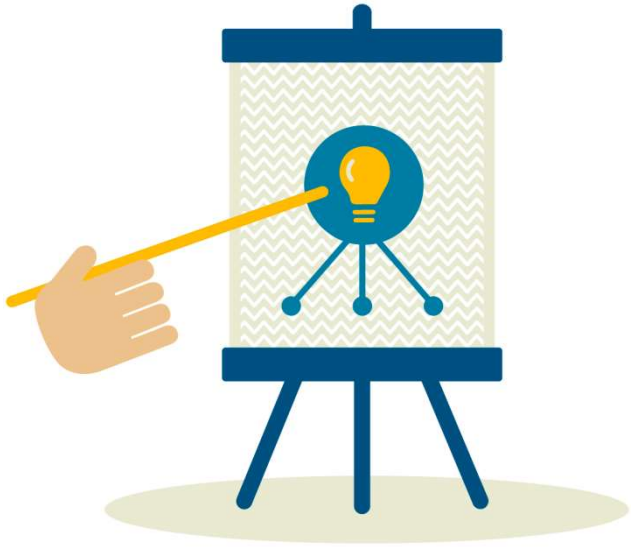
General Data Protection Regulation and Interreg

25 June 2021 I Webinar



Przemyslaw Kniaziuk, Interact

European Regional Development Fund

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

- GDPR 2016/679 came into force in May 2016, applicable from 25 May 2018
- Regulation (EU) 2018/1725 (DPR for Union institutions, bodies, offices and agencies)
- some MS establish more detailed sectoral rules or provide interpretations
- practicalities and details often up to court judgements -> see disclaimer

---

- Additional provisions for programmes in the Financial Regulation (FR) of 18 July 2018
- Draft Common Provisions Regulation 2021 – 2027 (19 May version) – article number change

GDPR and Interreg

FR defines the obligation to apply GDPR by programmes:

- Any processing of personal data by Member States bodies responsible for the management and control of Union funds shall comply with Regulation (EU) 2016/679 (article 63 (4) FR)

GDPR – reasons

- Stress the importance of personal data
- Make public and private bodies think which data is processed, what for (necessary?) and how it is protected
- Give the same rights across EU to citizens concerning their data (before transposed directive)
- Better protect personal data of EU citizens in a digitalized world (we give our data more)
- Think about the data risk management system

Definitions (1)

Personal data (GDPR)

- any information relating to an identified or identifiable, living natural person ('data subject')
- enterprises data (apart from self-employed persons) is not personal data
- multiple items put together that can identify the person (eg. IP address, function and nationality)
- personal data can be processed by automated and manual systems (handwritten participation list vs. data processed by Jems)

Definitions (2)

Data processing

- Reading AFs
- Collecting data from websites -> excel
- Sending of participation lists
- Recording events

Definitions (3)

Data controller

- Data controller is the data owner
- Responsible to individuals
- In Interreg MA/JS will usually be the data controller + National Authorities + others
- But LPs/PPs are data controllers as well (train them!)

Data processor

- Processes the data on behalf of the data controller (receive the data from the controller)
- Follows the instructions of the controller – DC inform!
- A company contracted to manage publicity of the programme (info campaigns, newsletter)
- Contact points, MC members, etc…

GDPR – application

- Does not apply for purely personal or household activity
- Every controller or processor located in the Union, disregardless of the processing place (programme in the UE, data server in the US)

GDPR – application outside of UE?

- Controller or processor not located in the Union but processing personal data of subjects in the Union (ENI + IPA programmes concerned when processing Union citizens data)
- UK has a bridge until 30 June 2021
- Adequacy decision for UK (adoption by the EC) expected for early June 2021! – 16 June MS app.
- The draft EU GDPR adequacy decision says that the UK provides adequate protection for personal data transferred from the EU under the EU GDPR.

General Principles

- Collect only the data that you need – minimal approach
- Data lifecycle (delete when not needed)
- Accountability – legal basis for processing AND processed data to be correctly protected,

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

Information requirement

Data controller	Legal entity DPO contact where applicable
Principal purposes and legal basis for processing	• Info about future calls (consent) • Project selection • Audits (FR Art. 63(4))
Rights	• Access • Rectification • Withdraw consent (if possible) • Objection or restriction of processing (if possible) • Erasure (if possible)
Principal recipients or categories of recipients	Managing Authority, MC Members, First Level Controller, Audit Authority, European Commission, European Court of Auditors (etc.)
Additional information	Storage period or criteria used to determine it If data used for different purpose than originally collected information on the new purpose And much much more …

