

As Processor

Data Privacy Policy


Project Reference: internal policy

Version: 1.1

Date: 2023.12.24



Campus Contern
17, rue Edmond Reuter
L-5326 Contern

 (+352) 266 793 1

anidris.lu

CONTACTS

ANIDRIS

NAME	PHONE	EMAIL	TITLE
Giovanni CUOCO	+352 621 153 817	cuoco@anidris.lu	Managing Director CEO
Jean-Francois LEMADEC	+352 661 267 490	lemadec@anidris.lu	COO
Didier ANNET	+352 621 269 927	annet@anidris.lu	DPO

Table 1 : ANIDRIS contacts

DOCUMENT VERSION CONTROL

VERSION	DATE	CHANGE(S)	Author
0.1	2023.11.03	First draft	DAN
0.9	2023.12.24	Final version, ready to be approved	DAN
1.0	2024.02.15	Reviewed by COO	JFLM
1.1	2024.03.15	Integrate change	DAN

Table 2 : Document version control

TABLE OF CONTENTS

- 1 Data Privacy Policy 4
 - 1.1 Introduction 4
 - 1.2 Scope & Purpose 4
 - 1.3 Ownership and review 4
 - 1.4 References 4
 - 1.5 Identity and contact details 5
 - 1.6 Management statement 6
 - 1.7 Purpose of the processing as a processor 7
 - 1.7.1 Service provision 7
 - 1.7.2 Categories of Personal Data/Data Subject 7
 - 1.7.3 Categories of recipients 7
 - 1.8 Retention period and data subject rights 8
 - 1.9 Security mechanisms 8
 - 1.9.1 Information Security Policy 9
 - 1.9.2 Asset Management 9
 - 1.9.3 Human Resources Security 9
 - 1.9.4 Access Management 9
 - 1.9.5 Operational Security 10
 - 1.10 Data breach notification 10
- 2 Appendixes 12
 - 2.1 Appendix 1 -Retention Policies 12
 - 2.2 Appendix 2 -Definitions 12



1 Data Privacy Policy

1.1 Introduction

The digital transformation and the customer communication management being the core business of Anidris, Anidris processes Personal Data of others entities within the context of service delivery agreed by a contractual agreement as Processor.

In accordance with the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") and the applicable national law, Anidris is committed to respect Personal Data entrusted by its customers for the performance of its services.

1.2 Scope & Purpose

The scope of this Data Privacy Policy covers Anidris and all Personal Data processed by Anidris as a Data Processor.

This data privacy policy ("Data Privacy Policy") provides the required information how Anidris intends to process Personal Data as part of the services provided.

1.3 Ownership and review

The owner of this policy is the Management and the DPO function. The review of this policy shall be triennial unless if required earlier.

1.4 References

The following files or documents are linked to the present procedure:

Document Title	Location
Records of processing	DPO's files
Legal Disclaimer	Anidris' website

1.5 Identity and contact details

Controller	Anidris S.A.
Short name	Anidris
Direction	Giovanni Cuoco (CEO)
Email	cuoco@anidris.lu
Web page	www.anidris.lu
Data Protection Officer (DPO)	Didier Annet
Phone	+352 266 793 1
Email	privacy@anidris.lu

1.6 Management statement

The General Data Protection Regulation (“GDPR”) entered into force on the 25th May 2018 repealing the former applicable European Directive 95/46/CE. The law of the 1st August 2018 completes the GDPR in the Grand-Duchy of Luxembourg.

The GDPR has reinforced data subjects’ rights and increased responsibility and accountability obligations of organizations.

Capitalized Terms included in this policy shall have the meaning assigned to them in Appendix B.

In this policy, we intend to define all information regarding how we process Personal Data in accordance with laws, regulations and contractual agreements including Controller’s instructions.

ANIDRIS is fully committed to the implementation of a strong framework for managing and protecting Personal Data. Hence, ANIDRIS has appointed a Data Protection Officer for coordinating, supporting and advising on each topic related to Personal Data management.

ANIDRIS undertakes to process Personal Data in accordance with the applicable laws and regulations and, especially, to implement appropriate technical measures aiming at protecting Personal Data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing.

ANIDRIS ensures that its employees or third-parties authorized to access Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Awareness-raising and training sessions are regularly provided to employees.

ANIDRIS agrees to process Personal Data lawfully in accordance with the lawful documented instructions of its clients, the latter acting as Controller. Hence, taking into account the nature of the process, ANIDRIS will reasonably assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of this latter’s obligation to respond to requests for exercising data subject’s rights.

ANIDRIS Management has approved this policy and understands the importance of managing Personal Data based on a risk approach and to ensure that rights and freedoms of data subjects are protected.

Note: ANIDRIS reserves the rights to modify this Data Privacy Policy at any time, which updated version will be available on ANIDRIS’ website or on demand.

1.7 Purpose of the processing as a processor

1.7.1 Service provision

Personal Data of data subjects will be processed as part of the performance of ANIDRIS services pursuant to the execution of a contract or any other type of agreement.

