[Organization logo]

[Organization name]

POLICY FOR DATA PRIVACY IN THE CLOUD

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

Commented [27A1]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [27A2]: To learn more about privacy in the cloud, read this article:

ISO 27001 vs. ISO 27018 – Standard for protecting privacy in the cloud http://advisera.com/27001academy/blog/2015/11/16/iso-27001-vs-iso-27018-standard-for-protecting-privacy-in-the-cloud/

Commented [27A3]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. 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].

Commented [27A4]: Subcontractors that process Personally Identifiable Information on behalf of the organization should follow this policy or similar document.

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

2. 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
- [Security Procedures for IT Department] / [Disposal and Destruction Policy]

Commented [27A5]: Delete these references if the organization does not provide cloud services.

Commented [27A6]: Delete this reference if the organization does not act as a Personally Identifiable Information (PII) cloud processor.

Commented [27A7]: If you don't have this List, then in these bullets list all the legislation and contractual obligations related to classification of information.

Commented [27A8]: Select the document that prescribes secure erasure of data.

3. Basic PII terminology

Personally Identifiable Information (PII) – any information that, by means of use or correlation with [illegible]

[illegible]

[illegible] under his responsibility can be processed or by which means.

Commented [27A9]: e.g.: a merchant that holds customer data and sends them to a bank for credit analysis acts as a PII controller.

[illegible]

Commented [27A10]: Any organization processing credit card [illegible]

[illegible] cloud model.

4. Protection of Personally Identifiable Information in Cloud Environments

[illegible]

4.1. Information collection, use, sharing and disclosure

4.1.1. Information collection

In order to perform business activities and/or fulfill contractual demands in cloud environments, [job [illegible]

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

4.1.2. Information use and sharing

[illegible]

- Purposes defined in the contract with the public cloud service customer
- [illegible]
- [illegible]

[Organization name] will share PII submitted to it with the following third parties, only to the extent [illegible]

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

[illegible]

4.1.3. Information disclosure

[illegible] policy to the following entities:

- [illegible]
- [illegible]
- [illegible]

Disclose of any personal information held by [organization name] to entities not listed above only can [illegible] the notification disclosure. The notification will be performed as defined in the contract.

[illegible]

[illegible] must include what PII has been disclosed, by whom, to whom, and at what time. In cases where the

Commented [27A11]: E.g.: Chief Privacy Officer (CPO), Chief Information Officer (CIO), Head of Human Resources department, Customer Relationship Manager, etc.

Commented [27A12]: As part of its cloud operations, an [illegible]

Commented [27A13]: E.g.: profile information (name, e-mail, pictures, etc.), access and purchase behaviour, etc.

Commented [27A14]: E.g.: processing resource allocation

Commented [27A15]: E.g.: administration of the business, [illegible]

Commented [27A16]: E.g.: payment service provider, for [illegible]

Commented [27A17]: This consent should not be defined as a condition to supply the service.

Commented [27A18]: You can delete this bullet if your organization is not a member of a larger group of companies.

Commented [27A19]: Other incident reporting systems may be added that are in use (e.g. help desk applications, etc.).

Commented [27A20]: Situations where a disclosure may happen are:

[illegible]

Commented [27A21]: This document should be named according to organization's existing documentation.

Commented [27A22]: Fill in here the name of the exiting document in your organization.

[illegible]

4.2. PII principal’s access to and control over information

[Job title] must ensure that [organization name]’s public cloud processors, owned or outsourced, [illegible]

- Unique identification and authentication credentials to access PII relevant to them
- [illegible]
- [illegible]

Commented [27A23]: E.g.: password, token, biometrics, or a combination of those.

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

[illegible] performance by using these capabilities.

Commented [27A24]: Limiting information publication may [illegible]

4.3. Information location, storage, transfer and access

4.3.1. Information location

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

- [illegible]

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

4.3.2. Information storage

To ensure the protection of PII submitted to [organization name], all assets used to store PII must [illegible]

[illegible] reports, must be restricted.

4.3.3. Information transfer over public networks

[Job title] is responsible to ensure that the transfer of PII submitted to [organization name] when [illegible]

4.3.4. Information access

[illegible] 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 [illegible]

[illegible] process PII data and the means by which the subcontractor is obliged to be compliant with the public cloud service customer and PII processor.

[illegible]

4.4. Information retention and disposal

[Job title] is responsible to ensure that all PII is retained only for the time defined as needed for the [illegible]

Commented [27A25]: This information generally can be found in the related process documentation.

[illegible] to review information systems' requirements to ensure these requirements are included.

[illegible]

Commented [27A26]: Select the document that prescribes secure erasure of data.

4.5. Logging, monitoring and compliance verification

Commented [27A27]: If you included this section in the "Cloud Environment Management Policy" you can delete this section here.

[illegible] about the results of the review.

Commented [27A28]: Logs may include user activities, [illegible]

[Job title] shall ensure that the business unit acting as public cloud processor, or subcontractor [illegible]

5. 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

Commented [27A29]: Please alter this record to match what you already have in your company. If you do not have a similar record, you can create a new one in the format that suits you best.

				terminated

6. 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.

Commented [27A30]: This is only a recommendation; adjust frequency as appropriate.

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

- [illegible]

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

Commented [27A31]: Delete this whole section if your organization does not provide cloud services as a PII processor.

[job title]
[name]

____
[signature]

Commented [27A32]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.