

# General Data Protection Regulation (GDPR)

---

Introduction to the General Regulation

Legal Bases for processing

Data Subject Rights

# Structure

A> Framework

B> Terminology

C> Data Protection Principles

D> Legal Basis

E> Data Subject Rights

A

Framework

## Protection + Flow

•Title: "**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)**"

It covers:

- Processing Personal Data by a data controller that resides in the EU
- Processing of data of data subjects residing in the EU
- Processing of data that

## Protection + Flow

• Recital 9: «Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. .»

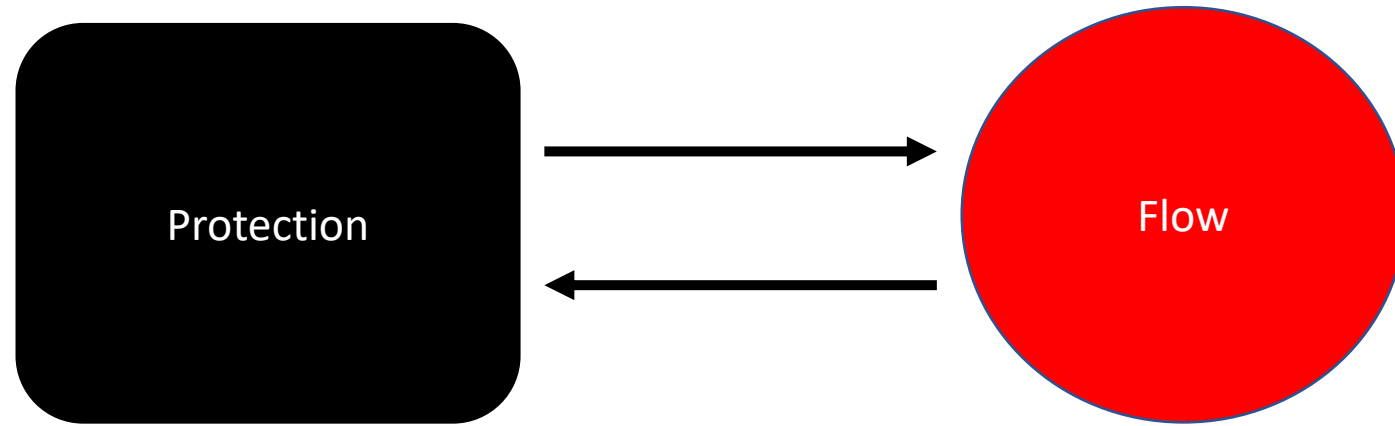
• Recital 12: "Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data."

## Protection + Flow

- Recital 4 “The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.”

Recital 18 “This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.”

