affected!

We all process personal data everyday.




## GDPR, who is affected?

---

**New company trends**

- Digitalisation
- Paperless
- Big data

**... new responsibilities for our customer and employee data!**

- Collection (consent)
- Transfer
- Storage
- Security

We all process personal data everyday.

For example, a simple email in the form [firstname.lastname@gmail.com](mailto:firstname.lastname@gmail.com) is already personal data since it allows someone to be identified.

In recent years, the use of personal data by companies has exploded.

There is a trend towards digitalisation and paperless processes.

The idea of big data is now common throughout business.

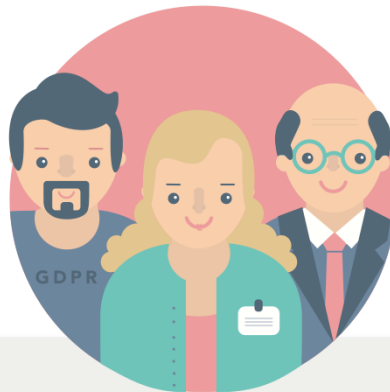
With the European General Data Protection Regulation, the protection of this personal data is reinforced and this is a good thing.

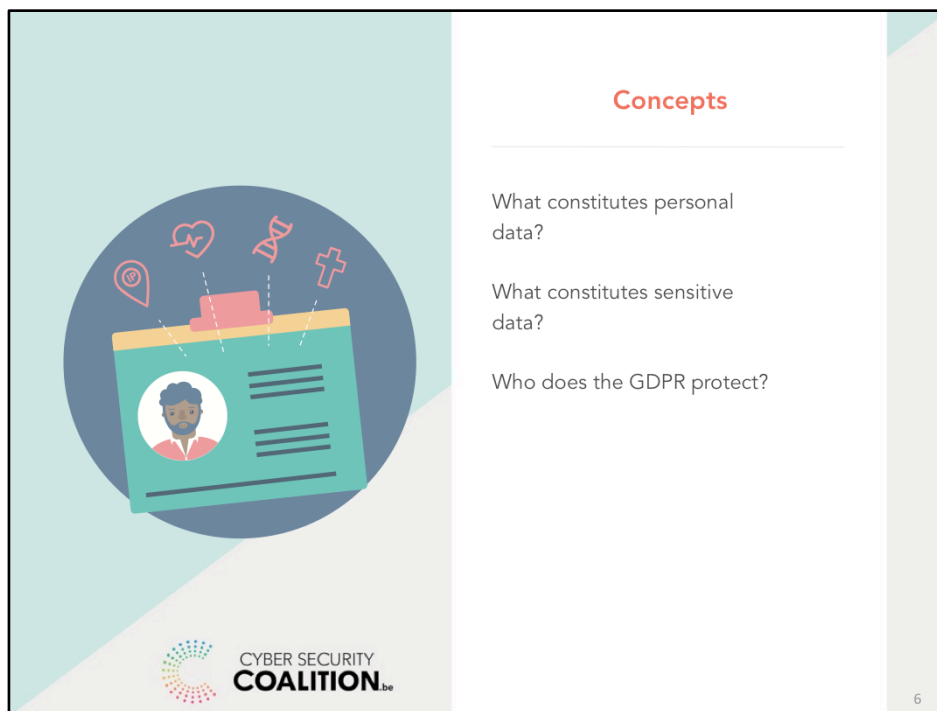
As consumers, we are better protected. As professionals or employees, we are responsible for ensuring the protection of our customer and employee data to offer them the same protection.

As an employee, I am responsible along with my employer for collecting, transferring and storing our customer and employee data in a secure way, while respecting their consent.

Let's think together!

How do we process personal data  
in our company? And how is it protected?





### **What constitutes personal data?**

Any data that allows someone to be identified is considered as personal data. Clearly the last name and first name. A phone number is considered personal data because it is possible, with a little searching, to identify its owner. Caution, two or more data items that are not considered as personal alone, can become personal if, by combining them, someone can be identified.

