

General Data Protection Regulation and Interreg

Audit Authorities network meeting
29 -30 May 2018 | Valencia, Spain

Przemyslaw Kniaziuk, Interact



Disclaimer

This presentation represents only the point of view of the presenter and serves for information purposes only.

By no means it constitutes a legal advice.

General Data Protection Regulation (1)

- Regulation came into force in May 2016 (before directive)
- Applicable from 25 May 2018
- 2 years to prepare already passed
- Data protection provisions apply to programmes as they process data

General Data Protection Regulation (2)

- General rules – some MS establish more detailed sectoral rules
- Specific provisions
 - Designation of Data protection officer (DPO) depending on the body where MA/JS is located
 - public/private
 - Records of processing activities depending if institution employs >250 persons, unless dealing with sensitive data
- Case law yet to come, practicalities and details often missing

Reasons of the Regulation

- Stress the importance of personal data
- Better protect personal data of EU citizens in a digitalized world
- Give rights to citizens concerning their data
- Make public and private bodies think which data is processed, what for and how it is protected
- Think about the data risk management system

Definitions (1)

Personal data

- any information relating to an identified or identifiable natural person ('data subject')
- multiple items put together that can identify the person (IP address)
- the data can be processed by automated and manual systems

Definitions (2)

Data controller

- Data controller is the data owner
- Responsible to individuals
- In Interreg MA/JS will usually be the data controller

Data processor

- Processes the data on behalf of the data controller
- Follows the instructions of the controller
- A company contracted to manage publicity of the programme (info campaigns, newsletter)

Examples of personal data sources in a programme

- Project data in monitoring system (contact details, sometimes salary sheets)
- Applicants (IP addresses, contact details)
- Publicity campaigns (subscribers of newsletters)
- Employees (salary sheets, travels)
- Job applications in MA/JS
- Business cards collected at conferences
- E-mails received
- Pictures of persons (e.g. conferences)
- Competitions participants
- List of MC members

Legal basis for processing

The data can be processed when there is:

- 1) Consent (be careful)
 - 2) Contractual necessity
 - 3) Compliance with legal obligation
 - 4) Necessity to protect vital interest
 - 5) Performance of tasks in public interest or in exercise of official authority vested in controller (legitimate interest);
- Programmes must process some personal data due to legal obligations and contracts – inform the subjects that processing is in place
 - Consents can be revoked – what to do then?

Principles

- Collect only the data that you need – minimal approach
- Data lifecycle (delete when not needed)
- Accountability – the data correctly protected, legal basis for processing,
- If the data is transferred to 3rd party there must be legal basis or consent

Data controller – responsibilities

1. Risk assessment

- implement appropriate technical and organisational measures to ensure GDPR compliance
- review and update technical and processes – audit mechanisms

2. Data mapping

- what and why, probability of losing the data
- identify the sources and classify the data (consent or legitimate interests) and the legal bases for processing – strategy for compliance

Data controller – responsibilities

3. Protect the data (depending on the nature of the data)
4. Code of conduct encouraged
 - fair and transparent processing
 - legitimate interests
 - consider rights

Security of processing (1)

- Appropriate measures to be taken (general provisions)
- Personal data can have different forms (electronic, paper, hand written participants list)
- Protection of the place where the data is stored, IT system, trainings for employees
- Encryption
- Data more vulnerable (health, card numbers) to be misused protected in a more sophisticated way
- Restore possibility if data lost

Security of processing (2)

- Data collected for certain purpose can only be used for this purpose, not for others
- The data subject to be informed how the data will be processed and for which purpose it will be used.
- Data only for its identified purpose (do not send the newsletter to the database of applicants if no consent for that)
- Human factor - employees to be aware what they are entitled to do
- IT systems might be protected, but unaware employees might create leakage (unprotected pendrive or laptop lost or stolen, undestroyed papers thrown away)

Data breach notification (1)

- a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed
- likely to result in a risk to rights and freedoms of natural persons should be notified to them without due delay
- Programme context: usernames and passwords to the monitoring systems are stolen

Data breach notification (2)

- not only theft, but data spill
- 72 hours from the moment the data processor notices a breach notice the supervisory authority (independent public authority)
- only if results in an infringement of privacy of data subjects

Rights of data subjects (1)

Right of access on request to data undergoing processing

- Controller should be able to present all data processed and should be able to establish the deletion date.
- Might be difficult for a programme – data in different data bases, some data not for deletion

Right to rectification

- rectification of "inaccurate personal data" and the completion of "incomplete personal data"

Rights of data subjects (2)

Right to erasure (right to be forgotten)

- the data is no longer processed
- only if no legal grounds for processing
- If 3rd party deals with the data it must remove it as well
- In case of Interreg much of the data must be retained for audit purposes according to the ESIF Regulations!

Rights of data subjects (3)

Right to restriction of processing (if data inaccurate, objection)

- if a data subject objects to the processing of that data, but the controller has a legal requirement to retain it
- controllers may need to employ technical means to prevent a specific data subject's personal data from undergoing certain processing activities

Right to data portability from one controller to another controller

- in a structured, commonly used, and machine-readable format. (csv, xml, pdf)
- where technically feasible

Controllers have 30 days to respond to requests

Compensation, fines and penalties

Compensation

- Any person suffered material or non-material damage
- Right to receive compensation from controller or processor for the damage (if responsible)

Administrative fines

- Individual cases analysed
- Gravest infringements – 20 m EUR fine or 4% of total annual turnover, whichever higher
- Google global turnover for 2017 – \$109 billion – max. fine:– \$4,36 billion

Penalties

- Additionally MS lay down rules on penalties for infringements not covered by GDPR

Cooperation works

www.interact-eu.net