# Protection + Flow

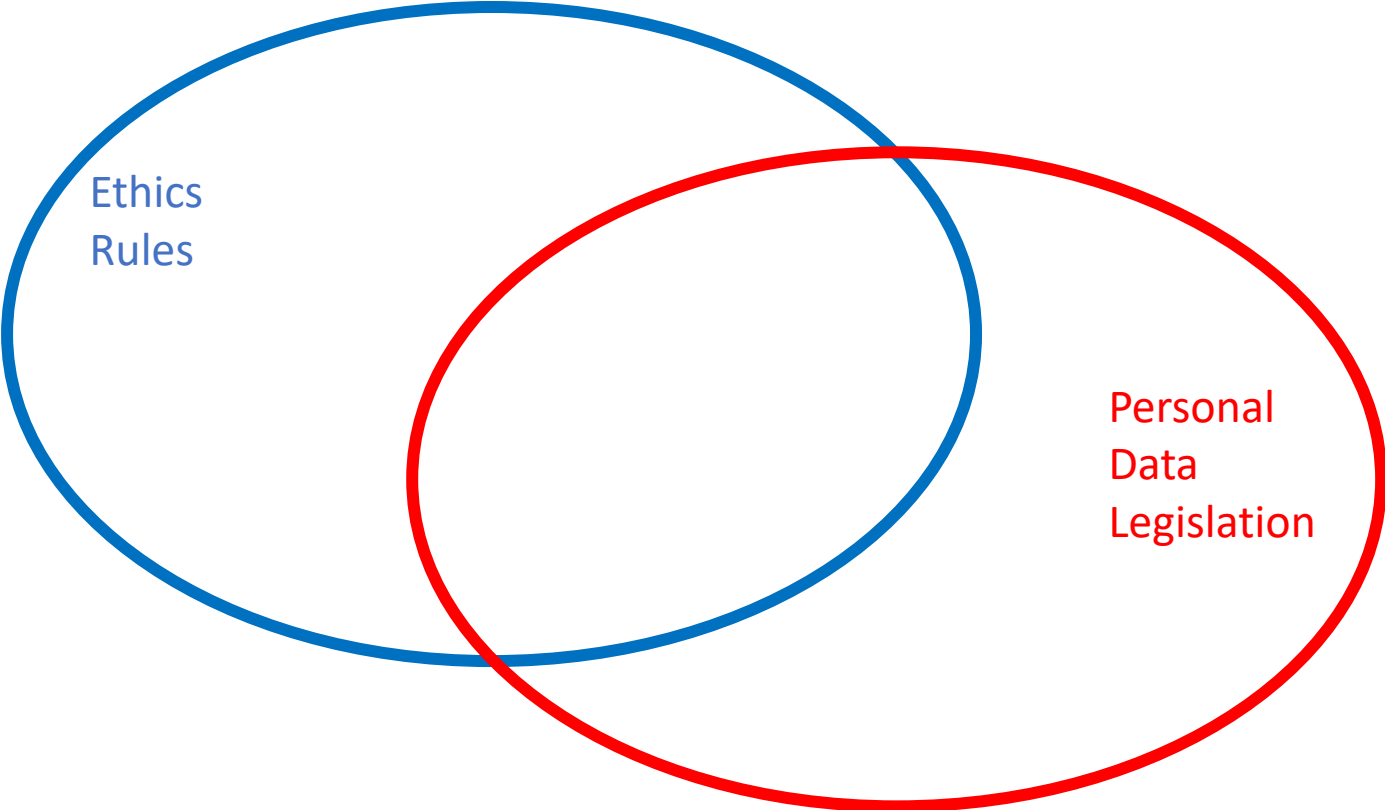


## Protection + Flow

- The 5<sup>th</sup> Freedom
- Adding to the other 4 freedoms (free flow of persons, goods, services, capital)
- Free and without barriers flow of knowledge/ information/ data within the EU  
[http://europa.eu/rapid/press-release\\_SPEECH-07-257\\_en.pdf](http://europa.eu/rapid/press-release_SPEECH-07-257_en.pdf)
- GDPR as part of the Digital Single Market Policies
- GDPR as Part of the broader policies for the Data Economy in Europe:
- Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the re-use of public sector information (recast) COM/2018/234 final - 2018/0111
- Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM(2017)495)



# Ethics vs Personal Data



# Types of questions related to personal data

Labor relations/ Administration

Data Subject

Admin of  
Data Controller/  
Data Processor

Research/ Service Provision

Data Subject

Admin of Data  
Controller/ Data  
Processor

Customer/ Citizen

Data Subject

**B**

Terminology

a

## Personal Data

- ‘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 a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

## Examples

- Name and Surname
- Address
- E-mail
- IP- Address
- Salary
- IBAN
- Telephone no
- Registration nos (e.g. social security)
- passwords

They include personal data:

- Authorizations
- Statutory documents , Public documents of corporations
- Certificates
- CVs
- Salary statements/ lists
- Contracts
- Transparency documents
- Research data
- Registries
- Log files
- Administrative documents/ correspondence
- Google Analytics
- Forms

Attention!

## Personal Data

- Only involve living persons
  - Not deceased
  - Not legal persons



## Special Categories of personal data

Art. 9(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.



## Examples

### Special Categories

- Leave of absence
- Research data
- CVs

## Special Categories of Personal Data I

### Special Categories of personal data may be processed under the following conditions:

- (a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment and social security** and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

## Special Categories of Personal Data II

### **Special Categories of personal data may be processed under the following conditions:**

- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- (e) processing relates to personal data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

## Special Categories of Personal Data III

### **Special Categories of personal data may be processed under the following conditions:**

- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

## Special Categories of Personal Data IV

### **Special Categories of personal data may be processed under the following conditions:**

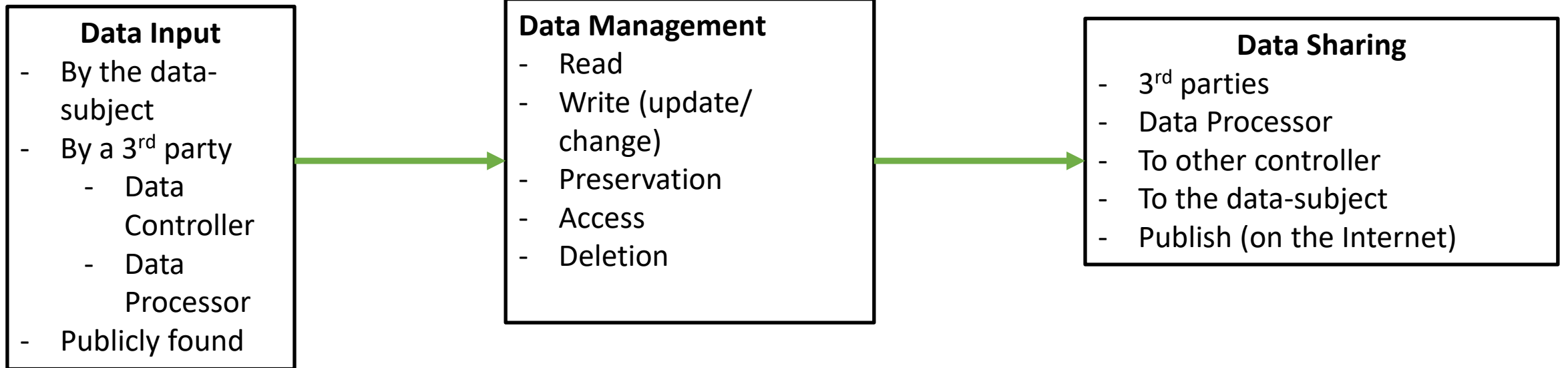
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

b

## Processing

- ‘processing’ means any 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

# Processing = Flow of data







- Almost all action in the context of management are processing
- Processing in the context of research appears:
  - When research involves humans
  - When research services are offered through e-infrastructures/ Research infrastructures

C

## Data Controller

- ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

d

## Data Processor

- ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

When someone is a controller and when a processor?

