FEB
Federation of Enterprises in Belgium

CYBER SECURITY COALITION.be

DATA PROTECTION

The new General Data Protection Regulation – implications for enterprises

- New rules directly applicable from **25 May 2018**
- **Impact** on almost every enterprise based in the EU
- Severe penalties for non-compliance

WHY THIS BROCHURE?

In our increasingly interconnected world with its growing volumes of personal data and ever-faster transmission rates, the protection of personal data and their subjects' privacy have become a major concern. A new European Union Regulation sets stringent requirements to be met by all enterprises (i.e. any organisation that processes personal data). In light of this highly complex piece of legislation, called the General Data Protection Regulation, FEB has produced this brochure to offer you guidance on situations in which data protection matters and on how you should handle this issue.

THE GDPR IS EVERYONE'S BUSINESS!

The GDPR will apply from 25 May. What exactly does that mean? It means that every business or organisation that stores or uses personal data (whether they relate to its own staff, suppliers' staff, actual or prospective customers, or anyone else) will need to be able to prove that its storage or use of the data complies with the rules laid out in the GDPR.

But compliance with the GDPR is not something that can be achieved overnight. Moreover, it requires a sound knowledge of both the GDPR and of your own business or organisation.

The Cyber Security Coalition has developed a number of tools to put businesses and organisations on the right track. Anyone who reads this brochure is sure to get a thorough grounding in the GDPR. The Coalition also offers a 'GDPR checkUp': a simple way for businesses and organisations to determine which measures they need to take to be fully GDPR-compliant by 25 May 2018.

You can find the GDPR checkUp at **www.cybersecuritycoalition.be.**

DO I PROCESS PERSONAL DATA ?

Processing = collection, recording, organisation, structuring, storage, consulting, editing, etc.

+

Personal data = any information relating to an identified or identifiable individual (name, tracking number, location data, etc.). This individual is called the **data subject**.

I process personal data, and so I must comply with the privacy legislation(*).

(*) For more information on the new European Union Regulation (EU) 2016/679 of 27 April 2016, see the website of the Commission for the Protection of Privacy: **www.privacycommission.be/en**

I am the **controller**:
I say how and why personal data is processed.

I am the **processor**:
I act on the controller's behalf.

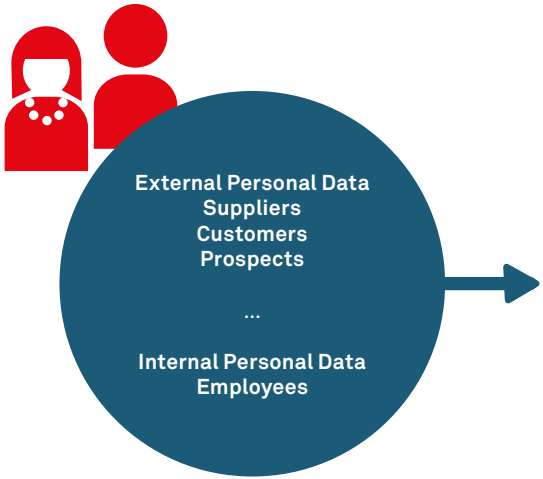
TO BE **COMPLIANT,** I MUST ENSURE THAT THE PERSONAL DATA ARE:

- processed **legally** and **appropriately** and with a clear view of how the information will be used;
- collected for specified, **explicit and legitimate purposes;**
- relevant and **limited** to the respective purposes;
- accurate and **kept up to date**;
- retained for **no longer than** is **necessary** for the relevant purposes;
- only processed if the data are kept **appropriately secure**.

ACCOUNTABILITY CONSIDERATIONS REQUIRE ME TO **DEMONSTRATE** THAT I:

- compile a **data register** for all processing activities (inventory);
- ensure that I only process the **minimum volume** of personal data necessary to achieve the legal purposes of doing so;
- draft a **privacy notice**, i.e. a statement issued to a data subject that describes how the organisation, among other things, collects, uses, retains and discloses personal data;
- develop an **internal policy** for informing and training my staff;
- appoint an employee who is in charge of data protection;
- use **data protection impact assessments** where appropriate (these pinpoint the most effective means of compliance and allow enterprises to identify and fix problems at an early stage;
- establish **effective (protection) procedures** to ensure the enterprise's compliance with the privacy legislation.

