

General Data Protection Regulation (GDPR) and Interreg

Przemysław Kniaziuk, Mikis Moselt

29 November 2023

Online

Interact



Co-funded by
the European Union
Interreg

Agenda

01

Meeting objectives
Legal intro

02

Definitions:
Personal data
Processing
Data controller
Data processor
Task 1

03

Consent
Legal obligation
Task 2

04

Rights of data subjects
Security & breaches
Fines & penalties

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](#)
 - [Common Provisions Regulation 2021/1060](#)

GDPR and Interreg

Financial Regulation 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 (GDPR) 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 leave our data everywhere)
- 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, voice, picture)
- 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 personal data from websites -> excel
- Preparing external experts' database
- Sending of participation lists
- Recording events
- Taking pictures of persons

Task 1

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
- State aid beneficiaries (Transparency Award Module)
- Beneficial owners

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
- Security cameras recordings
- Zoom / Skype / Teams recordings
- Cookies collected by webpages

Definitions (3)

Data controller

- Data controller is the data owner
- Responsible to individuals

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...

Interreg specificities

Data controller in Interreg Programmes

- Most of the times **your Programme is not a legal entity** by its own right but instead refers to its Hosting Institution;
- Most of the times your Programme belong to a public institution or organisation and as such you **MUST** have a DPO to refer to (art. 37 sub. A);
 - You are not the data controller, your hosting institution is;
 - You don't have a DPO, your hosting institution has.
- Importance to have an in house Data Protection referent to interface with your DPO.

Interreg specificities

Data controller in Interreg Projects

- When dealing with project, remember that your **Lead Partners (LP) and Partners (PP) are also Data Controllers** of their own data;
- Importance to train your project partners to privacy and to make sure that they are GDPR compliants and clearly understand the duties;
 - Specifically train your projects partners for GDPR compliance and involve their DPO;
 - Foresee a specifical set of articles and/or addendums in your Subsidy Contracts to regulate your data interactions.

Interreg specificities

Importance of Data Processors for Interreg Programmes

- The existence of Data Processors in the implementation of your Programme is **inevitable**;
- Importance to pay attention to all external service providers. Some are more obvious, like the company that builds your IT infrastructure or your website, some are less e.g. restaurant that provides catering and to which you send detailed list of diners with dietary restrictions;
 - Keep track of your Data Processors and map them;
 - Always include GDPR compliance in service contracts.

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)
- Iceland, Liechtenstein and Norway (EEA) also covered by GDPR from 2018 on

GDPR – application outside of UE ?

- Controller or processor not located in the Union but processing personal data of subjects in the Union (IPA + NEXT programmes concerned when processing Union citizens data)

Non-EU countries with adequacy decision

- Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay as providing adequate protection.

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
- Data subjects need to be informed that their data is processed

Information requirement

Data controller	Legal entity DPO contact where applicable
Principal <u>purposes</u> and legal basis for processing	<ul style="list-style-type: none"> • Info about future calls (consent) • Project selection • Audits (FR Art. 63(4))
Rights	<ul style="list-style-type: none"> • 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 ...

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!

Consent (1)

- Contacting potential beneficiaries
- Distribution of contacts
- Social media publications
- Receiving newsletters
- Pictures + videos

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

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.



This site uses cookies to offer you a better browsing experience. Find out more on [how we use cookies](#).

Accept all cookies

Accept only essential cookies

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, not law)
- Exemption: processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression (art 85 GDPR)

Consent needed ?



Photo by [Sebastian Herrmann](#) on [Unsplash](#)

Consent needed ?



Photo by [Teemu Paananen](#) on [Unsplash](#)

Consent needed ?



Photo by [Mikael Kristenson](#) on [Unsplash](#)

Consent needed ?



Photo by [Sebastian Herrmann](#) on [Unsplash](#)

Consent needed ?



Photo by [Headway](#) on [Unsplash](#)

Consent – pictures and videos – practical solutions



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)

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** (...)

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;**

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.

Preamble 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

Article 39 of CPR (Composition of the monitoring committee)

- MC members to be informed to exercise their rights

Legal obligation (6)

