How to write Privacy Policy and Terms of Use documentation for the EOSC Portal: Personal Data

Dr. Prodromos Tsiavos

Senior Legal & Policy Adviser

ARC/ OpenAIRE

ptsiavos@athenarc.gr
Prodromos.tsiavos@openaire.eu

https://www.athena-innovation.gr/
https://www.openaire.eu/

1 How does a PD policy look like

2 Legal Framework

3 The PD processing stack

4 PD policy components

5 Summary of a PD policy

1

How does a Personal Data (PD) Policy look like?

Privacy Policy

Type A:
Table-like

Questions to ask yourself when defining this policy:

- Who or what is your Data Controller?
- Will your Research Community have a Data Protection Officer?
- Which information do you need to collect on the user? Is this minimised?
- Specific data collected by each service may vary. Can your Infrastructure provide a template statement for all services?

This policy is effective from 2020-11-01.

Name of the Service	WORSICA
Description of the Service	WORSICA (Water Monitoring Sentinel Cloud Platform), is a one-stop-shop service to provide access to customized remote sensing services based on Copernicus data, currently applied to the detection of the coastal water land interface, the inland water detection, and for water irrigation infrastructure leak detections.
Data controller and a contact person	Alberto Azevedo (aazevedo@lnec.pt)
Data controller's data	Ana Paula Seixas Morais (paulamorais@lnec.pt)

Users' rights and obligations

The contents of this site are protected under literary and artistic property law, the Bern Convention, EU directive 96/9/CE and book 1 of the French Code de la propriété intellectuelle . All reproductions other than for the personal use of visitors to the site, notably with a view to publication in any form, are strictly forbidden without the express written permission of Pl@ntNet.

Visitors are responsible for their interpretation and use of the information consulted, and for the data they provide on forms included in the site. They are bound by the prevailing rules and regulations.

Intellectual property rights

No element of the Pl@ntNet application shall be copied, reproduced, modified, republished, downloaded, distorted, transmitted or distributed, howsoever done, partially or integrally, without the written and prior authorization from Pl@ntNet, except for the strict needs of the press and provided that the intellectual property rights and any other mentioned property rights are being respected.

Type B:
Free Text

Personal data

By registering to the Pl@ntNet API application, you accept that your identity, under the names, surnames and email address you specified when registering, is stored by Pl@ntNet until the account is cancelled.

In accordance with Articles 49 and following of Law No 78-17 of 6 January 1978 on data processing, files and freedoms and Articles 15 and following of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (RGPD or GDPR), any person may:

- have confirmation that personal data relating to him/her are or are not processed and, where they are processed, access to such personal data,
- request the correction or deletion of his/her personal data,
- request that the processing of his/her personal data be limited,
- request the portability of his/her personal data if the processing is based on consent or a contract.

Any person may also, for legitimate reasons, object to the processing of data concerning him/her.

Any person may give general or specific instructions regarding the storage, erasure and communication of your personal data after your death.

Initial Thoughts I: Basic Terminology

- **Privacy vs. Personal Data:** While frequently used as if synonymous, in most EU jurisdictions do not coincide: Privacy is related to the broader right of a person to retain her personal sphere private, in most cases as an emanation of her personality; Personal Data protection is strictly defined by the GDPR and respective national laws. PD protection is part of Privacy protection.
- **Policies:** are legally relevant documents expressing to the recipient of the service the self-imposed restrictions in relation to how personal data are to be processed.
- **Terms of Use (ToU):** are legally binding documents containing multiple terms to which the recipient of a service has to agree (either by explicitly accepting them or by using the service) in order to use the service.
- **Personal Data (PD) / Privacy Notices:** are legally relevant documents describing the ways in which personal data are processed, the data controller and/or processor, the legal basis of processing and the rights the data subject has. A PD Notice may contain or identify with a PD/ Privacy Policy
- **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 (art. 4(12) GDPR)

Initial Thoughts II: Why to go for a table-like PD Policy

- It is easier to read.
- You make sure you do not miss any of the essential parts of a policy
- It is easy to identify amendments from version to version
- It allows easy comparison between different service providers
- It is easy to update

Some key elements regarding the overall Terms of Use

Class A: conditions regarding accessing the service

- Is registration required
- Are there limitations in terms of:
  - IP location (geolocation)
  - Use of API
    - Volume
    - Requests
  - Institutions having access to the service