UNDER WHAT CIRCUMSTANCES CAN I PROCESS PERSONAL DATA?



EITHER WITH THE DATA SUBJECT'S CONSENT;

EITHER PROCESSING IS REQUIRED:

to ensure the **performance of a contract** (e.g. processing the data subject's address so that goods purchased online can be delivered, and processing credit-card details so that a payment can be made);

to comply with a **legal obligation** (e.g. the requirement for employers to report their employees' salary data to the social security or tax authorities, and financial institutions' obligation to report certain suspicious transactions);

to safeguard a data subject's **vital interests**;

to perform a task carried out in the **public interest**;

for the purposes of **legitimate interests** (e.g. certain specified personal data processed because a company has an interest in ensuring the health and safety of the staff working at its nuclear power plant).

Consent requires some form of **clear affirmative action**. Unresponsiveness, pre-ticked boxes and inactivity do not constitute consent!

Consent must be verifiable. This means that some form of record must be kept of how and when consent was given. Individuals have a **right to withdraw consent** at any time. This possibility should be made as easy as granting consent.

CHILDREN'S PERSONAL DATA

The General Data Protection Regulation (GDPR) contains new provisions intended to enhance the protection of children's personal data.

HOW ABOUT CONSENT OBTAINED PREVIOUSLY?

You will not be required to again seek consent from the individuals concerned if the standard of that consent meets the new requirements. This will entail a review of consent mechanisms to ensure they meet the standards required under the legislation.

- Ensure that data subjects are provided with a clear explanation of the processing for which they are granting their consent.
- Ensure that the consent mechanism is genuinely voluntary and of an 'opt-in' nature.
- Ensure that data subjects can withdraw their consent easily.
- Ensure that consent is not based on unresponsiveness or inactivity.

WHAT CAN A DATA SUBJECT ASK OF ME?

RIGHT TO BE INFORMED

I must provide appropriate information on the processing procedure and be transparent in how I use personal data (privacy notice).

What information I supply depends on whether I obtained the personal data directly or indirectly.

I must provide the information at the time the data are obtained (if obtained directly) or within a reasonable period (if obtained indirectly).

RIGHT TO DATA PORTABILITY

The data subject may ask for personal data to be transferred from one processor to another.

Only personal data provided by an individual (by consent or via a contract) are affected.

I must provide such data in a structured, commonly used and readable form.

I must do this free of charge and within one month (extendable by two months).

RIGHT TO DELETION

The data subject may ask me to 'be forgotten' and to be deleted from my data systems (with various exceptions).

The data subject has this right in specific circumstances if the processing causes him or her damage or distress.

There are some specific circumstances in which I can reject the deletion request.

RIGHT TO RECTIFICATION

I must rectify personal data if they are inaccurate or incomplete.

I must inform third parties accordingly if I have disclosed the personal data to them.

I must inform the relevant individuals about the third parties to whom the data have been disclosed.

I must respond within one month (extendable by two months).

AUTOMATED DECISION-MAKING AND PROFILING

Individuals have the right not to be issued with a fully automated decision.

You must ensure that individuals can (1) be assured of a human intervention; (2) express their point of view; and (3) obtain an explanation of the decision and challenge it.

This right does not apply if the decision is (1) required to enter into or ensure the performance of a contract; (2) authorised by law; or (3) based on explicit consent.

RIGHT OF ACCESS

The data subject has the right to know if his or her data is being processed or not.

The controller must supply a free copy of the processed data within one month (extendable by two months).

RIGHT TO OBJECT

Individuals may object to:

01 - direct marketing: upon receiving an objection, I must stop processing the personal data immediately (no exceptions);

02 - processing based on legitimate interests: upon receiving an objection, I must stop processing the data unless legal exemptions apply;

03 - **processing for scientific/historical research** in certain cases.