Clients are responsible for determining and knowing what data and what type of data are transferred into ANIDRIS' environments for processing. ANIDRIS is then responsible to take reasonable and appropriate organizational and technical measures to protect data as well as processing data according to documented instructions of clients.

The following services are provided by ANIDRIS and may include Personal Data processing:

- Customer communication services
- Content services
- Document outsourcing services

(hereinafter "Services")

To the extent that Personal Data are processed in the performance of Services, the processing shall be governed by a contract, usually in the form of a Data Protection Agreement, that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects and the obligations and rights of the Controller and the Processor.

1.7.2 Categories of Personal Data/Data Subject

For the performance of Services, ANIDRIS collects data from its clients that may include Personal Data of data subjects.

When providing Personal Data to ANIDRIS, clients must ensure that Personal Data have been collected from data subjects in full compliance with the applicable Data protection legislation.

In any circumstances, ANIDRIS will process all data, regardless of the fact that data actually include or not Personal Data, with the same high level of security in accordance with the client's documented instructions. In the case where client does not instruct ANIDRIS, ANIDRIS will implement its standard processes and measures.

1.7.3 Categories of recipients

Personal data processed by ANIDRIS as a Processor will only be disclosed to third parties as defined in documented instructions from the client, or when required by law. ANIDRIS reserves its rights to suspend or cease a processing of Personal Data if ANIDRIS becomes aware that such processing may not be compliant with Data protection legislation.

1.8 Retention period and data subject rights

ANIDRIS processes Personal Data for the execution of its Services based on contractual obligations. Retention instructions for each data processing shall be defined by the client and communicated to ANIDRIS, otherwise retention periods will be based on ANIDRIS standard retention policy as set out in Appendix A.

These retention policies shall be defined according to business and operational needs for the delivery of the service and shall not replace legal, regulatory, contractual or other business requirements of the client to store and/or archive Personal Data.

Personal Data retained for that purpose are only stored for traceability, queries/retrieval request from client and investigation needs and cannot be modified in order to ensure their integrity for the purpose of investigation needs. As such, these Personal Data are not subject to the right of rectification.

In any case, deviation with the ANIDRIS standard retention policy would involve additional costs for the client.

1.9 Security mechanisms

In order to protect all Personal Data processed and mitigate the risks for the rights and freedom of the data subjects which may result in the processing of their Personal Data, ANIDRIS will apply security measures (classified in legal, organizational and technical measures) to ensure integrity, confidentiality and availability of Personal Data and to ensure the rights of the data subjects.

In addition to complying with client's documented instructions, if any, ANIDRIS has defined security measures to protect data received from clients as part of the data processing related to the service.

1.9.1 Information Security Policy

ANIDRIS has defined an information security policies. This policy describe ANIDRIS requirements and needs regarding protection of assets and information, compliance with applicable laws and regulations as well as contractual obligations.

1.9.2 Asset Management

ANIDRIS has defined a process for classifying and managing all assets (informational and tangible assets) depending on the classification level.

ANIDRIS measures include, but are not limited to:

- Classification of information is defined with different levels depending on information security criteria.
- Inventory of assets is kept up-to-date.

1.9.3 Human Resources Security

Human resources processes take into account information security requirements for each activity, such as employees onboarding, change of position, employees departure, terms and conditions of employment, confidentiality agreements, awareness, training and employees evaluation.

ANIDRIS measures include, but are not limited to:

- A defined list of tasks for new joiners for ensuring that they are competent for the role(s) (background checks) and that they are informed and understood their responsibilities;
- A defined list of tasks for leavers for ensuring that all assets have been got back;
- Formal employees contract that includes confidentiality requirements and adherence to information security processes;
- Information security awareness program is in place and keeps employees aware of their role and responsibilities in relation with information security. In addition, specific awareness and training are provided to employees regarding privacy and data protection;
- Jobs description include information security responsibilities.

1.9.4 Access Management

Access to information and assets is based on data classification and on roles and responsibilities following a need to know basis.

ANIDRIS measures include, but are not limited to:

- Access are assigned depending on roles that are allocated based on employees' function and on a "need-to-know" principle.
- Specific access rights are subject to approval.
- Privileged access rights are restricted and controlled allocated following segregation of duties principle, and limited to what is strictly necessary.
- Access rights review are performed at regular intervals.
- Strong password management practices are in place for protecting and managing passwords.

1.9.5 Operational Security

Operational security is defined at different levels to ensure that confidentiality, integrity and availability of information are ensured depending on business needs.

ANIDRIS measures include, but are not limited to:

- Each laptop, workstation and server is equipped by an anti-virus managed centrally and updated.
- Laptop hard drives are encrypted.
- Use of resources is monitored and tuned depending on capacity requirements to ensure the required system performance and detection of unavailability. Backup copies of information, software and system are done and texted regularly based on a defined backup policy.

1.10 Data breach notification

A Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data (“Personal Data Breach”). This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing Personal Data.

