Is your business ready for the new data protection rules? protection

As of May 2018 the European Data Protection Directive shall be replaced by the General Data Protection Regulation (GDRP)

9CE73532277B134

If you collect, store or use data such as

Names or biometric data

Online identifier

Address

0898

Criminal record

Political preferences

Religious or philosophical beliefs

Income

Health or genetic info

other personal data

Then you **must comply** with the new requirements of the GDRP

Where?

C3AC4A21BE

EU-based organizations

! Even if the data is being processed outside the EU

Non-EU organizations

! As long as they offer goods and services to subjects located in the EU

Or

! If the conduct of a data subject takes place in the EU and is also monitored in the EU

protection

What rules?

THE PARTY OF THE P

Main obligations implemented by the GDRP

Stricter rules for data portability and a right to be forgotten notify data protection supervisory authorities if a data breach takes place

obligation to carry out privacy impact assessments

Data protection officers

protec

non-compliance fines of up to EUR 20,000,000 or (if higher) 4% of the global annual turnover of the organisation; special rules for profiling and use of children's data



The Operator – Data Subject relationship

ALLES TO DE TO

0898

Consent to use personal data

any freely given, specific, informed and unambiguous indication of the data subject's will by which he or she, by a statement or clear affirmative action, confirms an agreement to the processing of personal data relating to him or her.

Guiding principles

Lawfulness
Fair use
Transparency
Consistent purpose
Data minimization
Confidentiality
Accountability

Main rights

Data erasure

Can require the controller to erase personal data on request

Receive a copy of the data

Data portability

receive their personal data "in a structured, commonly used and machine-readable format" and to transmit data in that format to another controller

Object processing

Individuals have the right to object to processing based on legitimate interests.

If exercised, this request must be respected unless the organisation can show there are compelling grounds to continue with the processing which overrides the individual's rights, or if the processing is required to establish, exercise or defend legal claims.

Notifying data subjects

C3AC4A21BE

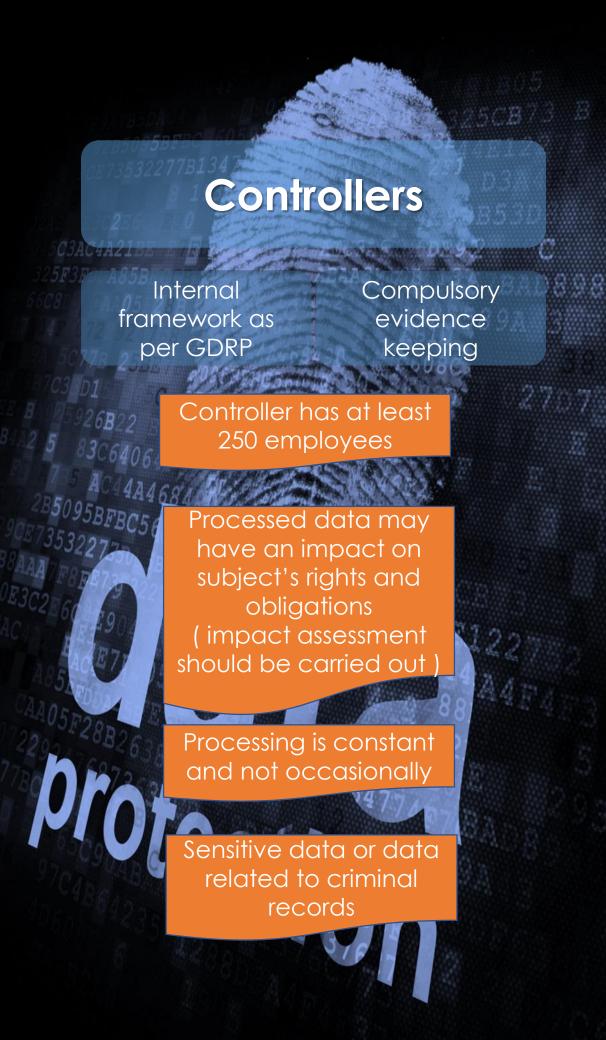
Cases when notice for data breach is necessary

- breach constitutes a significant risk for the subject's rights;
- if the controller has not notified the subject yet, the supervising authority may request to do so;
- ! Notice shall be made without any delays (max 72h)
- ! Notice in a plain and simple language.
- ! Should explain the nature of the data breach plus information and measures submitted to the supervising authority.

Cases when notice for data breach is unnecessary

- Controller has already taken adequate technical measures which were applied to the beached data (i.e. cripted data);
- The risk is unlikely to be caused due to measures taken after the data breach;
- Would require a disproportionate effort (subjects can be publicly informed)
- ! Supervising authority can decide whether these conditions were actually met

protection



Mandatory elements of the evidence

Name, contact details of the controller/its representative/per son in charge with data protection

Scope of the processing Description of processed data

Foreseeable time frame as to erase data

Transfers to third party states and destination

Description of data subjects

Description n of technical measures adopted

The names and contact details of the person or persons empowered by the operator and of each operator in whose name those persons operate

The categories of processing activities carried out by the person empowered on behalf of each operator

The Data Protection Officer (DPO)

Mandatory when

05 2

prote

 Processing is made by a public authority or entity

898

- Main activities of the operator require a frequent and systematic supervision on a large scale
- 3) Main data processed by the operator is sensitive data or criminal records

DPO's tasks

Informing and advising the operator/representative s/employees regarding their obligations;

Monitoring compliance with GDRP and the allocation of responsibilities within the organization;

Risk assessment upon request

Cooperation with the supervising authority

Contact person in relation with the data subjects

Sanctions

Breaches related to principles guiding fair processing and consent, data subjects rights, transfers to third party states, decisions of the national supervising authority are subject to a fine up to

EUR 20,000,000 or (if higher) 4% of the global annual turnover of the organisation;

Failure of the controllers or persons empowered by them may be subject to a fine up to

EUR 10,000,000 or (if higher) 2% of the global annual turnover of the organisation;