

As Controller

Data Privacy Policy


Project Reference: internal policy

Version: 1.0

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 released	DAN
1.0	2024.02.15	Reviewed by COO	JFLM

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 Accountability principles 5
 - 1.7 Information on the processing of Personal Data 6
 - 1.7.1 Categories of Data Subjects, Personal Data and Purpose 6
 - 1.7.2 Categories of personal data 8
 - 1.7.3 Categories of recipients 8
 - 1.8 Retention period and criteria used 9
 - 1.9 Security mechanism 10
 - 1.9.1 Information Security Policy 10
 - 1.9.2 Asset Management 10
 - 1.9.3 Human Resources Security 10
 - 1.9.4 Access Management 10
 - 1.9.5 Operational Security 11
 - 1.10 Data breach notification 12
 - 1.11 Rights of the Data Subject 13
 - 1.11.1 Complaints handling 13
 - 1.11.2 Consent 13
 - 1.11.3 Attendance to rights 14
- 2 Appendixes 15
 - 2.1.1 Appendix 1 - RPA as a controller 15
 - 2.2 Appendix 2 -Definitions 16

1 Data Privacy Policy

1.1 Introduction

The European Union's General Data Protection Regulation n° 2016/679 of 27 April 2016 ("GDPR") and the applicable national legislation (hereinafter altogether "Data Protection Legislation") provides major protection rules to natural persons, whose Personal Data are processed.

Anidris is fully committed to respect the Data Protection Legislation and to ensure the privacy and appropriate use of Personal Data entrusted by you to Anidris.

In the course of its activities, Anidris can act as Controller or as Processor. It is clearly identified as Controller when it determines the purposes and means of the processing of your personal data.

1.2 Scope & Purpose

The scope of this policy covers all personal data processed by ANIDRIS as Controller.

The purpose of this policy is to provide:

- guidelines and principles to comply with in order to protect Personal Data in accordance with the Data Protection Law;
- information on the processing of Personal Data.

This policy is completed by the below- referenced documents.

1.3 Ownership and review

The owner of this policy is the Management and the DPO function. The owner of the policy shall initiate the review process at a minimum on a yearly basis unless if required earlier.

1.4 References

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

Document Title	Location
Cookies Management Policy	Anidris' website
Privacy Statement	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	+352 621 26 99 27
Email	privacy@anidris.lu

1.6 Accountability principles

ANIDRIS Management has implemented different tools to ensure its compliance to the Data Protection Legislation. Amongst those, a data mapping has been performed and has led to the establishment of Records of processing including all required information set out in the GDPR, which is yearly reviewed and approved.

ANIDRIS Management has decided to appoint a Data Protection Officer whose contact details are provided above.

ANIDRIS takes into account the protection of Personal Data on a risk based approach from designing and by default and undertakes to conduct Data Privacy Impact Assessment each time that it may appear that a high risk exists for data subjects whose Personal Data are processed.

ANIDRIS Management ensures that its employees authorised to access Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

ANIDRIS applies the principle of minimisation, which requires that only personal data strictly necessary for the processing are processed.

1.7 Information on the processing of Personal Data

1.7.1 Categories of Data Subjects, Personal Data and Purpose

1.7.1.1 Employees

Personal data of employees are processed to enable ANIDRIS to execute your employment agreement and comply with legal obligations. Within this context, ANIDRIS process your data for the main following purposes:

- **Recruitment and staff management:** Recruitment and selection of staff and intermediaries, administration of wages, salaries and commissions, application of social legislation.
- **Staff monitoring:** Evaluation and monitoring of staff, training and career planning.
- **Planning and monitoring of tasks:** Workload and benefits, Professional agenda, monitoring of IT activities for security purpose, GPS tracking system.
- Protect employees from harassment conducts coming from other employees (team members or managers).

For each processing, ANIDRIS has different legal grounds justifying the process of personal data. For instance, ANIDRIS needs employees' bank details to pay salaries and provide other contractual entitlements. In addition, ANIDRIS has a wide range of legal obligations towards their employees. For instance, ANIDRIS needs to maintain records of sick leave and other leaves for which employees are entitled to statutory payments and are also subject to health and safety laws in certain circumstances.

In some cases, legitimate interest can be argued to process employee's personal data, provided it doesn't infringe an employee's right to privacy. For example, for physical archives transport, ANIDRIS requires employees to be tracked through a GPS system. ANIDRIS also needs to record when employees enter and leave the office premises for security reasons. ANIDRIS does need this data to perform their contractual obligations or to comply with legal obligations and, for security reasons.