Payslips

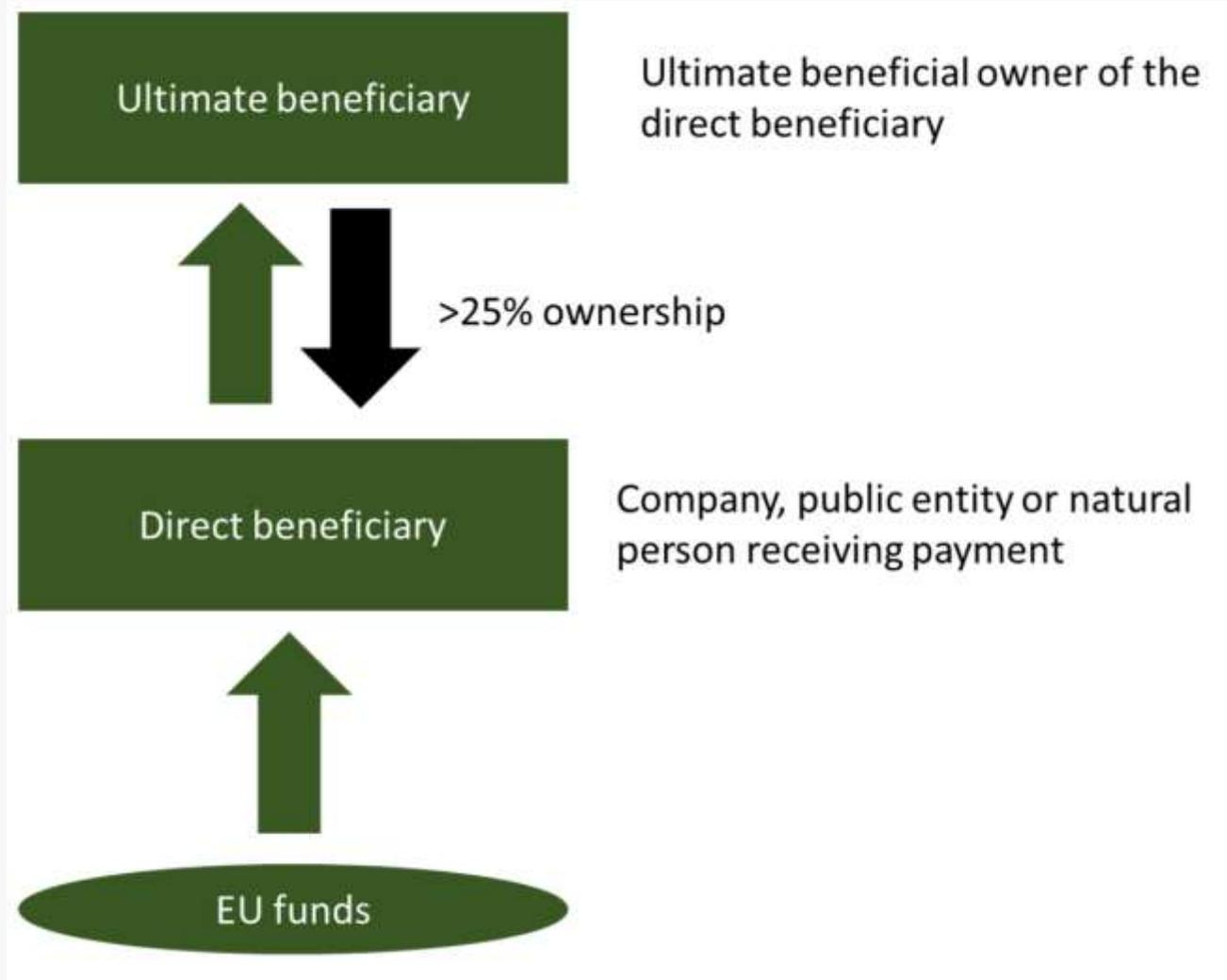
- If staff costs are reimbursed as full time employment they need to be proven by the **employment document and payslips**);
 -
- Art 39 (3) of Interreg Regulation (Staff costs)

Legal obligation (7)

Beneficial owners

- Annex XVII of CPR - Data to be recorded and stored electronically on each operation
- beneficial owners = ultimate beneficiary = ultimate beneficiary owner (UBO)
- Information on all beneficial owners of the beneficiary, if any, as defined in Article 3(6) of Directive (EU) 2015/849, namely **first name(s) and last names(s), dates(s) of birth and VAT registration number(s) or tax identification number(s)** – field 3
- beneficial owners of the contractor - field 23
- beneficial owners of the final recipient – field 69

Beneficial owners – who are they?



Source: [The Largest 50 Beneficiaries in each EU Member State of CAP and Cohesion Funds](#)

Beneficial owners – examples

Table 4.22 Top 50 direct beneficiaries CAP 2018 – EU

Rank	Direct beneficiary	Country	Beneficiary type	Union contribution [EUR]	Ultimate beneficiary(s)
1	EUROPEAN INVESTMENT BANK GROUP	EU	PUBLIC	46 937 643	
2	CONSEJERIA DE AGRICULTURAM. AMBIENTE Y D.RURAL	ES	PUBLIC	43 212 375	
3	DIRECCIÓN GENERAL DE DESARROLLO RURAL Y P	ES	PUBLIC	42 456 210	
4	LOGISTIEKE EN ADMINISTRATIEVE VEILINGSASSOCIATIE	BE	OTHER LEGAL PERSON	38 888 752	BELORTA (BE; 46%)
5	ΔΙΕΥΘΥΝΣΕΙΣ ΥΠ.Α.Α.Τ. (DIEUTHUNSEIS UP.A.A.T.)	GR	PUBLIC	35 622 068	
6	AGRARMARKT AUSTRIA	AT	PUBLIC	32 470 574	
7	SAS SUCRIERE DE LA REUNION	FR	LIMITED	31 800 725	TEREOS SCA (FR; 100%)
8	XUNTA DE GALICIA	ES	PUBLIC	31 602 567	
9	F.IN.A.F. FIRST INTERNETIONAL ASSOCIATION FRUIT SOC.CONSORTILE A RL	IT	OTHER LEGAL PERSON	28 431 602	
10	AOP GRUPPO VI.VA. VISIONE VALORE SOCIETA' COOPERATIVA AGRICOLA	IT	OTHER LEGAL PERSON	22 956 983	