Key elements regarding the overall Terms of Use I

Class A: conditions regarding accessing the service

- Is registration required (classes of Users – Registered/ unregistered)
- Are there limitations in terms of:
  - IP location (geolocation)
  - Use of API
    - Volume
    - Requests
  - Institutions having access to the service
- Other obligations:
  - Attribution
  - Non-commercial use
  - Private Use
  - Non-redistribution
- Adherence to specific policies:
  - Personal Data
  - Confidentiality

Key elements regarding the overall Terms of Use II

Class B: conditions regarding the assets

- Copyright ownership
- Copyright licensing
  - All rights reserved Assets
  - Open Licensing
    - Custom licence
      - Key terms
    - Standard licence
      - Software (e.g. GPL/ BSD)
      - Content (e.g. CC)
      - Service (e.g. GPL Affero)
- Treatment of other types of Intellectual Property Rights
  - Trademarks
  - Confidential Information / Trade Secrets
  - Patents

Task 0: Key Elements of ToU

- Identify:
  - Key conditions regarding access to the service
  - Key conditions regarding assets

2 Legal framework

What is GDPR?

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)

Is the GDPR framework enough?

- Initially yes…
- …but make sure you are familiar with your national PD processing framework
- De minimis:
  - What are the national Personal Data Laws
  - What kind of further specification of the GDPR they include (mostly in relation to labour relationships, national security and special categories of data)
  - What your National Data Protection Authority is and if it has issued any guidelines in relation to research services

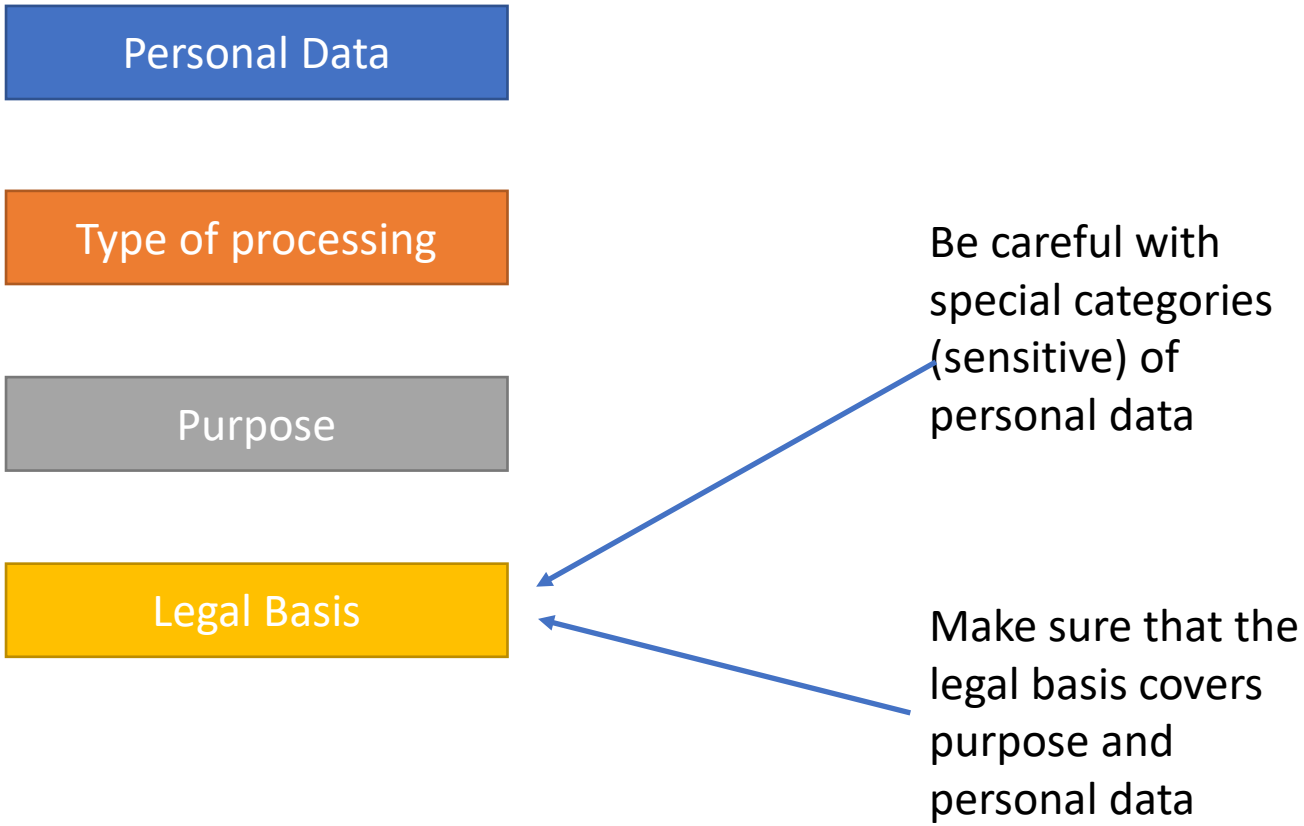
Task I: Legal and Institutional Framework