Examples of personal data (1)

- Applicants (contact details, IP addresses)
- Project data in monitoring system (applicants contact details, beneficiaries, salary sheets)
- Publicity campaigns (subscribers of newsletters)
- Employees (contact data, salary sheets, travels)
- Competition participants
- List of MC members

Examples of personal data (2)

- Job applications in MA/JS (until when to keep them?)
- Business cards collected at conferences
- E-mails received
- Pictures of identifiable persons (e.g. conferences)
- Voice recordings with identifiable voice
- Zoom / Skype / Teams recordings
- Cookies collected by webpages

Legal basis for processing

The data can be processed when there is:

1) Consent
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);

No need to always ask for consent – there are many legal obligations to process personal data!

Legal obligation (1)

Processing and protection of personal data The Member States (…) allowed to process personal data only where necessary for the purpose of (…) monitoring, reporting, communication, publication, evaluation, financial management, verifications and audits and, where applicable, for determining the eligibility of participants (…)

Draft Article 4 of CPR

Legal obligation (2)

List of operations

The managing authority shall make the list of operations selected for support by the Funds publicly available on the website (...)

update that list at least every four months

(b) where the beneficiary is a natural person the first name and the surname;

Draft Article 49 of CPR

Legal obligation (3)

List of operations

- Where personal data of recipients is **published for** the purposes of **transparency** in relation to the use of Union funds and the control of award procedures, **those recipients should be informed of such publication**, as well as of their rights and the procedures applicable for exercising those rights.

Preambule to FR point 18

Legal obligation (4)

Applicants and beneficiaries

- In any call made in the context of grants, procurement or prizes implemented under direct management, potential beneficiaries, candidates, tenderers and participants shall be informed that their personal data may be transferred to internal audit services, to the Court of Auditors or to the European Anti-Fraud Office (OLAF) and between authorising officers of the Commission

Article 57 FR

Legal obligation (5)

MC Members

- The list of the members of the monitoring committee shall be published on the website referred to in Draft Article 49(1).

Draft Article 39 of CPR (Composition of the monitoring committee)

Various practices with publishing contact data

- MC members to be informed to excercise their rights

Legal obligation (6)

Payslips

- Staff costs may be reimbursed either:

(i) Full time (proven by the employment document and payslips);

Draft art. 39 (3) of Interreg Regulation (Staff costs)

Consent (1)

- Pictures + videos
- Receiving newsletters
- Contacting new possible beneficiaries
- Distribution of contacts
- Social media publications
- Etc.

Consent (2)

- Affirmative consent (opt-in tickbox, agree button, signature, etc.)
- No opt-out (prefilled tickbox), always opt-in (tickbox to be actively ticked)
- Freely given (necessary for the performance of a contract?)
- In written
- Given in unequivocal way
- No objection, silence, inactivity -> tacit content is no consent!
- Consent can be easily withdrawn at any time!

Consent (3)

- Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
- Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

Consent – Pictures and videos

- Pictures where an individual is the focus of an image the image is likely to be personal data (practice)

- Exemption: processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression

  (art 85 GDPR)

Consent

I authorize Interact to use any pictures taken at this event in which I appear on its website and other social media or publications.

- (•) Yes, I do.
- ( ) No, I don't

(If you choose "Yes", these pictures will only be used to illustrate the event itself, or in further dissemination/reporting. Choosing "No" will not prevent you from being accepted as a participant in the event. Should you have any question about this or should you need any clarification, please contact Mikis Moselt at dataprotection@interact-eu.net.)

I allow Interact to share my contact details (email, office phone number, organization and role) with the other participants in this event.

- (•) Yes, I do.
- ( ) No, I don't

(If you choose "Yes", your contact details will appear on a participant list handed out at the event, to help participants network and communicate. These details will also appear in Interact's Contact Database. Choosing "No" will not prevent you from being accepted as a participant in the event. Should you have any question about this or should you need any clarification, please contact Mikis Moselt at dataprotection@interact-eu.net.)

I allow Interact to record the online meeting I am participating to.

- (•) Yes, I do.
- ( ) No, I don't

The purpose of the recording may be archiving as well as possibly further dissemination of the event topic towards a larger audience. By applying to this event, you acknowledge and accept the recording in accordance and within the limits sets by GDPR regulation.