I must inform the data subject of his/her right to object in my first communication and in my privacy notice.

WHAT ARE MY OBLIGATIONS AS THE CONTROLLER AND/OR PROCESSOR?

Each time I process personal data, I will do so as either a controller or a processor.
The old legislation only imposes direct compliance obligations on controllers, while now compliance obligations are also imposed on processors.

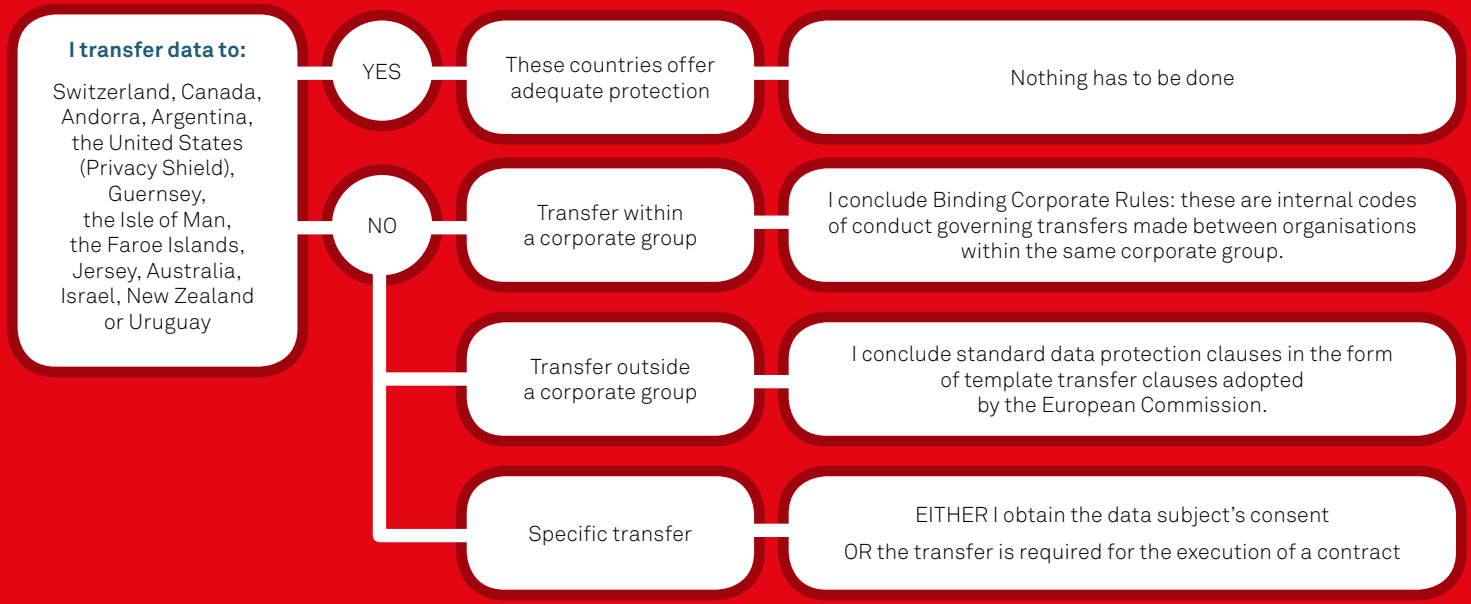
AS THE CONTROLLER I MUST:

- review all of my data-processing activities and keep verifiable records of these activities;
- ensure that I have implemented appropriate technical and organisational measures to appropriately protect the security of the personal data;
- ensure that I comply with the accountability principle and cooperate with the Privacy Commission where appropriate;
- ensure that I have appropriate processes and templates in place for identifying, reviewing and promptly reporting data breaches to the Privacy Commission.