- Identify your national Data Protection Law
- Identify your Data Protection Authority

3

The personal data processing stack

DP processing structure



4

PD Policy Components

The Service

- Define the service
- This is not a strict GDPR requirement
- It is an essential starting point for identifying the GDPR required definitions, i.e.:
  - Who controls the data processing
  - Who conducts the data processing
  - What processing does it take place
  - What data are processed
  - What is the duration of the processing

Task II: Service Definition

- Define and describe your services in less than 150 words

Personal Data

b

‘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;

Try not to conflate personal data and legal basis in one category

Personal data processed and the legal basis	*A. Personal data retrieved from your Home organization:* • *Name* • *Username* • *Password* • *Email* • *Affiliation* • *Country* • *UUID - Unique user identifier (SAML persistent identifier) ** *If the registry of the users is done via EGI Check-In, the personal data retrieved in the process is responsibility of EGI.* *B. Personal data gathered from the users* - *Logfiles on the service activity** ** = no personal data is used, only the UUID and the processing outputs are used for management and debugging purposes of the service.*

Personal data processing is not just about collecting data

Personal Data Collected by Athena RC Website

We collect personal data only when you wish:

a) if you subscribe to our newsletter, your email address will be solely used for this purpose and shall not be shared with third persons. You will be able to be deleted from the newsletter anytime

b) if you contact by phone, fax or e-mail with the Athena RC and in order to serve the purpose of communication, personal data are kept as needed to fulfill the purpose of your communication.

During your visit at our website, certain information may be automatically collected, such as the IP address of your computer, but they do not reveal identifiable elements of your physical identity, but they are used solely for statistical reasons for traffic to our web presentation. In addition, cookies are collected and processed at the time of entry.

For more information, please see the relevant Cookies policy below

Examples

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

<u>They include personal data:</u>

- 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
- Medical Data
- COVID-19 (pandemic data – including movement)
- Research data
- CVs

Task III: Personal Data and Data Subject Definition

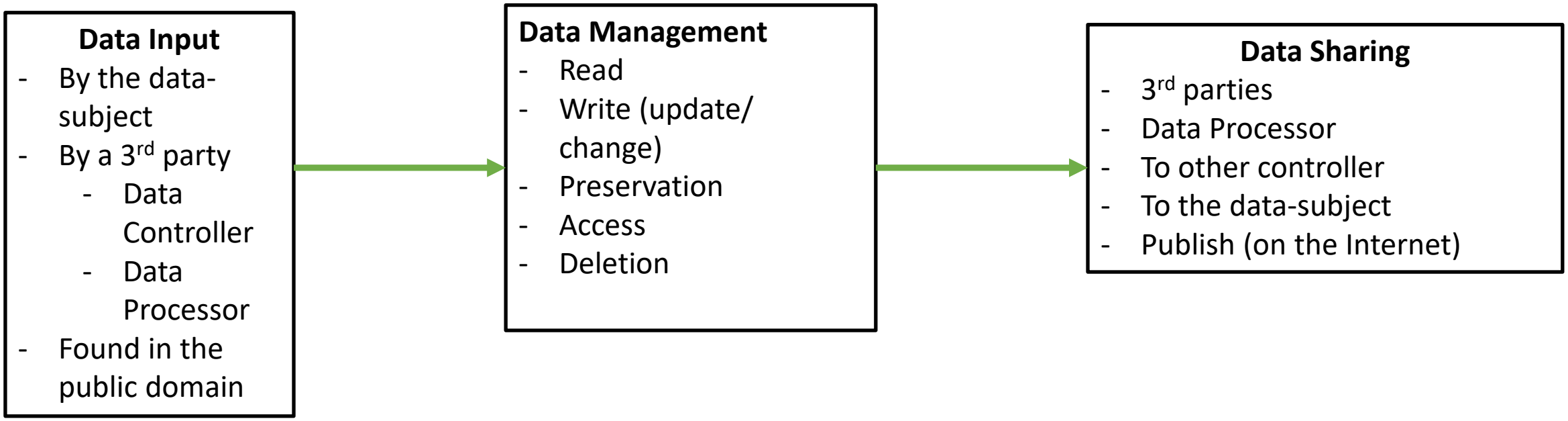
- Identify the Personal Data that are processed by your service
- Identify the potential data subjects whose data you are processing
- Are there any Special Category of Personal Data you are processing
    - If yes, identify them