### **What constitutes sensitive data?**

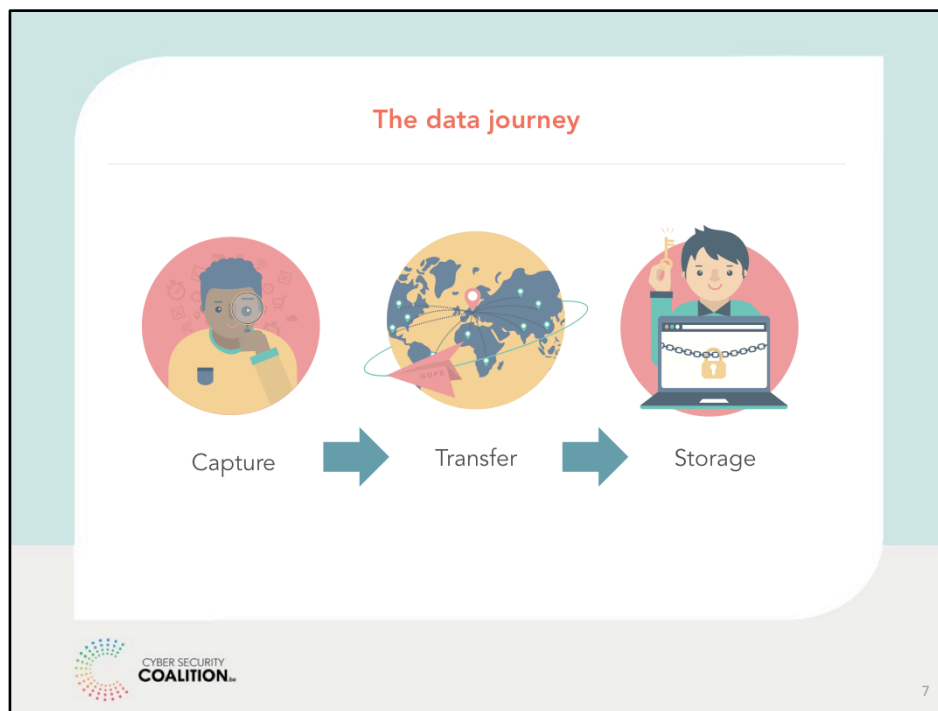
Sensitive data generally means medical data, political preferences, sexual orientation. Geo-tracking data is not considered as sensitive. However, it can be considered as personal if it can be used to identify someone. For example, the geo-tracking of my home is personal data.

### **Who does the GDPR protect ?**

Everyone, whatever their origin, who is located physically or electronically in Europe at a given moment in time.

Examples:

- a Chinese citizen who fills in a form at Brussels airport during a transfer between China and the United States is protected by the GDPR for the data they enter on the form.
- a Russian citizen who visits the fnac.be site from Russia is protected by this European regulation.



Now let's talk about how we collect, transfer and store data in our company and our own professional activity.

This is the data journey.

The next slides are discussion guides, with generic answer elements to be adapted to each company.

It is important to make team members aware of the data used and how it is processed.



### **What types of data are processed in our company?**

This can be customer data: last name, first name, date of birth, email address, reading preferences, history of web pages visited, CVs, etc.

And also more sensitive data like medical data...

Ask the question: does this data have a personal or sensitive nature (refer above for definitions).

### **How is our data encrypted?**

On paper? In a computer terminal at a trade show? On an iPad? On our website, etc.?


### **What programs are used to encrypt our data?**

A mobile app? A HR recruiting site? An internal company program? A program in the cloud? An accounting program, etc.?

### **Who can encrypt?**


The customer? A company sales rep? The HR services, etc.?





## Transfer

- Where is our customer or employee data transferred to?
- How is our data transferred?
- Are memory sticks used to transfer data?
- Is the data encrypted during the transfer?


