

Appendix

Data Dictionary

Class: Actor	
Represents the different kinds of stakeholders of the application. Can be a natural or legal person.	
Attribute	Description
actorId	Actor's unique identifier.

Class: MainActor	
Corresponds to entities playing central roles in the privacy management process (<i>e.g.</i> , controller, data subject).	

Class: SecondaryActor	
Represents the natural /legal person entitled to obtain communication of collected / produced data. Can be a third-party or data processor.	
Attribute	Description
name	Name of the entity / secondary actor.
address	Physical address associated with the secondary actor.
phone	Telephone number associated with the secondary actor.
email	Email address associated with the secondary actor.
safeguard	All measures or commitments taken by an organization or data processor to ensure that personal data processing complies with legal protection standards. Measures / commitments for legal compliance.
safeguardType	Type of safeguard (Adequacy decision, Contractual clause, Derogation, BCR)

Class: ApplicationOwner	
Refers to the data controller in GDPR, who is responsible for ensuring compliance in personal data processing and for determining its purposes.	
Attribute	Description
aoName	Name of the application owner.
aoAddress	Physical address of the application owner.
aoPhone	Telephone number of the application owner.
aoEmail	Email address of the owner.

Class: DataSubject	
Person whose personal data is collected, processed, transmitted or stored.	
Attribute	Description
age	Age of the concerned person.
referenceId	Unique identifier linking to PRIAM database.

Class: DPO	
The Data Protection Officer, responsible for enforcing personal data regulations within an organization, acts as the interface for GDPR compliance.	
Attribute	Description
dpoName	Name of the DPO.
dpoAddress	Physical address of the DPO.
dpoPhone	Telephone number of the DPO.
dpoEmail	Email address of the DPO.

reason	Reason for not appointing a DPO.
--------	----------------------------------

Class: ThirdParty
Entity other than data subject, controller, or data processor authorized to process personal data.

Class: Country	
Country information for actors (data subjects, owners, DPOs, etc.).	
Attribute	Description
countryId	Unique country identifier.
name	Country name.
minorAge	Age of majority in the country.
adequate	GDPR-equivalence indicator for data protection.

Class: Data	
Holds the description of a kind of collected and stored data.	
Attribute	Description
dataId	Unique data identifier.
dataName	Attribute name (of a data item).
source	Origin or provenance of personal data. It can take one of three values: Indirect (the data subject is not the source of his/her data), Direct (data subject is the source of his/her data), and Produced (automatically generated data via a decision-making system, inference, etc.).
sourceDetails	Detailed information concerning the origin of data when this is an indirect source.
dataConservation	Retention period, the length of time for which personal data is stored.
isPersonal	An indicator specifying whether the data in question is considered personal, i.e., linked to an identifiable person.
isPortable	An indicator specifying whether personal data is portable.

Class: PersonalDataCategory	
Category of personal data.	
Attribute	Description
pdcId	Unique identifier of a personal data category.
pdcName	Name of a category of personal data (health, identification, profile, sensitive, etc.).

Class: DataType	
Defines the content of the data as a classifier (set of attributes associated with primitive types).	
Attribute	Description
dataTypeId	Unique identifier of a data type.
dataTypeName	Name of the data type referring to the name of a class or table in a database.

Class: Processing	
Any operation or set of operations which is performed on (personal) data.	
Attribute	Description
processingId	Unique identifier for a processing operation.
processingName	Processing name/title.

pt	Processing type can take 4 values. <i>Default processings do not require the consent of data subjects. Necessary processings are the basic functionalities of an application. The consent of the data subject must be granted in order to use the application. Mandatory processings are lawful processings that are not contractual ones or those requiring consent. Optional Processings do not mitigate the basic operation of the application when consent is refused or withdrawn by users).</i>
pc	Processing category refers to the legal basis in GDPR (Consent/Contract, Vital Interests, Legitimate Interests, Legal Obligations, Public Interests).
createdAt	Processing creation date.
modifiedAt	Processing modification date.
endedAt	Processing end date.
consequence	Describes the specific impacts of not providing the data required for a given processing operation.