Processing

C

‘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



Tips and hints

- Use the Service Description in order to derive the range of data processing you are conducting
- If you have a Data Management Plan (DMP) or other workflow in relation to the processing of the data, use it in order to identify the types of processing you are engaged with
- Follow the data:
  - Identify where you got the data from
  - Describe how you use them in the service
  - Identify who has access to them (internally and externally) for the purposes of providing the service
  - Describe duration of processing and identify retention period
  - Describe if entities beyond your organisation are going to have access to the data

Reality Check

- Go back to the personal data list and check if you need to add more data

Task IV: Types of Processing

- Identify:
  - Where did you get your data from
  - How are you storing/ processing/ retaining them
  - If you are sharing the data with any other entities beyond your organisation

Data Controller

d

‘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;

Do NOT conflate the data controller with the contact person

Data controller and a contact person	Alberto Azevedo (aazevedo@lnec.pt)

Provide the legal entity details, address and contact info

Data Controller

The personal data controller for the purpose of the operation of this website is as follows:

Athena-Research and Innovation Center in Information, Communication and Knowledge Technologies -Athena RC (Research Organisation private law legal body)
Artemidos 6 and Epidavrou
15125, Maroussi, Athens
tel: + 302106875300, fax: 2106854270
email: info@athena-innovation.gr

Tips and hints I: natural and legal persons

- Start with the service and processing descriptions and try to identify who is the entity that defines purpose and means of processing the personal data
- The data controller is the entity responsible for setting and supervising the objectives and means of data processing
- The data controller in the vast majority –if not in all- of the cases is going to be a legal entity; **NOT** the natural person responsible for the provision of the service (e.g. the Head of IT).
- If you wish to have a natural person as a contact point, indicate her at a separate field

Tips and hints II: co-controllers

- It is common that a service is offered by more than one entities. In such a case:
  - If the entities are engaged in autonomous processing of personal data, e.g. one is providing a log-in service and the other a data processing service, then:
    - each one needs to present PD Terms separately
    - if you are the entity that either receives or shares the data to other controllers, then you need to indicate this clearly
  - If one entity is defining the purpose and means of processing, then this is the data controller, and if the other one is processing on the former's behalf, then the latter is the data processor

Task V: Data Controller

- Identify:
  - The legal entity that sets the purpose and means of processing
  - If there are more than one entities offering the service identify their roles:
    - Who are the data controller(s)
    - Who are (if any) the data processor(s)

Data Processor

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

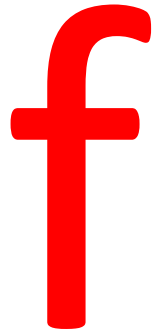
Tips and hints

- The data processor scenario appears only in the case where there are more than one entities engaged in personal data processing
- Check the terms and conditions under which you
  - got the data from
  - shared the data with
- Just because you obtained the data from or you shared the data with a third entity, does not mean that you are operating or working with a data processor.
- A data processor does not have control over the purpose and means of processing but only follows the directions of the data controller
- The data controller and the data processor are linked through a contract that needs to identify in detail the terms under which the processing will be taking place
- If you are operating as a data processor or are a controller that uses a processor you need to identify the data subject accordingly

Task VI: Data Processor

- Identify:
  - Where you get the PD from or whom you are sharing the PD with
  - If you have obtained from or sharing with a third party data:
    - Is there any controller – processing relationship
    - Is there a co-controller relationship
  - If you are using or operating as a Data Processor
  - If that is the case, under which terms is the processing taking place

