[organization logo]

[organization name]

**POLICY FOR DATA PRIVACY IN THE CLOUD**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Abdullah | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc454535771)

[2. Reference documents 3](#_Toc454535772)

[3. Basic PII terminology 3](#_Toc454535773)

[4. Protection of Personally Identifiable Information in Cloud Environments 3](#_Toc454535774)

[4.1. Information collection, use, sharing and disclosure 4](#_Toc454535775)

[4.1.1. Information collection 4](#_Toc454535776)

[4.1.2. Information use and sharing 4](#_Toc454535777)

[4.1.3. Information disclosure 4](#_Toc454535778)

[4.2. PII principal’s access to and control over information 5](#_Toc454535779)

[4.3. Information location, storage, transfer and access 5](#_Toc454535780)

[4.3.1. Information location 5](#_Toc454535781)

[4.3.2. Information storage 5](#_Toc454535782)

[4.3.3. Information transfer over public networks 5](#_Toc454535783)

[4.3.4. Information access 5](#_Toc454535784)

[4.4. Information retention and disposal 6](#_Toc454535785)

[4.5. Logging, monitoring and compliance verification 6](#_Toc454535786)

[5. Managing records kept on the basis of this document 6](#_Toc454535787)

[6. Validity and document management 7](#_Toc454535788)

# Purpose, scope and users

The purpose of this document is to define rules to ensure that Personally Identifiable Information (PII), and user data privacy, are protected at an appropriate level in cloud environments.

This document is applied to public cloud services provided by [organization name], as well as to all public cloud service providers who process PII under responsibility of [organization name].

Users of this document are top management and persons responsible for public cloud service providers in [organization name].

# Reference documents

* ISO/IEC 27001 standard, clauses A.5.1.1, A.7.1.2, A.12.4.1, A.12.4.2, A.14.3.1, A.16.1.2 and A.18.1.4
* ISO/IEC 27017 standard, clauses 5.1.1, 12.4.1 and 16.1.2
* ISO/IEC 27018 standard, clauses 5.1.1, 11.2.7, 12.4.1, 12.4.2, 12.4.3, 16.1.2, A.1.1, A.2.1, A.2.2, A.5.1, A.5.2, A.7.1, A.9.1, A.9.2, A.10.1 and A.10.2
* Information Security Policy
* Statement of Applicability
* List of Legal, Regulatory and Contractual and Other Obligations
* Incident Management Procedure
* [Operating Procedures for Information and Communication Technology] / [Disposal and Destruction Policy]

# Basic PII terminology

**Personally Identifiable Information (PII)** – any information that, by means of use or correlation with other information, can be used to uniquely identify a person.

**PII principal** – the person to whom the PII refers.

**PII controller** – a person or organization that can decide for which purposes a person’s PII that is under his responsibility can be processed or by which means.

**PII processor** – a person or organization that processes PII on behalf of a PII controller, or the PII principal, and in accordance with his instructions.

**Public cloud service provider** – party which makes cloud services available according to the public cloud model.

# Protection of Personally Identifiable Information in Cloud Environments

The [job title] is responsible to coordinate all activities necessary to ensure the proper application of this policy.

## Information collection, use, sharing and disclosure

### Information collection

In order to perform business activities and/or fulfill contractual demands in cloud environments, [job title] must ensure that the public cloud service providers, owned or outsourced by [organization name], may only collect the following types of Personally Identifiable Information:

* [list here the PII that may be collected].

### Information use and sharing

[Job title] must ensure that Personally Identifiable Information processed by public cloud service providers, owned or outsourced by [organization name], will be used only for the following purposes:

* Purposes defined in the contract with the public cloud service customer
* Technical purposes required to fulfill the customer’s contract
* [list here other situations that PII may be used for]

[Organization name] will share PII submitted to it with the following third parties, only to the extent necessary to perform business activities and/or fulfill contractual demands:

* [list here the third parties that will have access to PII and for what purpose]

[Organization name] will not supply PII submitted to it to any third party for direct marketing or advertisement purposes, unless with the expressed consent of PII principal / PII controller.