A Personal Data Breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of Personal Data. In short, there will be a Personal Data Breach whenever any Personal Data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorization; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

When a Personal Data Breach has been identified and proven in the execution of Services, ANIDRIS will notify the client without undue delay and assist the client for any related question. Conversely, ANIDRIS expects the Controller, when detecting any Personal Data Breach or security incident potentially impacting Services and/or data subject’ rights, to notify ANIDRIS without undue delay. It shall be noted that, most of the time, Personal Data breach will be identified by the client or data subject and not by ANIDRIS. Furthermore, at this step of the process, there is no analysis of who is responsible of the incident.

Diagram in Figure 1 - Data Personal Breach notification process (page 11) summarizes this.

Personal Data Breach Notification

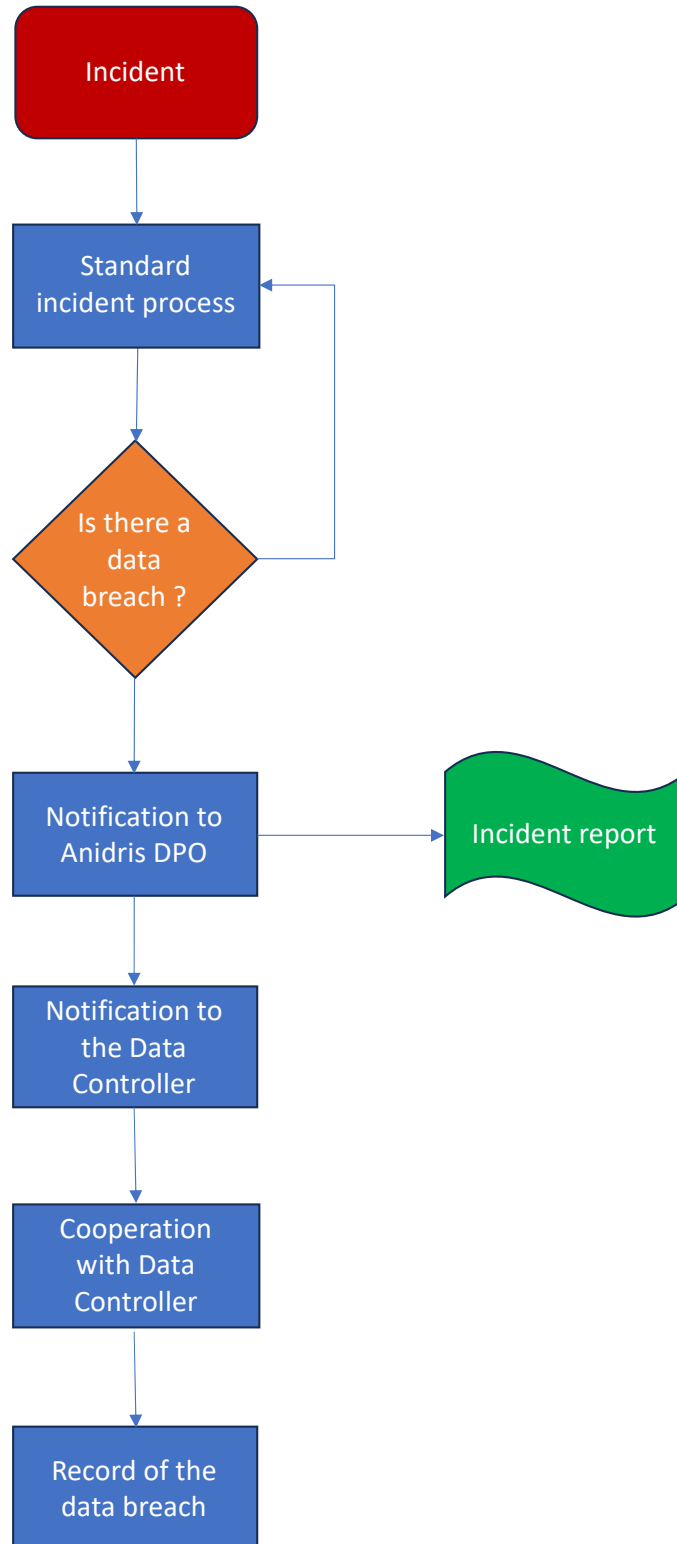


Figure 1 - Data Personal Breach notification process

2 Appendixes

2.1 Appendix 1 -Retention Policies

	Retention period of Incoming data	Retention Period of Output data

2.2 Appendix 2 -Definitions

- **Controller:** 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.
- **Incoming Personal Data** shall have the meaning of all Personal Data received from the Customer in a data set by the agreed communication channel for the provision of the Service.
- **Output Personal Data** shall have the meaning of all Personal Data included in data set and output files that are generated for the delivery of the Service.
- **Personal Data:** 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.
- **Processing:** 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Processor:** a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.
- **Recipient:** a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not.



Anidris S.A

Campus Contern
17, rue Edmond Reuter
L-5326 Contern

☎ (+352) 266 793 1

@ info@anidris.lu

anidris.lu