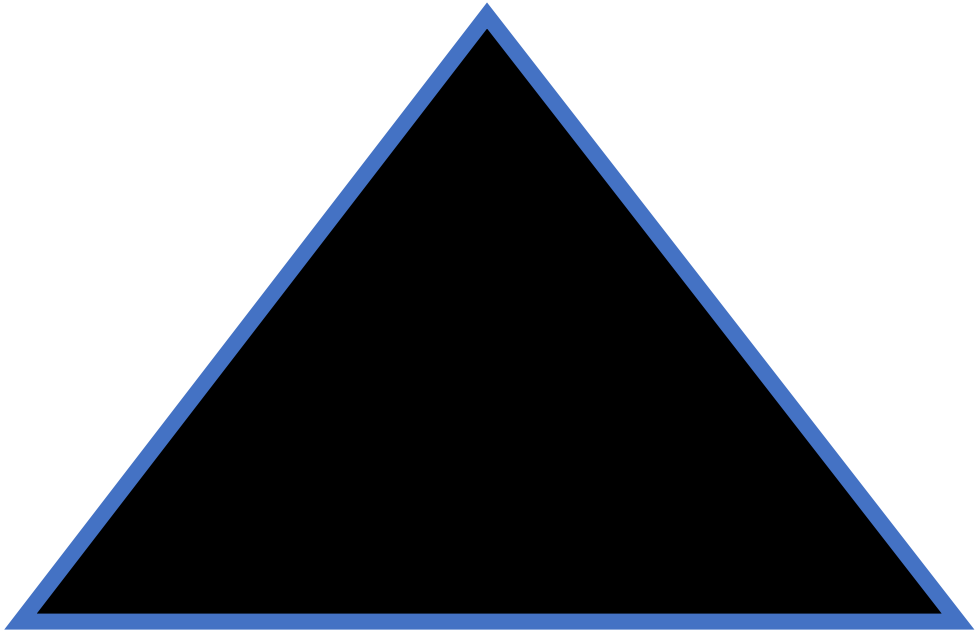
Data Protection Officer



- **<u>Data Protection Officer</u>**
  - 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

Management
(decide)



DPO
(coordinates, controls, advises)

Employees
(execute)

Needs to be a natural person

Data controller's data protection officer (if applicable)	Ana Paula Seixas Morais (paulamorais@lnec.pt)

Tips and hints

- You need to identify a natural person as the DPO
- DPO needs to be registered with the national supervisory authority
- Ensure the DPO is not involved in other activities of the organisation
- DPO may be part of an Ethics Committee as an independent advisor
- Try to use DPO@<domain of institution> instead of personal address to anticipate changes

Purpose of PD processing

- Not strictly defined in the GDPR
- Related to the principles of data protection (art.5(1) GDPR)
- Personal data shall be:
  - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
  - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
  - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

Tips and hints

- Start with the service description and then go to see to what extent the personal data and their respective processing types serve specific purposes to offer the aforementioned service
- Examine each type of data separate by asking the question of why you are collecting, managing and sharing it and to what extend these acts serve the purpose of processing
- The purpose of processing shall persist for all the duration of processing including retention
- If any data processing does not serve the processing purpose, then it should not be processed

Task VII: Purpose

- Identify:
  - Identify the purpose of data processing in accordance to the content of the service, the data collected and the type of processing including retention period and data disclosure

PD processing legal basis (lawfulness)

- Personal Data processing shall be lawful only if and to the extend that is done in accordance to the legal bases that arts. 6 and 9 (for special categories) of the GDPR provide
- The legal basis has to cover the purpose and the type of processing per data type at all times of the data processing life cycle