1.7.1.2 Visitors

Personal data of visitors are processed to enable ANIDRIS to execute ANIDRIS Non Disclosure Agreement (NDA) and comply with legal obligations as well as maintaining the security within its installations. Within this context, ANIDRIS process visitors' data for the main following purposes:

- Planning and monitoring of tasks.
- Preserve customer and ANIDRIS data
- Health and safety

1.7.1.3 Clients and suppliers

Personal data of clients and suppliers are processed to enable ANIDRIS to execute ANIDRIS agreements and comply with legal obligations. Within this context, ANIDRIS process clients and suppliers' data for the main following purposes:

- **Client administration:** Order management, deliveries and billing of services, know your customer obligations (in relation with anti-money laundering, anti-bribery and counter-terrorist financing laws and regulations), monitoring of solvency, marketing and advertising, registration of the client on the database.
- **Client support and investigation assistance:** logging of activities, request for supports.
- **Suppliers' administration:** Management of orders issued, payment of suppliers, prospection of potential suppliers and their evaluation.

1.7.1.4 Website visitors

ANIDRIS' websites, online services, interactive applications, email messages, and advertisements may use "cookies" and other technologies such as pixel tags and web beacons. These technologies help ANIDRIS to better understand user behaviour, to know which parts of our websites people have visited, and facilitate and measure the effectiveness web searches.

ANIDRIS also uses cookies and other technologies to remember personal data when users use website, online services, and applications. Objective in these cases is to make experience with ANIDRIS website more convenient and personal.

Users have the opportunity to disable cookies and to manage their preferences. However, certain features of ANIDRIS website will not be available once cookies are disabled.

As is true of most Internet services, ANIDRIS gathers some information automatically and store it in log files.

This information includes Internet Protocol (IP) addresses, browser type and language, Internet service provider (ISP), referring and exit websites and applications, operating system, date/time stamp, and clickstream data.

ANIDRIS uses this information to understand and analyses trends, to administer the site, to learn about user behaviour on the site, to improve our product and services, and to gather demographic information about our user base as a whole.

ANIDRIS may use this information in our marketing and advertising services.

ANIDRIS informs all users in a privacy statement available on ANIDRIS website.

ANIDRIS has defined a specific Cookies Management Policy available on ANIDRIS website as well.

1.7.2 Categories of personal data

In order to fulfil the above-mentioned purposes ANIDRIS processes the following categories of personal data:

- **Personal identification data:** Name, Surname, address, telephone number.
- **Financial identification data:** Account number, credit card.
- **Criminal record:** Whether or not the employee has a criminal record.
- **CV:** History of working life.
- **Salary:** Payments, bonus, expenses, meal vouchers, retained taxes, labour union payments, payment methods, etc.
- **Appraisal (Evaluation) / Psychological Data:** Personal evaluation on how the employee is / feels on his/her position and exposition of possible problems.
- **Absence:** Reason for the absence, measures envisaged.
- **Agenda:** Actual responsibilities, projects, timesheet, agenda.
- **Electronic Data:** such as IP address, cookies.

1.7.3 Categories of recipients

Personal data processed by ANIDRIS as a controller (from employees, visitors, clients or suppliers) will only be disclosed to third parties such as public organizations when there exists a legal obligation for ANIDRIS to disclose it, to suppliers when it is necessary in order to receive the service provided and under a contract specifying the lawfulness of the processing done by the supplier and to clients when necessary to carry out some service provided by ANIDRIS. In particular:

- Relevant public bodies (such as CNS, Administration des Contributions Directes, CSSF);
- ANIDRIS providers: IT providers, accounting company, insurance broker, leasing company, meal vouchers issuer;
- ANIDRIS clients (to the extent necessary for the provision of services to ANIDRIS clients);
- ANIDRIS shareholders for reporting activities (POST in particular).

1.8 Retention period and criteria used

Personal data are processed for a duration equivalent to limitation period. Hence, ANIDRIS has defined a retention policy for each data processing and depending on the purpose. In any case, retention periods have been defined based on legal grounds (consent, contractual obligations, legal obligations or legitimate interests).

All retention periods have been defined in the record of processing of ANIDRIS as a controller that is available on demand to the DPO.

1.9 Security mechanism

1.9.1 Information Security Policy

ANIDRIS has defined a documentation framework (**draft**) for its information security policies. These policies 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. Back up copies of information, software and system are done and tested regularly based on a defined backup policy.
- A log management architecture is in place for recording user Retention period and data subject rights

