





POLKEN



REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. of 27 April 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

replaces the Data Protection Directive 95/46/EC

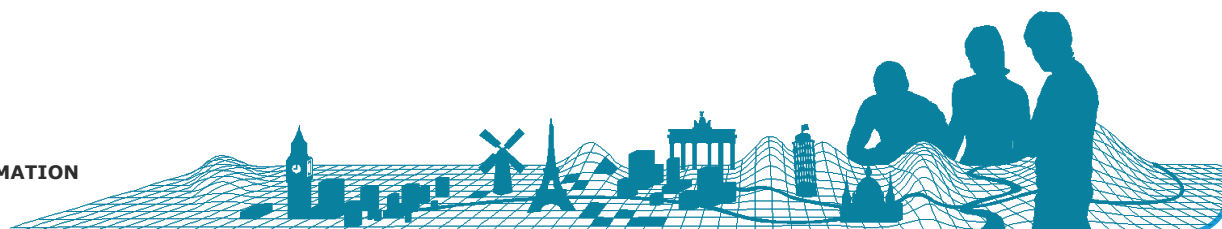
designed to **harmonise data privacy laws across Europe**, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

KEY CHANGES:

Increased Territorial Scope (extra-territorial applicability)

Penalties

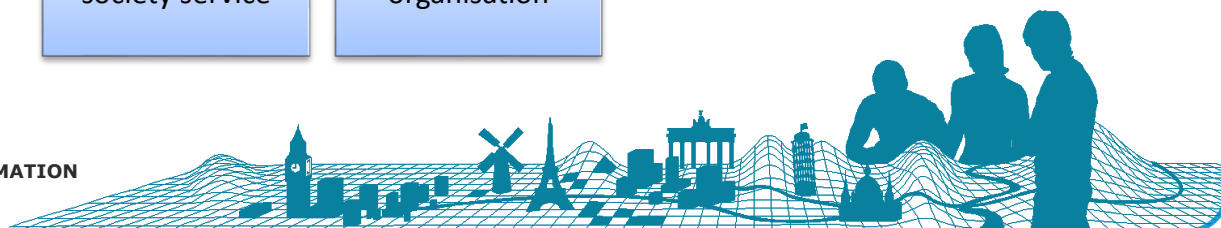
Privacy by design





DEFINITIONS - 26

processing	restriction of processing	filing system	controller	third party	consent
biometric data	personal data	profiling	pseudonymisation	processor	recipient
personal data breach	genetic data	data concerning health	main establishment	representative	enterprise
group of undertakings	binding corporate rules	supervisory authority	supervisory authority concerned	cross – border processing	relevant and reasoned objection
		information society service	international organisation		





Lawfulness of processing

- When it is necessary for compliance with a legal obligation to which the controller is subject (public authorities performing their tasks)
- More specific provisions are allowed by MS in this case in order to adapt the application of the rules of the Regulation.



"PERSONAL DATA"



Directive 95/46/EC

- "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.



GDPR

- "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable 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**, online identifier or to one or more factors specific to the physical, physiological, **genetic**, mental, economic, cultural or social identity of that person.



Impact

- The definition is, for the most part, unchanged.
- The explicit inclusion of location data, online identifiers and genetic data may result in additional compliance obligation





"DATA PROCESSING"



Directive 95/46/EC

- "Processing" means any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.



GDPR

- "Processing" means any operation or set of operations performed upon personal data **or sets of personal data**, whether or not by automated means, such as collection, recording, organisation, **structuring**, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.



Impact

- The GDPR introduces minor amendments to the wording of the definition of "processing". These amendments are unlikely to make any practical difference to most organisations.





"CONSENT"



Directive 95/46/EC

- "The data subject's consent" means any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.



GDPR

- "The consent of the data subject" means any freely given, specific, informed **and unambiguous** indication of his **or her** wishes by which the data subject, **either by a statement or by a clear affirmative action**, signifies agreement to personal data relating to them being processed.



Impact

- For organisations that rely on consent for their business activities, the processes by which they obtain consent will need to be reviewed and revised to meet the requirements of the GDPR.



Data Subject Rights

Right to be
Forgotten

Data
Portability

Privacy by
Design

Right to
Access

Breach
Notification

Data
Protection
Officers



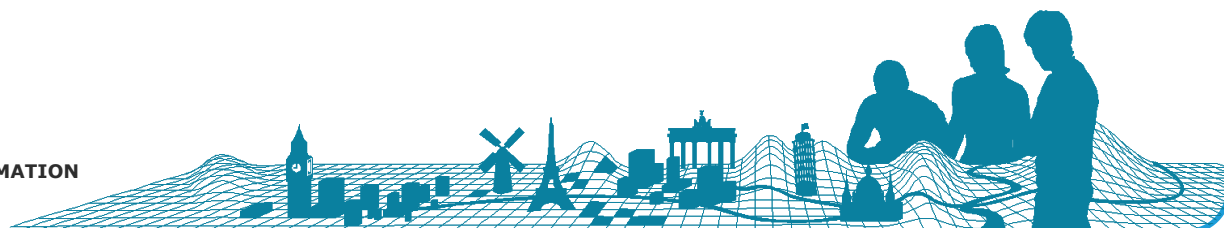
Impacts most on operators whose CORE business is DATA PROCESSING and/or dealing with sensitive personal data

‘processing’ - operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

NMCAs processing personal data

Is there a risk of material breach of GDPR?

Possibility to create privacy policies templates to meet all privacy requirements!



GDPR Guidelines prepared by the WP29

Finalised GDPR Guidelines

- on Data Protection Officers (DPO)
- on the right to data portability
- for identifying a controller or processor's Lead Supervisory Authority
- on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"
- on Automated individual decision-making and Profiling
- on Data Breach Notifications
- on Administrative fines
- BCR referential for data controllers
- BCR referential for data processors
- Adequacy referential

GDPR Guidelines currently to be open for public consultation

- Guidelines on Derogations for transfers
- Guidelines on Accreditation

GDPR Guidelines no longer under public consultation but still to be finally adopted by the WP29

- Guidelines on Consent
- Guidelines on Transparency





‘Personal data’ 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...

...name, an identification number, location data, an online identifier,

one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”

It can be anything from a name, a photo, **an email address**, bank details, **posts on social networking websites**, medical information, or a **computer IP address**.

‘forename.surname@company.eu’
or employees’ business telephone numbers.