- Vital Interest

- Public Interest
- Legal Obligation

- Contract
- Consent

- Legitimate Interest

No discretion

discretion

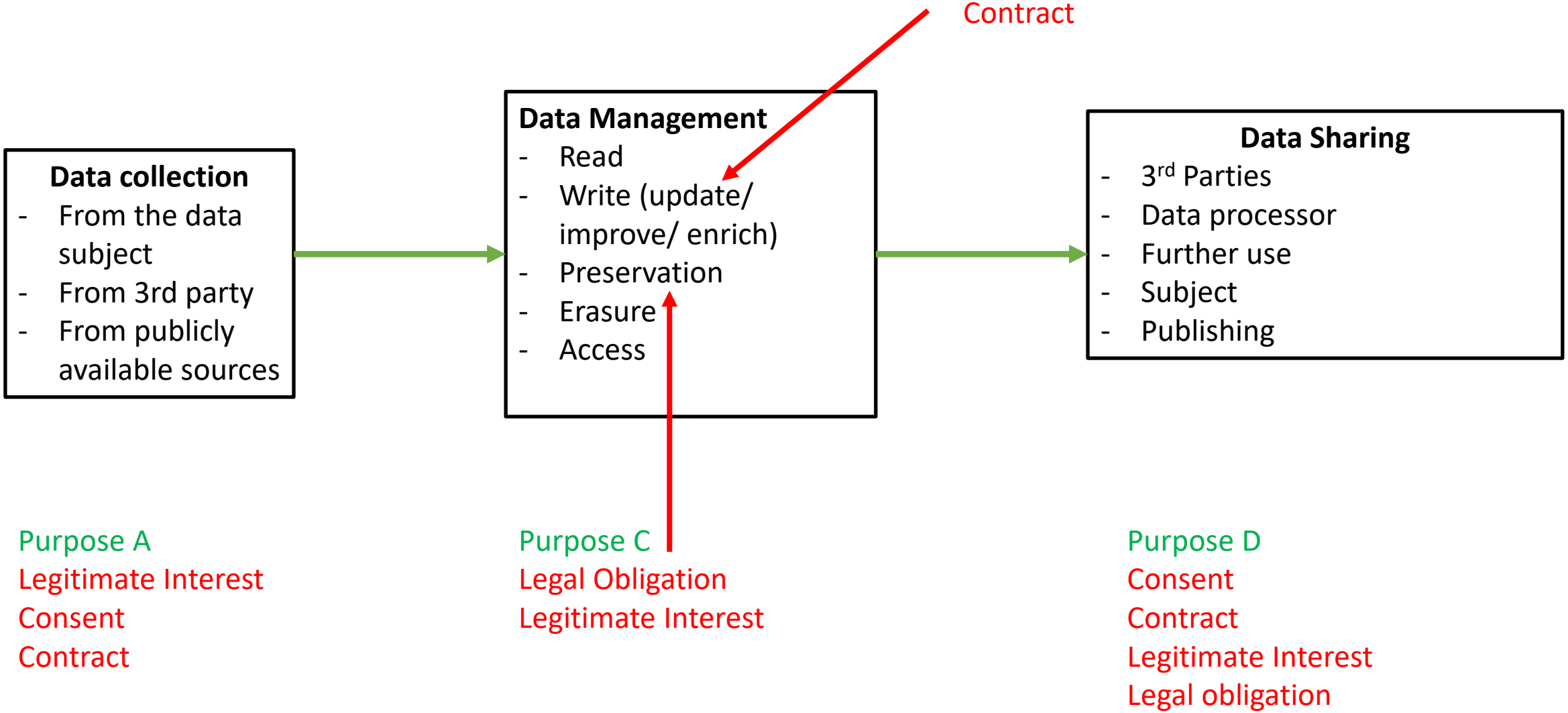
Decision: both parties

Decision: data controller

Trace the life cycle

- ✓Follow the data (use the DMP as your backbone)
- ✓Different types of data processing may have different purposes and legal bases
- ✓Always stay within the legal basis

Data Management Plan (processing/ purposes/ legal basis)



Try not to conflate personal data and legal basis in one category

Personal data processed and the legal basis	*A. Personal data retrieved from your Home organization:* • *Name* • *Username* • *Password* • *Email* • *Affiliation* • *Country* • *UUID - Unique user identifier (SAML persistent identifier) ** *If the registry of the users is done via EGI Check-In, the personal data retrieved in the process is responsibility of EGI.* *B. Personal data gathered from the users* - *Logfiles on the service activity** ** = no personal data is used, only the UUID and the processing outputs are used for management and debugging purposes of the service.*

Tips and hints: what is an appropriate legal basis

- If it is deemed as scientific research, then it is a form of public interest
- It is very likely that some of the data are going to involve further processing, hence, appropriate safeguards have to be put in place
- It could be that consent is obtained for processing types that do not relate to research (e.g. contact information)
- For information that has been obtained through electronic communication and are intended for similar use, legitimate interest may be sufficient
- **If the legal basis is either contract or consent, an approval stage from the data subject is required; in all other cases a notice would suffice**

i – scientific research

How is scientific research defined

Sources:

- Recitals: 26, 33, 50, 52, 53, 62, 65, 113, 156, 157, 159, 160, 161, 162
- Relevant articles: 5(1)(b), (e), 89 (1), (2), (3), 9(j), 14(5)(b), 17(3)(d), 21(6).