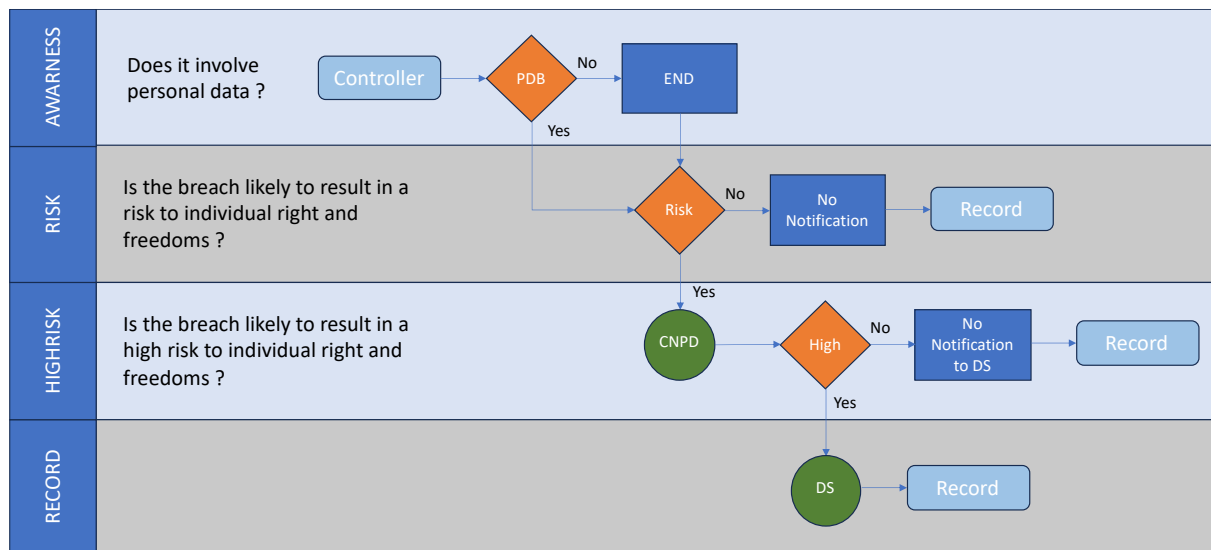
1.10 Data breach notification

When a personal data breach has occurred, ANIDRIS will establish the likelihood and severity of the resulting risk to data subjects’ rights and freedoms. If it’s likely that there will be a risk then ANIDRIS will notify the CNPD. This notification to the CNPD will be done at the latest 72h after ANIDRIS becomes aware of the data breach.

If the data breach is likely to result in a high risk to data subjects’ rights and freedoms, ANIDRIS will notify all data subjects were feasible. Otherwise, ANIDRIS will do a public communication.

The communication will include at least:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one)
- or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.



1.11 Rights of the Data Subject

ANIDRIS has defined a Privacy Statement where the process for managing rights of data subject is described.

Rights of data subject include:

- Right of access.
- Right to rectification.
- Right of erasure (right to be forgotten).
- Right to restrict processing.
- Right to data portability.
- Right to object.

Specific notices explaining each of those rights are available to all employees on intranet.

1.11.1 Complaints handling

ANIDRIS is doing its best to comply with the GDPR, not only as a legal obligation, but also because ANIDRIS truly believes in Privacy as a fundamental principle that everyone should follow.

However, in case there is an infringement of the regulation (GDPR) or if you think that your personal data is not being processed according to your expectations, you have the right to lodge a complaint to the Commission Nationale pour la Protection des Données (CNPD).

1.11.2 Consent

Whenever the legal basis of the processing is based on the consent provided by the data subject, ANIDRIS will make sure that the consent request is prominent, concise, separate from other terms and conditions, and easy to understand.

ANIDRIS will ask individuals to actively opt in.

ANIDRIS will keep records to evidence consent – who consented, when, how, and what they were told.

Individuals have the right to withdraw its consent at any time. To do so they can request the withdrawal of the consent at:

Email : privacy@anidris.lu

Adress : Campus Contern, 17, rue Edmond ReuterL-5326 Contern

1.11.3 Attendance to rights

ANIDRIS has a process in place in order to manage all requests of data subjects for which it is processing personal data as a controller. This process is described on ANIDRIS website and on ANIDRIS internal documentation.

Data subjects have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

You may exercise the above mentioned rights and/or lodge a complaint at the following email address: privacy@anidris.lu

Data subjects have the right to object to processing based on legitimate interests or the performance of a task in the public

2 Appendixes

2.1.1 Appendix 1 - RPA as a controller

Purpose	Categories of individuals	of Categorization of personal data	of Retention period of Incoming data	Retention Period of Output data
Staff administration, HR	Employees	Contact details, financial details	1 years after leaving	N/A
	Emergency contact	Contact details,	1 years after leaving	N/A
Customer order	Customers	Contact details, financial details, various documents	5 years after usage	Unlimited
	Suppliers	Contact details, financial details, various documents	5 years after usage	Unlimited
Marketing	Customers	Contact details	5 years after usage	Unlimited
Technical operation	Customers	Contact details	5 years after usage	unlimited

2.2 Appendix 2 -Definitions

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, organisation, 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.

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.

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.

Cookies: A cookie is a text file that a Web browser stores on a user's machine.

IP address: An IP address is a unique address that identifies a device on the Internet or a local network. It allows a system to be recognized by other systems connected via the Internet protocol.



Anidris S.A

Campus Contern
17, rue Edmond Reuter
L-5326 Contern

☎ (+352) 266 793 1

@ info@anidris.lu

anidris.lu