**CYBER SECURITY COALITION**<sub>be</sub>

9

### **Where is our customer or employee data transferred to?**

After capture, is the data kept in the same place? Or is it transferred? By means of another app for processing?

### **How is our data transferred?**


What apps use the data of our customers or employees? What do they do with this data (transfer, archiving, etc.)?

### **Are memory sticks used to transfer data?**

Very practical, memory sticks are also easy ways of losing personal or sensitive data. The stick can fall from a pocket or can be lent to someone else with no consideration for the data stored on these memory sticks.


### **Is the data encrypted during the transfer?**

It is essential: anyone who uses a memory stick or external hard drive to transport data must ensure its protection during the transport, for example, by encrypting it. A simple means is to use a Zip app which enables compressed data to be encrypted with a code. It is also possible to use specific memory stick encryption programs, sometimes available by default on certain models.



## Storage

- Where is our data stored?
- Are our backups protected?
- Who can store our data?
- Who can access our data?


**CYBER SECURITY COALITION**<sub>be</sub>

10

### **Where is our data stored?**

Where do we store/archive our customer or employee data in our company?  
In a computer? In the cloud? On an external hard drive?

### **Are our backups protected?**


Is the archived data encrypted?  
Are the data archiving machines protected?  
Are the external hard drives secured by key?

### **Who can store our data?**

Can I extract company data when I want?  
Can I send data by email to work at home? (how is it protected in this case?)

### **Who can access our data?**

Who can access the data stored or archived in the company?  
It is not necessary for the whole company to have access to customer or employee data.  
It is recommended to only ensure access to data to people who need it regularly and to make these people responsible for data protection.

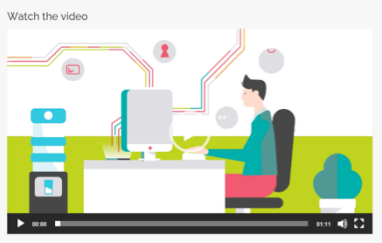


CYBER SECURITY  
**COALITION**.be

## Video!

With the “GDPR – Data clean-up” campaign, the Cyber Security Coalition would like to encourage everyone to perform an efficient data clean-up, pursuant to the GDPR. By means of an animated film you will discover the importance of a data clean-up and how to proceed.

Watch the video



11

[https://www.cybersecuritycoalition.be/content/uploads/4217\\_Cyber-Security-Coalition-1-Data-Awareness-STAND-60s-EXTRA-MET-LOGO\\_v3.mp4](https://www.cybersecuritycoalition.be/content/uploads/4217_Cyber-Security-Coalition-1-Data-Awareness-STAND-60s-EXTRA-MET-LOGO_v3.mp4)



### What constitutes personal data?

#### ANSWER



Any data that allows someone to be identified is considered as personal data. Clearly the last name and first name. A phone number is considered personal data because it is possible, with a little searching, to identify its owner. Caution, two or more data items that are not considered as personal alone, can become personal if, by combining them, someone can be identified.

### What constitutes sensitive data?

#### ANSWER



Sensitive data generally means medical data, political preferences, sexual orientation. Geo-tracking data is not considered as sensitive. However, it can be considered as personal if it can be used to identify someone. For example, the geo-tracking of my home is personal data.

**If I send an email to a customer by mistake containing data about another customer, is this data leakage?**

ANSWER



Yes, it is considered as data leakage.



**What do I do if I think there has been a data loss  
in the company?**

ANSWER



Inform company management (or line manager) as soon as possible. Companies are required to report data losses to the Data protection authority.



16

<https://www.dataprotectionauthority.be>



**How should personal or sensitive data be encrypted for its transport in a memory stick?**

ANSWER



A simple means is to use a Zip app which enables compressed data to be encrypted with a code. It is also possible to use specific memory stick encryption programs, sometimes available by default on certain models.



CYBER SECURITY  
COALITION



17



Thank you for your attention!