- The same organization may play different roles in different processing scenarios
  - Research Institute (language processing)
    - Employees' personal data (data controller)
    - Tender for LREC (data processor for the EC)
- What I must always check:
  - Who is in control of the purpose and the means of the processing?
  - Is there a contract?



I work for an organization, am I the data controller or processor?

- NO
- The controller is the legal person I work for
- I operate as a third party or as a “data manager”



e



# DPO

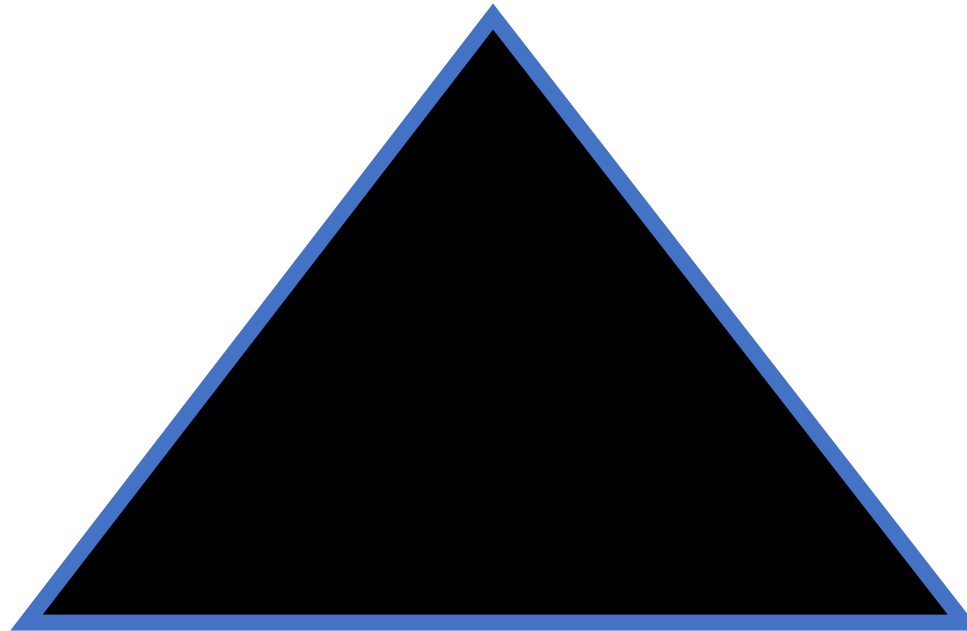
- \* **Data Protection Officer**

- \* Understanding of the role (coordination not decision making)
- \* Understanding the relationship with existing organizational structure and roles (e.g. Internal Audit, owners of procedures)
- \* The person of the DPO
  - \* Need to have experience and understanding of the organisation
  - \* Conflict of interest (the owner of a process cannot be the DPO as well)

# Responsibilities/ liability

**Administration**  
(Board of Directors/ CEO: decide)

**DPO**  
(coordinates, controls,  
advises)



**Employees**  
(third parties: the  
execute)

f

## Third party

- 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

gg

## Pseudonymisation

- pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

h

## Consent

- 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;