Most important article:

- Art. 89

Defining Scientific Research I: **Definitions**

- It falls under the broader **public interest** legal basis (though this is not the only possible legal basis)

- Could be a form of **further processing** (e.g. when obtaining data from a public source or e.g. the government)

- Need to be subjected to **appropriate safeguards**
  - Technical and organizational measures are in place
    - Focus on data minimization (use only necessary data)
    - Means: pseudonymization (without affecting research objectives)

Defining Scientific Research II: **Special Categories**

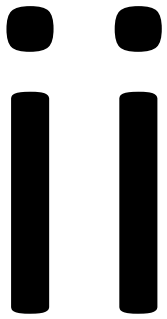
- In relation to special categories of data (art.9), the processing:
    - shall be proportionate to the aim pursued
    - needs to respect the right to data protection
    - needs to provide suitable and specific measures to safeguard the fundamental rights and interests of the data subject

The purpose

- ✓Possible purposes:
  - ✓ Overall: **scientific research** (art. 89 GDPR)
  - ✓ Specific type of research
  - ✓ Further use/ exploitation
- ✓What happens when the purpose changes over time?
  - ✓ **Legal basis**? [e.g. from public task to consent / collection by a public hospital – secondary use by researchers)
  - ✓ Am I **covered** by the legal basis?

Legal Basis

- ✓Mostly forms of **public interest** (needs to be specifically documented per institution and research project)
- ✓**Contract** (tender)
- ✓**Consent** (specific research)
- ✓Could **change** from collection, to retaining to sharing. There always needs to be one covering the purpose of processing.



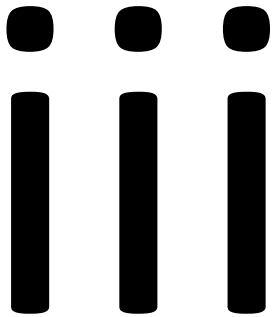
– consent

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

Contract

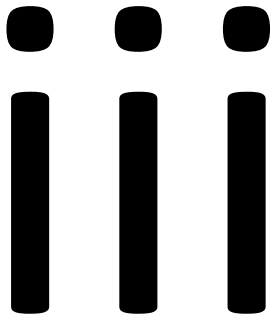
You can rely on this lawful basis if you need to process someone's personal data:

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.



– legitimate interest

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.

iV – special categories data

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 national laws may introduce additional conditions and safeguards.
- You must determine your conditions for processing special category data before you begin this processing under the GDPR, and you should document it.

Task VIII: Legal Basis

- Identify:
  - The legal basis of data processing
  - Ensure that it covers:
    - Data collection
    - Main data processing for the purposes of the service
    - Data sharing
    - Data retention

Data Subject Rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Legal Bases and Data Subject Rights

GDPR individual rights – which rights for which legal basis?

Legal basis	**Subject access**	**Rectification**	**Erasure (1)**	**Restriction**	**Portability (3)**	**Objection (4)**	**Automated decisions**
Consent	√	√	√	√	√		
Contract	√	√		√	√		
Legal obligation	√	√		√			√
Vital interests	√	√		√			√
Public interest task	√	√	(2)	√		√	√
Legitimate interests	√	√	(2)	√		√	√

Notes:

1) Right to erasure applies under all legal bases where personal data are no longer necessary in relation to the purpose for which they were processed or where the processing was unlawful
2) Erasure under these grounds requires the right to objection to be exercised first
3) Portability only applies where the processing is carried out by automated means
4) Right to objection to direct marketing applies to all legal bases

Exercising data subject rights

- ✓Limitation of rights of the data subject (arts. 14(5)/17(3)/ 21(6) GDPR))
- ✓Scientific research/ statistical purposes/ archiving
- ✓Public interest
- ✓Technical and organizational measures (mostly pseudonymization)
- ✓Condition: “it is likely to render impossible or seriously impair the achievement of the objectives of that processing”
- ✓Notices (proactive data subject information)

Limitations to data subject's rights: (I) information

- Information to be provided where personal data have not been obtained from the data subject (art. 14(5)(b)
- Researchers are exempt when:
  - The provision of such information proves impossible or would involve a disproportionate effort
  - Such obligations would render impossible or seriously impair achievement of the objectives of scientific research
  - The controller takes appropriate measures to protect the data subject's legitimate interests

Limitations to data subject's rights: (II) erasure

- Right to erasure ('right to be forgotten') (art. 17(3)(d)
- Researchers are exempt when:
  - Such obligations would render impossible or seriously impair achievement of the objectives of scientific research

Limitations to data subject's rights: (III) objection

- Right to object (art. 21(6)
- Researchers are exempt when:
  - the processing is necessary for the performance of a task carried out for reasons of public interest.