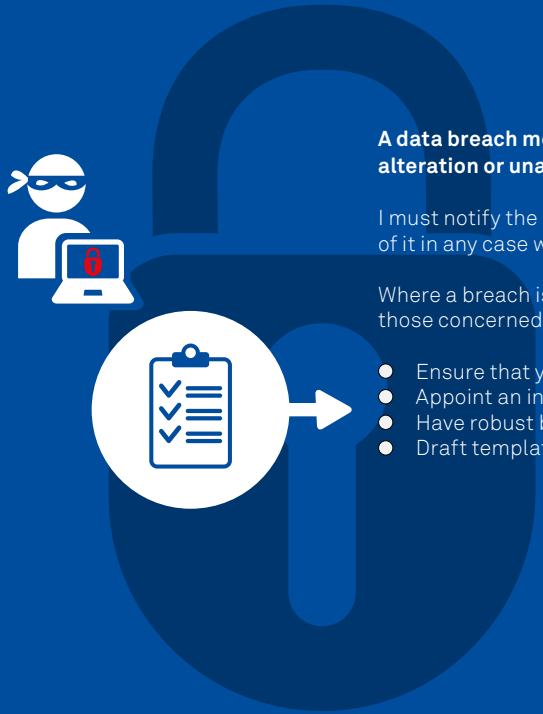
AS THE PROCESSOR I MUST:

- review my existing data-processing agreements and ensure the appropriate security and confidentiality of personal data I process;
- only process data in accordance with the controller's instructions;
- ensure that I have appropriate processes and templates in place for identifying, reviewing and (insofar as required) promptly reporting data breaches to the relevant controller;
- be aware that I am only allowed to appoint sub-processors with the controller's consent.

WHAT IF I TRANSFER DATA OUTSIDE THE EU?



WHAT DO I NEED TO DO IN CASE OF A DATA BREACH?



A data breach means a breach of security leading to the destruction, loss, alteration or unauthorised disclosure of or access to personal data.

I must notify the Privacy Commission of any breach within 72 hours of becoming aware of it in any case where it is likely to put an individual's rights and freedoms at risk.

Where a breach is likely to put an individual's rights and freedoms at high risk, you must notify those concerned directly.

- Ensure that your staff or the employees in charge understand what constitutes a data breach.
- Appoint an individual to take responsibility for reviewing and reporting data breaches.
- Have robust breach detection, investigation and internal reporting procedures in place.
- Draft template letters to report any data breach.

PERSON IN CHARGE OF DATA PROTECTION AND DATA PROTECTION OFFICER

FEB ADVISES ALL ENTERPRISES TO APPOINT A PERSON IN CHARGE OF DATA PROTECTION.

When your core business involves large-scale systematic monitoring of individuals or special categories of data, you must appoint a Data Protection Officer (DPO).

THE TASKS OF A DATA PROTECTION OFFICER:

Inform and advise the enterprise and its employees of the organisation's obligations to comply with the GDPR and other data protection laws; monitor compliance with the GDPR;

Be the first point of contact for data protection.

You can give an existing employee the role of DPO as long as his/her professional duties are compatible with the duties of a DPO and do not result in a conflict of interests.

You can also contract out the role of DPO externally.

COLOPHON

Edited by
Nathalie Ragheno

Content officer
FEB asbl
Stefan Maes
Rue Ravenstein 4
B - 1000 Brussels
www.feb.be

Design and layout by
manythink

Printed by
Graphius

Legal deposit
D/0140/2016//17

Deze brochure
is ook verkrijgbaar
in het Nederlands

Cette brochure
est aussi disponible
en français

SEVEN KEY RECOMMENDATIONS

1. Keep a record of all personal data processes along with their intended purpose.
2. Handle the processed data legally and transparently.
3. Only register mandatory data, and do so for no longer than necessary.
4. Put appropriate security measures in place to protect the personal data.
5. Clearly notify the data subjects concerned.
6. Devise an internal data protection and privacy policy.
7. Appoint a person in charge of data protection and privacy.

CENTRE FOR CYBER SECURITY BELGIUM

BNP PARIBAS FORTIS

ING

KBC

proximus

SWIFT

FEB
Federation of Enterprises in Belgium

Rue Ravenstein 4 - 1000 Bruxelles
T: + 32 2 515 08 11
info@vbo-feb.be
www.feb.be

Facebook VBO-FEB
Twitter @VBOFEB
LinkedIn VBO-FEB