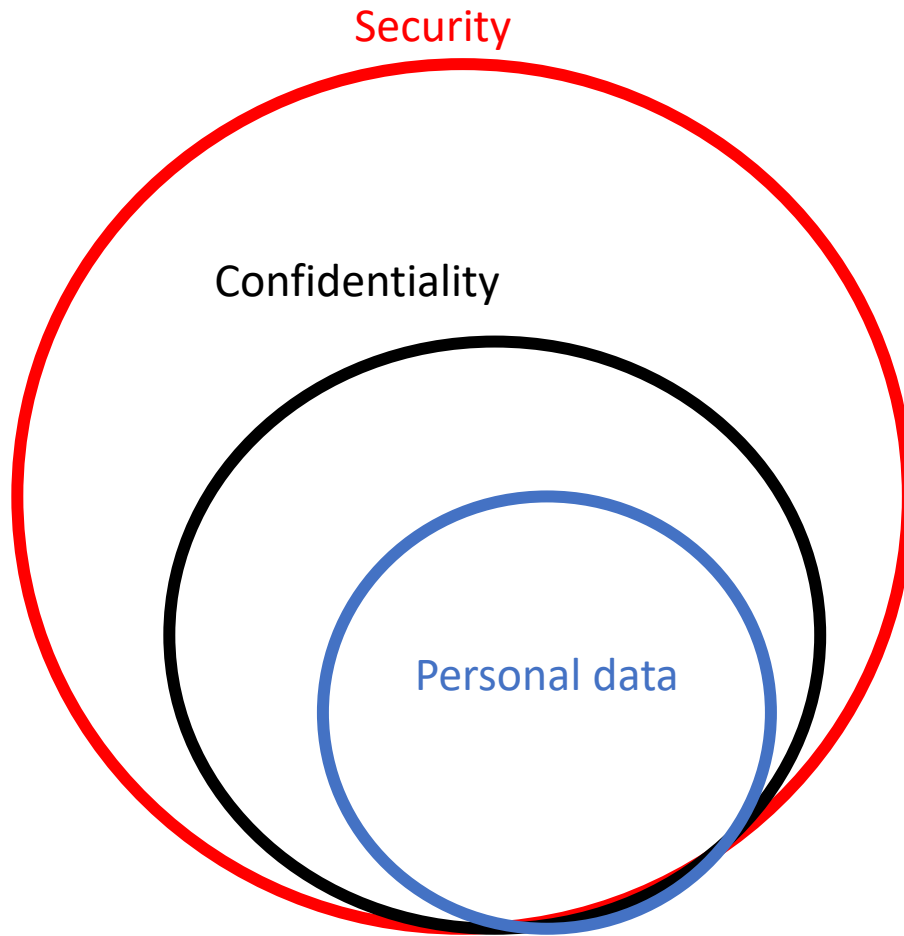
i

## Data breach

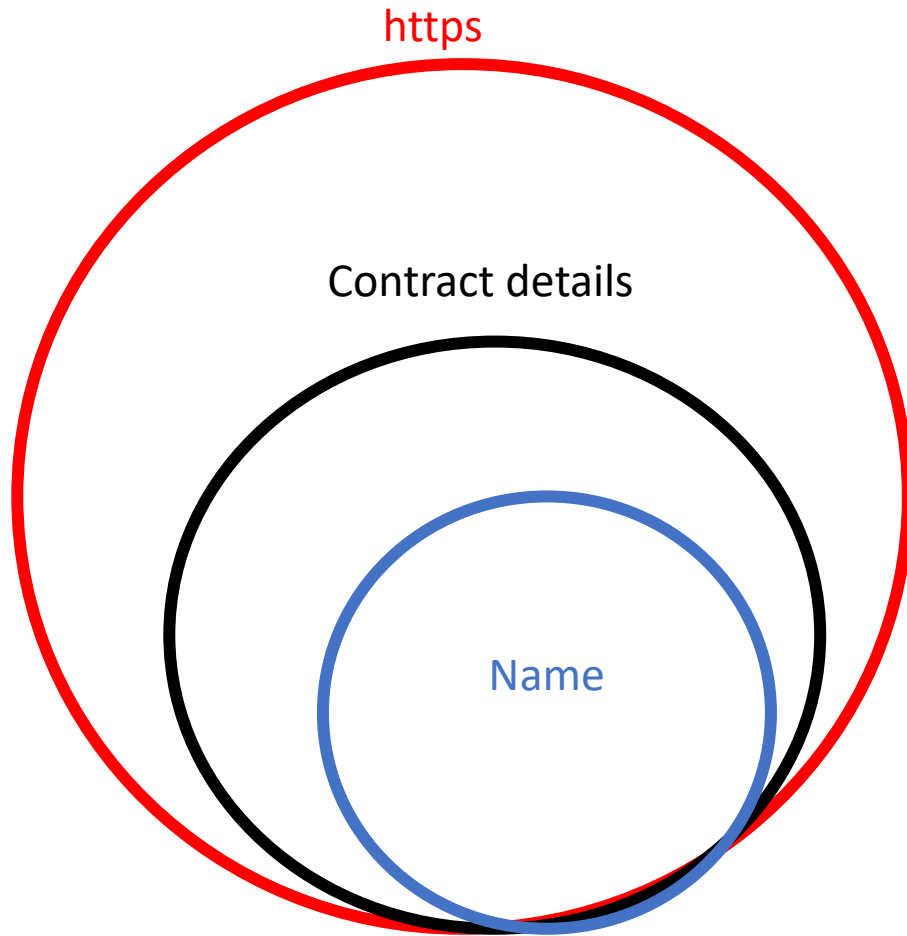
‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

j

## Conceptual Cycles



# Conceptual Cycles

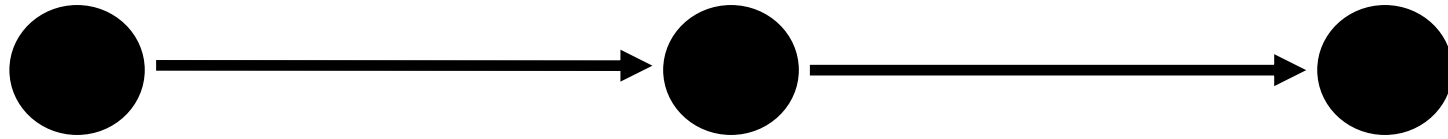


i info

What to read



Άρθρο 4 GDPR: Definitions

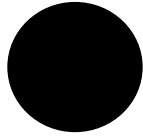


Assessment

Gap Analysis  
Technical/ Org/  
legal measures

Continuous  
compliance

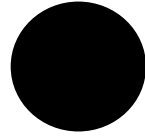




## Assessment

- Identification of data/ information resources
- Data flows diagrams
- 4 levels control  
(legal/ technical/ Organisational/ procedural)
- Gap identification and analysis