Class: DataUsage	
Links processings to the data they use to assess their status regarding privacy management.	
Attribute	Description
dataUsageId	Unique identifier of a data usage.
hasPersonalStatus	Status of personal data (personal or not) in a specific processing.
c / r / u / d	Operation (create, read, update, delete) that a processing can perform on data.

Class: PersonalDataTransfer	
Transfer personal data, keeps track of any data transfer. It allows knowing to whom the data has been transferred and for what purpose.	
Attribute	Description
transferId	Unique identifier of a transfer.

Class: Purpose	
Objective of the processing in the application (e.g., profiling, automated decision making, marketing, statistics, research).	
Attribute	Description
purposeId	Unique identifier of a purpose.
description	Description of purpose.
type	Type of purpose (primary or secondary).

Class: Measure	
Action taken to protect personal data and processing against threats, risks, or breaches.	
Attribute	Description
measureId	Unique identifier for a measure.
description	Measure description.
Mtype	Measure type (organizational, technical).
Mcategory	Measure category (encryption, anonymization).

Class: ProcessingLink	
Links two processings together. For now, we distinguish two types of links: Similarity when processings have similar purposes and Inclusion when one processing includes the other. In both cases, a single consent is sufficient.	
Attribute	Description

typeOfLink	Type of link (Similarity, Inclusion).
------------	---------------------------------------

Class: Contract	
An agreement between the data subject and the controller. It represents a set of consents.	
Attribute	Description
contractId	Unique identifier of a contract.
signatureDate	Contract signature date (start date).
expirationDate	Contract expiry date (contract termination date).

Class: Consent	
Represents the explicit consent given by a data subject to the processing of his / her personal data.	
Attribute	Description
consentId	Unique consent identifier.
startDate	Consent start date.
endDate	Consent end date.

Class: Request	
A formal request sent by the data subject to exercise one of his or her rights.	
Attribute	Description
requestId	Unique request identifier.
claim	Request justification.
issuedAt	Request issue date.

Class: DataRequest	
A “data request” refers to a request made by a data subject that concerns a specific piece of data or several specific pieces of data about him/her (concerns individual data). It may be a request for rectification, deletion, access, or portability.	
Attribute	Description
newValue	In the case of a rectification request, this attribute represents the new value of the data to be modified.
type	Type of data request (rectification, deletion, access).
isIsolated	In the case of a rectification request, the data concerned is isolated until a response is issued.

Class: ProcessingRequest	
A “processing request” refers to a request concerning the entire processing of personal data, not just specific data. It concerns data processing as such, not just specific data. It may be a request for objection, limitation, and information.	
Attribute	Description
type	Type of processing request (Objection, Knowledge, Restriction).

Class: Answer	
The response provided by the controller in response to a request from the data subject to exercise a right.	
Attribute	Description
answerId	Unique response identifier.
answer	Yes or no answer to a request.
issuedAt	Date of response.
claim	Justification for response.

Class: Breach	
A breach in data security, leading to unauthorized access or disclosure of personal data.	
Attribute	Description
breachId	Unique identifier of a breach.
nature	Nature of the personal data breach.
riskLevel	Level of risk generated by the breach (None, Medium, High).
createdAt	Date of creation of the breach.
sprvAuthNonNotifReasons	Reasons why supervisory authority has not been notified of a breach.
dataSubjNonNotifReasons	Reasons why the data subject has not been notified of a breach.

Class: Consequence	
The impact or effect resulting from an incident, such as a personal data breach.	
Attribute	Description
impactId	Unique identifier of a consequence.
description	Consequence description.

Class: Document	
A file containing relevant information about the processing of personal data.	
Attribute	Description
docId	Unique document identifier.
content	Content of the document. It can be in the form of a PDF file, text file, etc.
createdAt	Document creation date.

Class: RecordProcessingA	
A document listing the processing of personal data and its details (data processed, its category, purposes, security measures, etc.).	

Class: RecordBreach	
A document detailing a personal data breach, including the data breached and the data subjects affected.	

Class: DPIA	
Data Protection Impact Assessment (DPIA) is a process used to evaluate and mitigate privacy risks when processing personal data. It helps organizations assess the impact of data processing activities on individuals' privacy, especially when such processing may pose high risks, and ensures compliance with data protection laws like GDPR.	
Attribute	Description
toolUrl	URL of the tool used to perform the impact analysis.