Beneficial owners – examples

29	AOP UNOLOMBARDIA SOCIETA' AGRICOLA CONSORTILE A RESPONSABILITA' LIMITATA	IT	LIMITED	11 806 492	BONDUELLE (IT; 100%)
30	ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ (ΚΟΙΝΩΝΙΑ ΤΙΣ ΠΛΗΡΟΦΟΡΙΑΣ)	GR	LIMITED	11 691 238	GENERAL GOVERNMENT GR (100%)
31	RURAL PAYMENTS AGENCY	UK	PUBLIC	11 635 447	
32	AGENCJA RESTRUKTURYZACJI I MODERNIZACJI ROLNICTWA	PL	PUBLIC	11 366 823	
33	GOBIERNO DE ARAGÓN	ES	PUBLIC	10 659 708	
34	NATIONAL TRUST	UK	OTHER LEGAL PERSON	10 548 893	
35	SC AGRICOST S.A.	RO	LIMITED	10 458 317	SHEIKH AHMED BIN KHALED AL NAHYAN (AE; 50%), SHEIKH KHALED BIN ZAYED AL NAHYAN (AE; 50%)
36	LAND MECKLENBURG-VORPOMMERN MINISTERIUM FÜR LANDWIRTSCHAFT	DE	PUBLIC	10 357 941	

Legal obligation (8)

State aid recipients in Transparency Award Module

The Member State concerned shall ensure the publication, in the Commission's transparency award module or on a comprehensive State aid website, at national or regional level

(c)

the information referred to in Annex III on each individual aid award exceeding EUR 100 000 (...)

GBER Article 9(1)

Consent or Legal obligation ?

Task 2

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 time 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)

- Physical protection of the place where the data is stored, IT systems, trainings for employees
- Shredding old papers with personal data
- **Encryption of data (attachments to e-mails, pendrives, laptops) ALWAYS**
- Data more vulnerable (health, card numbers, ID numbers) to be misused protected in a more sophisticated way
- Restore possibility if data lost

Security of processing (2)

- Data only for its identified purpose not for others: hidden copy in emails, protected pdfs, sections in Monitoring System visible to entitled, restricted folders on shared drives
- Human factor - employees to be aware what they are entitled to do with the data
- IT systems might be protected, but unaware employees might create leakage (unprotected pendrive, phone or laptop lost or stolen, undestroyed papers thrown away)

Data breach notification

- 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 - **not only theft, but data spill**
- likely to result in a risk to rights and freedoms of natural persons should be notified to them without due delay
- 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 privates / public in some MS

- 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

Interact to support your GDPR compliance

Regular webinars:

- Interact will investigate the areas of major interest for Interreg Programmes within GDPR compliance and offer targeted webinars

Establishment of a dedicated Thematic Network on GDPR issues

- Creation of a dedicated community animated by Interact to disseminate GDPR best practices, answer questions and doubts but also allow its members to discuss with each other and exchange common issues and best practices

Annual GDPR on site event

- The occasion once a year to meet in person for the purpose of reinforcing the network and discuss together



Wrap-up and closure

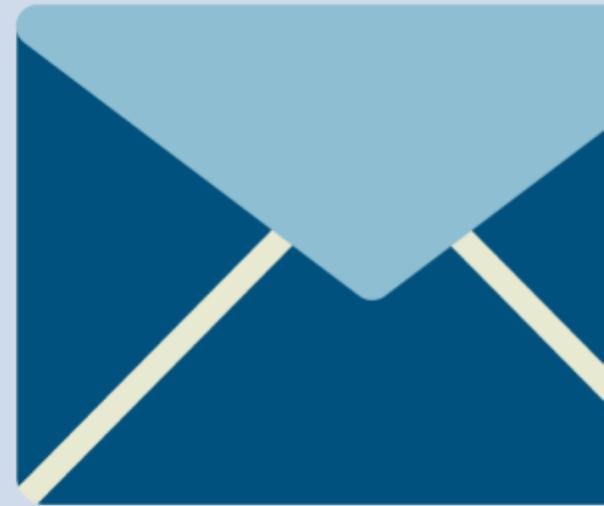
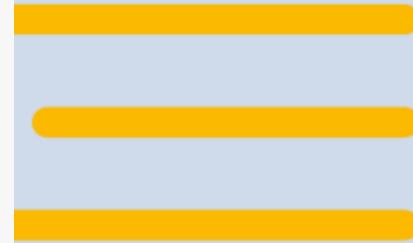
Please fill in our evaluation survey – thank you in advance!



Contact us @

Przemyslaw.kniaziuk@interact-eu.net

Mikis.moselt@interact-eu.net



Cooperation works

All materials will be available on:
[Interact / Library](#)