| XXXX DATA PROCESSING                                      |  |   |   |                             |  |   |  |   |  |  |   |  |  |  |   |  |  |
|---|--|---|---|-----------------------------|--|---|--|---|--|--|---|--|--|--|---|--|--|
|   | DATA INPUT   |   | DATA INTERNAL PROCESSING                                      |                             |  |   |  |   |  |  |   |  | DATA OUTPUT  |  |   |  |  |
| THE QUESTION WE ASK OURSELVES TO FIND WHAT INFO TO INSERT | How did the data arrive to us?   | Was there an official opt in method? To what do they opted in?  | In what kind of list do we put the data (Genre of recipients) | File name and date created  | What data do we store for each member of the list        | Where and how is the list stored?         | Is the list transferred to another kind of file? | Who received the data? Who has access to the list (view or edit)? | Who processes the data? Who has access to the list (view or edit)? | Who uses the list? (Department / role)?  | What do we communicate to the list?   | What tool of comms do we use?                            | With who (outside the organization) do we share listed data?   | Who shares the data? (Department / role) | For what purpose do we share the data?                                  | How do we export and send the data?                                    | Who else may have access to the data exported ?  |
| EXAMPLES OF POSSIBLE ANSWERS                              | Private contacts / Official website / Ticket buyer / Scholarship application / Newsletter subscription | Yes - Newsletter opt in box in website<br>Yes - Scholar who deposited contact info<br>Yes - a business card after a meeting<br>No - email found cced in a group mail<br>No - contact on private smart phone | Patients/ Friends/ Family/ Staff                              | e.g. <Medica_D_P2> Dec 2014 | e.g. First name, surname, Age, email address, cell phone | e.g. Common drive / Excel doc AND/ OR CRM | e.g. Yes - Newsletter platform segmented list    | e.g. Personnel  | e.g. Personnel/ Marketing/ Admin                                   | e.g. Marketing department & All departments who have access to the newsletter platform | Promo material / Communication regarding a request from the interested party / Questionnaires for customer satisfaction assessment or other surveys | Newsletter platform / Social media / Direct mail / Phone | Digital Performance collaborators (e.g. XXXX), Insurance, Security, Social media platforms, Legal advisors, PR offices | e.g. REA admin/ Doctors / all members    | Social campaign targeting / Event coordination / sms promo campaign ... | create new excel which is sent via direct mail / data printed in paper | anyone who has access to the mailbox of the receiver / anyone who can copy the printed papers etc. |



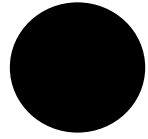
Analysis



Gap Analysis



Choice/ selection/ implementation of compliance measures



Continuous compliance



Setting up of data protection forum



Following application and compliance



Updating measures



Training

C

Principles

## Principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability principle


a


## Lawfulness, fairness and transparency

- You must identify valid grounds under the GDPR (known as a ‘lawful basis’) for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.




← → ↻ 🔒 https://www.athena-innovation.gr

 **ATHENA** Έρευνα & Καινοτομία  
Τεχνολογίες Πληροφορίας

Ο ιστότοπος είναι υπό κατασκευή  English Είσοδος Επικοινωνία

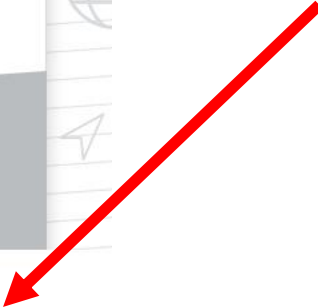
Ινστιτούτα & Μονάδες Ταυτότητα Άνθρωποι Έρευνα Έργα Καινοτομία Υποδομές Νέα

 **Climate-KIC**

**Επίσημη τελετή έναρξης του EIT Climate-KIC Hub Greece**

**We use cookies on this site to enhance your user experience**  
By clicking any link on this page you are giving your consent for us to set cookies.

[More info](#) [OK, I agree](#) [Decline](#)