### Information disclosure

Disclosure of PII may be done as reasonably necessary for the purposes stated in clause 4.1.1 of this policy to the following entities:

* [Organization name]’s employees, suppliers, or subcontractors
* members of [Organization name]’s group of companies;
* [list here other entities to which PII may be disclosed]

Disclose of any personal information held by [organization name] to entities not listed above only can be made after the [job title] obtains consent from the information owner for the disclosure, or upon legally binding request made by law enforcement authority, if such legal request does not prohibit the notification disclosure. The notification will be performed as defined in the contract.

In cases where the PII disclosure was caused by an incident, the notification to the PII principal and PII controller will be reported as soon as possible, by phone or in person.

Any PII disclosure must be recorded by [job title] in the [registry of PII disclosure]. This document must include what PII has been disclosed, by whom, to whom, and at what time. In cases where the disclosure is demanded by law, the legal reference that is used to authorize the disclosure must also be included in the record.

## PII principal’s access to and control over information

[Job title] must ensure that [organization name]’s public cloud processors, owned or outsourced, offer the following capabilities for PII principals and/or PII controllers to access and control their PII in a timely fashion:

* Unique identification and authentication credentials to access PII relevant to them
* Privacy settings to enable them to control the publication of their information
* Editing functionalities to enable them to include, correct, update, and exclude information

The specificities of implementation alternatives are described as the contract’s requirements.

Concerning privacy and editing capabilities, the public cloud processors must provide warnings to PII principal and/or PII controller about possible impacts that may occur to product or service performance by using these capabilities.

## Information location, storage, transfer and access

### Information location

The PII submitted to [organization name] may be stored in the following locations:

* [list here the countries where PII may be stored, including those related to subcontractors and third parties listed in clause 4.1.3 of this policy].

[job title] is responsible to ensure that this location’s information is part of the contract terms presented to the public cloud service customer.

### Information storage

To ensure the protection of PII submitted to [organization name], all assets used to store PII must make use of encryption solutions. In situations where such solutions are unavailable, the use of an unencrypted asset must be authorized by [job title] and documented.

[job title] is responsible to ensure that the use of hard copy material containing PII, e.g., printed reports, must be restricted.

### Information transfer over public networks

[job title] is responsible to ensure that the transfer of PII submitted to [organization name] when done through public data-transmission networks must ensure the PII is encrypted prior to transmission.

### Information access

[organization name]’s employees only will have access to PII reasonably necessary for performance of activities related to the purposes stated in clause 4.1.2 of this policy. The owner of each business process that is related to the purposes stated in clause 4.1.2 of this policy is responsible to define which PII may be accessed by their employees.

Subcontractors’ access to PII only can be granted after acceptance of the public cloud service customer, which must be informed by the [job title] the countries in which the subcontractor may process PII data and the means by which the subcontractor is obliged to be compliant with the public cloud service customer and PII processor.

[job title] is responsible to ensure that all individuals under [organization name] with access to PII must sign a non-disclosure agreement before being granted access to PII data.

## Information retention and disposal

[job title] is responsible to ensure that all PII is retained only for the time defined as needed for the achievement of its intended purpose.

Regarding information systems acquisition, development, and maintenance, requirements shall be established to ensure that temporary files and documents created in the normal course of operation are deleted as soon as those files and documents are not needed anymore. [job title] is responsible to review information systems’ requirements to ensure these requirements are included.

All the methods for secure erasure and destruction of PII is prescribed in the document [Operating Procedures for Information and Communication Technology] / [Disposal and Destruction Policy].

## Logging, monitoring and compliance verification

[job title] is responsible to ensure that logs are kept, monitored, and reviewed on PII data to ensure means to verify whether or not it has been changed, to identify unusual behavior over PII handling, and to provide appropriate corrective actions if errors are identified. [job title] must be informed about the results of the review.

[Job title] shall ensure that the business unit acting as public cloud processor, or subcontractor performing this activity on behalf of the organization, provides the cloud service customer with all relevant information, in a timely manner, so the cloud service customer can have means to verify if the operation is compliant with all requirements defined in this policy.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [Registry of PII Disclosure] | [job title]'s computer | [job title] | Only [job title] is authorized to edit data | 3 years for registries in which service contract has already been terminated |

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* number of incidents related to unauthorized access to PII

Previous versions of this policy must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]