Consent needed

Photo by Sebastian Herrmann on Unsplash

Consent needed

Photo by Sebastian Herrmann on Unsplash

Consent not needed

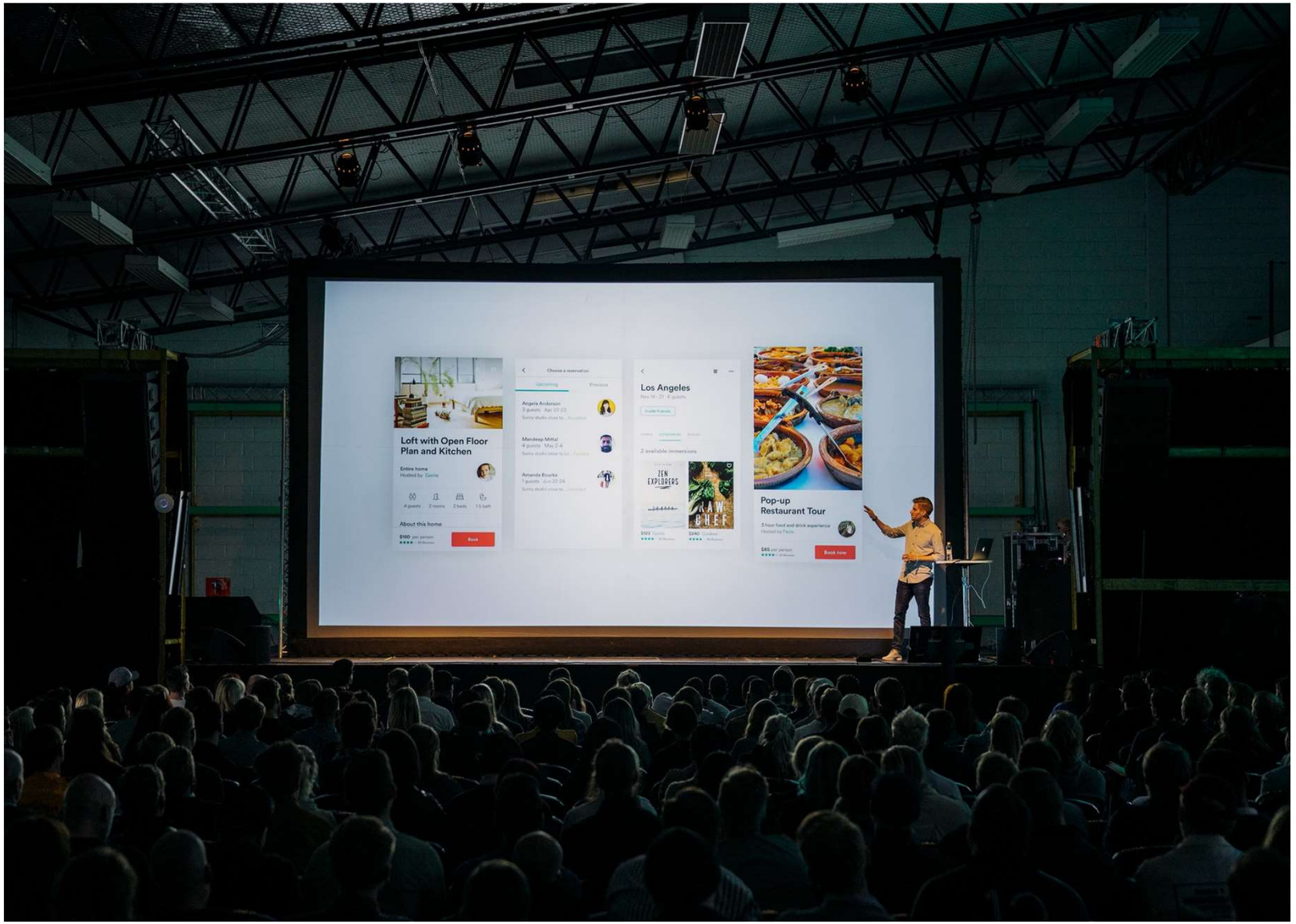


Photo by Teemu Paananen on Unsplash

Consent not needed

Photo by Headway on Unsplash

Consent not needed

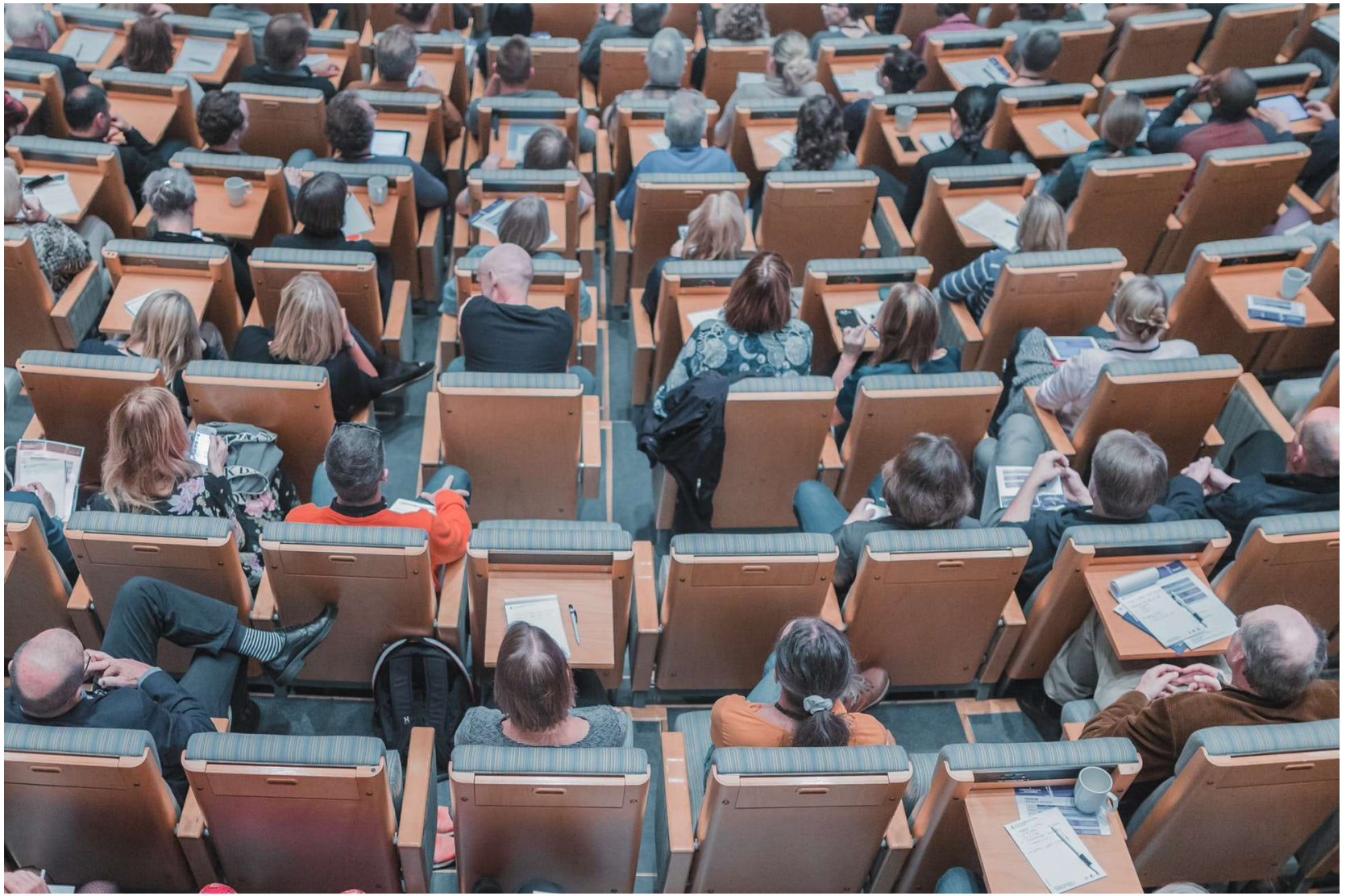


Photo by Mikael Kristenson on Unsplash

Website cookies

- GDPR requires a cookie policy and corresponding cookie banner to alert visitors
- Explains to site visitors how and why cookies are being used (revealing all cookies and trackers operating on your website)
- Receive users' informed consent before using any non-essential cookies.
- Document and store consent received.
- Allow visitors to access your content even if they don't allow the use of certain cookies.
- Allow visitors to withdraw consent (switch off previously activated cookies).

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, when do we delete data?

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 a lot of data must be retained for audit purposes according to the ESIF Regulations!
- Some MS require to keep some categories of data for a long lime or forever!

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

Security of processing (1)

- Personal data can have different forms (electronic, paper, hand written participants list)
- Physical protection of the place where the data is stored, IT systems, trainings for employees
- Encryption of data (attachments to e-mails, pendrives, laptops)
- Data more vulnerable (health, card numbers, ID numbers) to be misused protected in a more sophisticated way
- Restore possibility if data lost (Youtube videos)

Security of processing (2)

- Data only for its identified purpose not for others
- Human factor - employees to be aware what they are entitled to do with the data, restricted access to some personal data?
- 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 hacked and stolen, unprotected laptop with personal data lost or 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

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 for privates

- 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

European Regional Development Fund