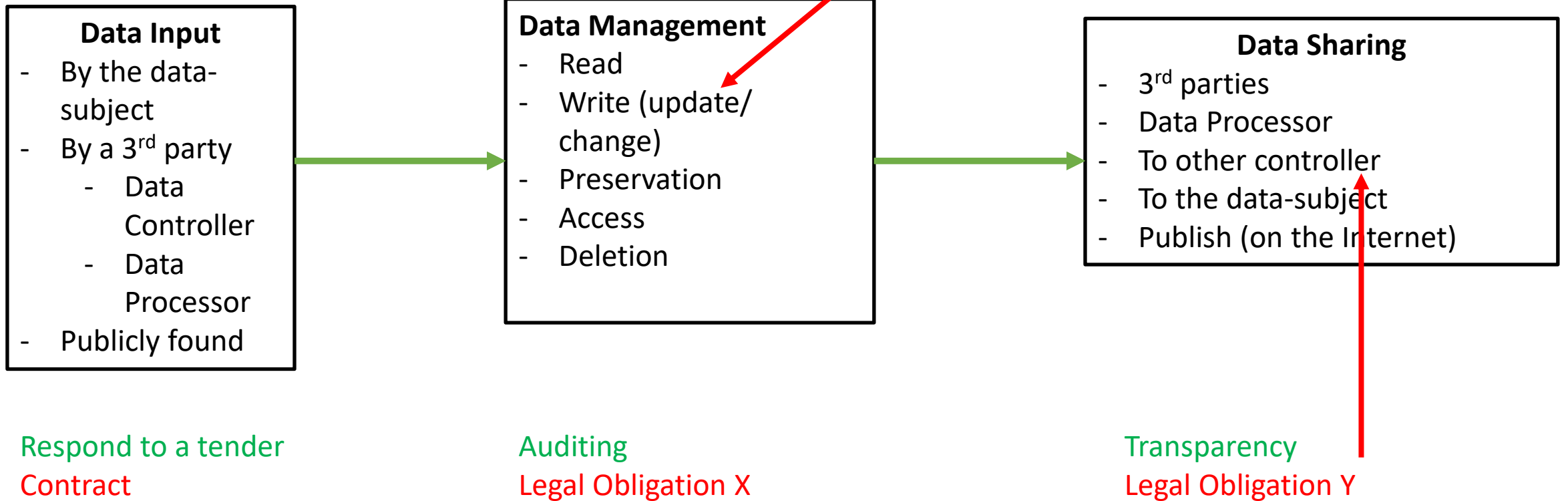


b

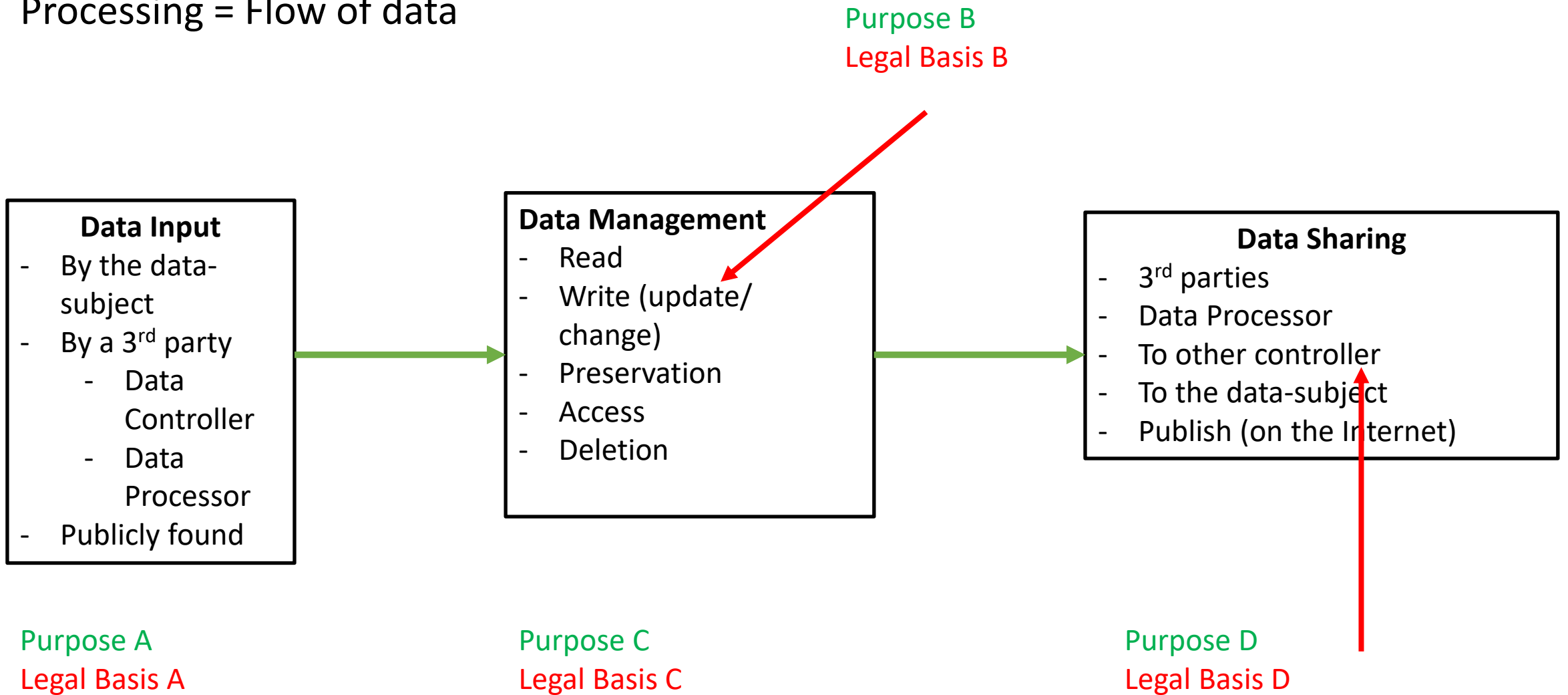
## Purpose limitation

- You must be clear about what your purposes for processing are from the start.
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law.

# Processing = Flow of data



# Processing = Flow of data



C

## Data minimisation

- You must ensure the personal data you are processing is:
  - adequate – sufficient to properly fulfil your stated purpose;
  - relevant – has a rational link to that purpose; and
  - limited to what is necessary – you do not hold more than you need for that purpose

## Examples

### Employee's data

- I retain only the data that are necessary for the specific data processing objectives



d

## Accuracy

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.