Limitations to data subject's rights: (IV) Member States Derogations

- Member State derogations in relation to data-subject rights:
  - Right of access by the data subject (art.15)
  - Right to rectification (art.16)
  - Right to restriction of processing (art.18)
  - Right to object (art.21)

Tips and hints

- Data Subject rights are contingent upon the legal basis of processing
- If the legal basis of processing is public task (research) then there are serious limitations with respect to the data subject rights
- Refer to the table of data subject rights vis-à-vis legal basis in order to identify the rights of the data subject to be communicated
- The data subject needs to always have access to a list of her rights as well as a ways in which these may be satisfied:
  - This means *de minimis* an email address (or even better a form) by which the rights may be exercised
  - In addition, a dash-board where the data subject may directly have access to her data could improve the exercising of such rights

Task IX: Data subject rights

- Identify:
  - The rights of the data subject in accordance to the legal basis of processing
  - For each right identify ways in which it may be exercised

Personal Data Transfers to third countries

- It involves the transferring of data to non-EU countries
- Items:
  - Conditions (contract or legal act) art.28
  - Notifications and notices (data subject rights information – access) (arts.13(1)(f), 14(1)(f), 15(1), (2))
  - Keep records (art.30)
  - Use of Codes of Conduct (art.40)
  - Explore certification schemes, seals and marks (art.42(2))
  - See entire Chapter V (arts.44-50)
    - Adequacy decision
    - Appropriate Safeguards
    - Binding corporate rules
    - Authorization by Union Law

- See EC Standard Contractual Clauses (SCC)
  - Standard contractual clauses for data transfers between EU and non-EU countries.

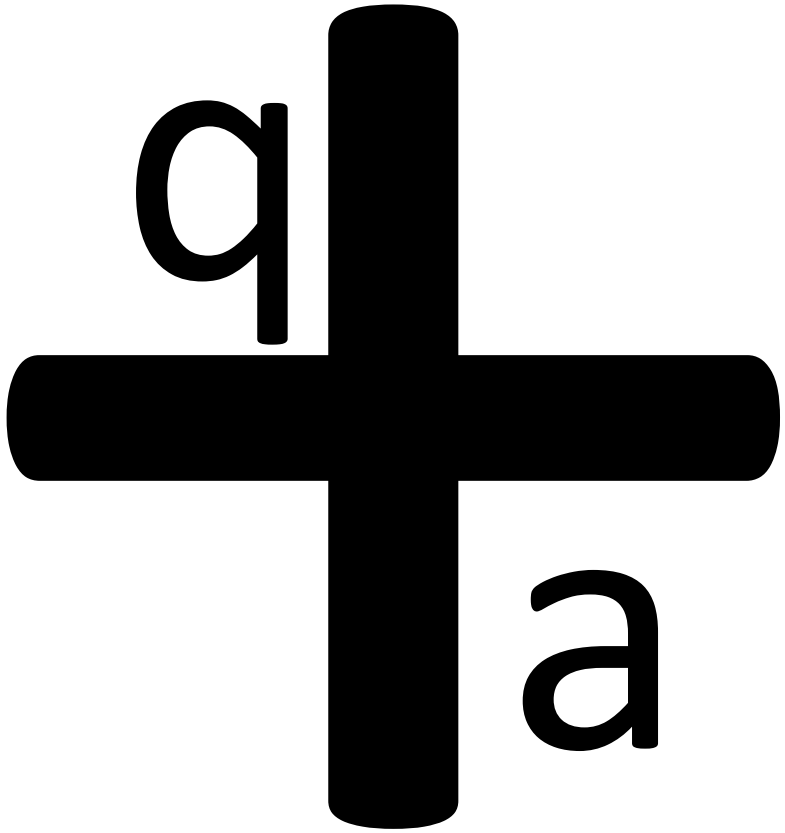
5

Summary of a PD policy

Component	Description
Service Definition	
Personal Data Types	
Processing Types	
Data Controller	
Contact Details	
Data Processor	
DPO	
Purpose of processing	
Legal Basis (per purpose of processing) [if consent provide link to consent document]	
Data Subject Rights and ways of exercising them	
Sharing of data with third parties	
Sharing of data outside the EU (3rd Countries)	
Retention Period	
Deletion Process	
Pseudonymisation	
Anonymisation	
Applicable Code of Conduct	

Task X: Policy Drafting

- Complete the table of previous slide



ptsiavos@athenarc.gr
prodromos.tsiavos@openaire.eu

@prodromos