## Example

### Employees' data

- request updating of data once per year

### Research data

- Updating data once per year
- Informing data subjects when their data are updated

e

## Storage limitation

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

## Examples

### Employee Data

- Τα διατηρώ μόνο για το διάστημα που είναι απαραίτητος για το νόμιμη βάση επεξεργασίας
- Δημιουργώ πρωτόκολλα καταστροφής

### Δεδομένα Έρευνας:

- Τα καταστρέφω μετά τη λήξη της έρευνας και σύμφωνα με τους όρους της χρηματοδότησης/ ελέγχου
- Δημιουργώ πρωτόκολλα καταστροφής

f

## Integrity and confidentiality (security)

- A key principle of the GDPR is that you process personal data securely by means of ‘appropriate technical and organisational measures’ – this is the ‘security principle’.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the ‘confidentiality, integrity and availability’ of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.
-



## Examples

### Employee/ Research Data:

- Registering different measures
  - security (technical)
  - legal

gg

## Accountability principle I

- The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.
- You must have appropriate measures and records in place to be able to demonstrate your compliance.

## Accountability principle II

- Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance. You need to put in place appropriate technical and organisational measures to meet the requirements of accountability. There are a number of measures that you can, and in some cases must, take including: adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on your behalf;
- maintaining documentation of your processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer; and
- adhering to relevant codes of conduct and signing up to certification schemes.

## Accountability principle III

- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

D

Legal Basis

## Lawful basis for processing

- 1. Consent**
- 2. Contract**
- 3. Legal Obligation**
- 4. Vital Interests**
- 5. Public Task**
- 6. Legitimate Interests**
- 7. Special Category Data**
- 8. Criminal Offence Data**

## Consent I

- The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.
- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh your consents if they don't meet the GDPR standard.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.



## Consent II

- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.

## Contract

- You can rely on this lawful basis if you need to process someone's personal data:
  - to fulfil your contractual obligations to them; or
  - because they have asked you to do something before entering into a contract (eg provide a quote).
- The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

## Legal obligation

- You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.
- This does not apply to contractual obligations.
- The processing must be necessary. If you can reasonably comply without processing the personal data, this basis does not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.
- You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.

## Vital Interests

- You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
- The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.
- You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.
- You should consider whether you are likely to rely on this basis, and if so document the circumstances where it will be relevant and ensure you can justify your reasoning.

## Public task

- You can rely on this lawful basis if you need to process personal data:
  - ‘in the exercise of official authority’. This covers public functions and powers that are set out in law; or
  - to perform a specific task in the public interest that is set out in law.
- It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
- You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.
- The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.
- Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

## Legitimate interests I

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests. Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to: identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

## Legitimate interests II

- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

## Special Category Data

- Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.
- In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.
- There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Act 2018 introduces additional conditions and safeguards.
- You must determine your condition for processing special category data before you begin this processing under the GDPR, and you should document it.



## Criminal offence data

- To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.
- The Data Protection Act 2018 deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.
- You can also process this type of data if you have official authority to do so because you are processing the data in an official capacity.
- You cannot keep a comprehensive register of criminal convictions unless you do so in an official capacity.
- You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

- Vital interest

- Public Task
- Legal Obligation

- Contract
- Consent

- Legitimate Interest

No discretion

Discretion

Decision: Data Subject/ Controller

Decision: Data Controller

Objective

Processing employee data

Legal Basis

Contract

Data Subject Rights

All rights

The background features a stylized illustration of two hands holding a document. The document is tilted and contains several horizontal lines representing text, a square box, and a red checkmark. The hands are rendered in a light orange color. In the top right corner, there is a solid red rectangular box containing the text 'Checklist I' in white.

## Checklist I

- We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.
- We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
- We have documented our decision on which lawful basis applies to help us demonstrate compliance.

## Checklist II

- We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.
- Where we process special category data, we have also identified a condition for processing special category data, and have documented this.
- Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.

- Vital interest

- Public Task

- Legal Obligation

- Contract
- Consent

- Legitimate Interest

No discretion

Discretion

Decision: Data Subject/ Controller

Decision: Data Controller

# Lawful Bases

## Employment / Administration

- Contract
  - Call for proposals
  - Contract
- Legal Obligation
  - Transparency
- Consent
- Legitimate Interest
  - CCTV
  - Security Cards

## Research / Service provision

- Contract
  - (grants/ tenders)
  - ToS
- Consent
  - Research
  - Direct Marketing
- Legitimate interest
  - ToS
  - Notices
- Public Task
  - Notices
  - Legal documentation

## Legal Bases and Data Subject Rights

|                      | Right to erasure | Right to portability | Right to object                           |
|----------------------|------------------|----------------------|---|
| Consent              |                  |                      | <b>x</b><br>but right to withdraw consent |
| Contract             |                  |                      | <b>x</b>                                  |
| Legal obligation     | <b>x</b>         | <b>x</b>             | <b>x</b>                                  |
| Vital interests      |                  | <b>x</b>             | <b>x</b>                                  |
| Public task          | <b>x</b>         | <b>x</b>             |   |
| Legitimate interests |                  | <b>x</b>             |   |



**E**

Data Subject Rights

# Data Subject Rights

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

a

## Right to be informed I

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this ‘privacy information’.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

## Right to be informed II

- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.
- User testing is a good way to get feedback on how effective the delivery of your privacy information is.

## Right to be informed III

- You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.
- Getting the right to be informed correct can help you to comply with other aspects of the GDPR and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

b

## Right of Access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.



C

## Right to rectification

- The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You have one calendar month to respond to a request.
- In certain circumstances you can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

d

## Right to erasure

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as ‘the right to be forgotten’.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on you to consider whether to delete personal data.

e

## Right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have one calendar month to respond to a request.
- This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

f

## Right to data portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.
- Some organisations in the UK already offer data portability through midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.



gg

## Right to object

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies you may be able to continue processing if you can show that you have a compelling reason for doing so.
- You must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- You have one calendar month to respond to an objection.

h

## Rights related to automated decision making including profiling I

- The GDPR has provisions on: automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
- The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

## Rights related to automated decision making including profiling II

- You can only carry out this type of decision-making where the decision is: necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.
- You must identify whether any of your processing falls under Article 22 and, if so, make sure that you: give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

- In order to be able to respond to the data subject request, there is recording of:
  - procedures (steps)
  - Third Parties (administrators)
  - Data Types
  - Processing objectives per type of data
  - Lawful basis in the data life-cycle
  - Notices
  - Consent
- If there is legitimate interest or large quantities/ special data types
  - Perform Data Protection Impact Assessment/ Legal Interest Impact Assessment (DPIA/ LIIA)



## Personal Data Breaches

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

## Documentation I

- The GDPR contains explicit provisions about documenting your processing activities.
- You must maintain records on several things such as processing purposes, data sharing and retention.
- You may be required to make the records available to the ICO on request.
- Documentation can help you comply with other aspects of the GDPR and improve your data governance.
- Controllers and processors both have documentation obligations.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.



## Documentation II

- Information audits or data-mapping exercises can feed into the documentation of your processing activities.
- Records must be kept in writing.
- Most organisations will benefit from maintaining their records electronically.
- Records must be kept up to date and reflect your current processing activities.
- We have produced some basic templates to help you document your processing activities.

## Data Protection by design and by default

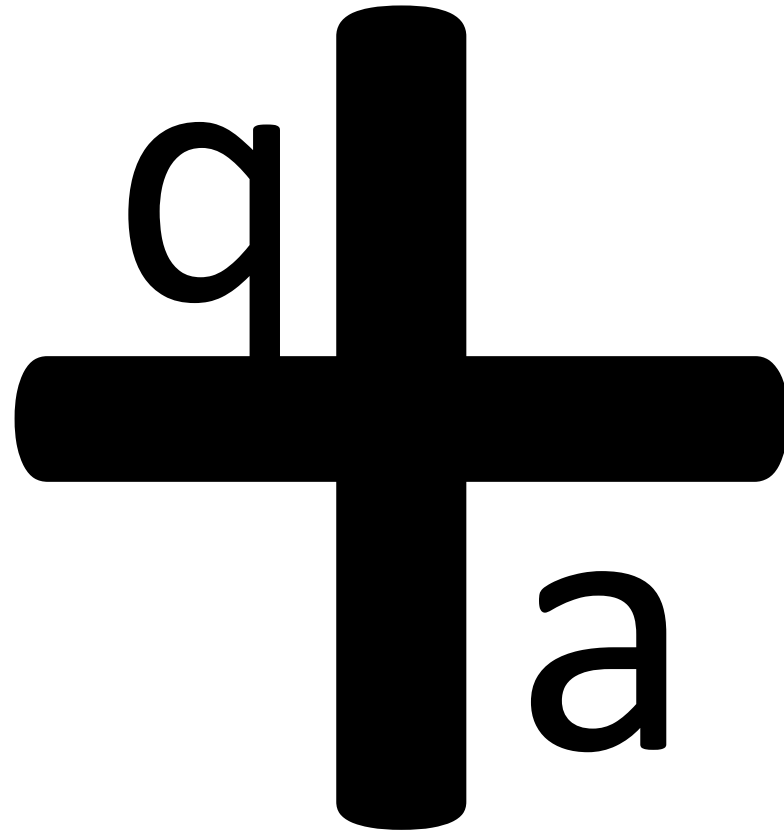
- The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is ‘data protection by design and by default’.
- In essence, this means you have to integrate or ‘bake in’ data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as ‘privacy by design’, it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR’s fundamental principles and requirements, and forms part of the focus on accountability.

## Data protection impact assessments I

- A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. You can use our screening checklists to help you decide when to do a DPIA. It is also good practice to do a DPIA for any other major project which requires the processing of personal data. Your DPIA must: describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

## Data protection impact assessments II

- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals.
- High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult your data protection officer (if you have one) and, where appropriate, individuals and relevant experts.
- Any processors may also need to assist you.
- If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, we may issue a formal warning not to process the data, or ban the processing altogether.



[ptsiavos@eplo.int](mailto:ptsiavos@eplo.int)  
@prodromos