# PERSONAL DATA PROTECTION POLICY

**NOVEMBER 2022**

**Personal data protection policy of A.R.T. Assurances et Réassurances Techniques**

A.R.T
LE SPÉCIALISTE DE L'ASSURANCE
D'OBJETS D'ART ET D'OBJETS PRÉCIEUX

# SUMMARY

# 1. Introduction

In the course of our business, we are required to collect and process personal data which, in some cases, may prove to be of a particularly sensitive nature, such as financial or medical information.

In general, the handling of personal data (belonging to clients, employees, prospects, insured members, beneficiaries, annuitants, etc.) requires us, on a personal and corporate level, to make every effort to preserve confidentiality and to fulfil our legal obligations in this area.

This document presents the principles which CABINET ART strives to apply in order to preserve the confidentiality of the data entrusted to us, with due respect to human identity, privacy and freedoms.

**Why privacy is a business issue?**

As organizations are required to collect growing amounts of personal information, they become increasingly vulnerable to multiple risks such as the loss, misuse, unauthorized access or unauthorized disclosure of that information. These increased vulnerabilities raise concerns for companies, governments, individuals and the public in general.

People today are careful to protect and preserve the confidentiality of their personal information (in particular with regard to financial or medical data). They expect their privacy to be respected and the companies to which they entrust their information to protect it.

The following risks may be incurred if protection procedures are inadequate:

- damage to corporate image and reputation,
- legal risks, industry sanctions, action by the regulator, liability in the event of identity theft, etc.,
- loss of credibility by the company with regard to its clients or employees,
- loss of business and its impact in terms of reduction in profit and market share, etc.

In our case, as our activity extends over a number of different countries, the management of these risks is complex: we must comply with French legislation on data protection and freedom of information, with European directives (such as those relating to cross-border transfer of data) and also with any relevant local legislation.

This policy aims to provide a comprehensive, corporate framework to ensure the protection of the personal data entrusted to us, while preserving the characteristics of each entity, with respect to the risks incurred and the legislation and contexts which apply.

**Personal data and privacy**

Privacy can be defined as "the rights and obligations of individuals and organizations with respect to the collection, retention, disclosure and disposal of personal information".

Personal information is information regarding an identifiable individual or information which may be used to identify an individual. This includes clients, prospects, employees and any other persons with whom the entity has dealings.

Most information collected about a person is considered to be personal:

- name,
- home or email address,
- telephone number,
- identification numbers (such as Social Security or insurance policy numbers), etc.

Sensitive data (such as medical, health or financial information, etc.) requires greater levels of care and protection.

The collection of some other types of data, such as racial or ethnic origin, political, religious, or philosophical views, membership of a trade union or sexual orientation, is forbidden.

## 2. General system to be adopted

**Overall privacy objective**

Personal information must be collected, used, retained, disclosed, and disposed of in accordance with both the country's privacy laws, and the CABINET regulations presented in this document.

To meet this objective, each entity must create a system designed to protect the personal data entrusted to it, whether by clients, prospects, partners, suppliers, or employees.

This system must include the following features:

1. The appointment of an individual responsible for the management and monitoring of these issues.

This individual should be selected internally by the CABINET PRESIDENT.

His or her role is to ensure the proper consideration of all aspects of our policy and the legal compliance of any existing system.

2. The production of a formal internal document describing the system and the means used for the protection of data.

This document should specify the principles to be applied in respect of the protection of privacy. These principles must:

- comply with the key principles that the Group strives to apply, as specified in part 3 of this document,

- comply with local regulatory requirements (if no legal obligations are applicable locally, the document may be reduced to contain only the principles relating to the implementation and monitoring of CABINET regulations),
- be commensurate with the risks incurred by the entity and in line with market practices.

3. Internal or external controls ensuring proper compliance with the procedures implemented and the monitoring of our potential vulnerabilities with regard to electronic access to our data.

# 3. Basic principles to be adopted

## 3.1. The principle of relevance

The information collected and processed must be relevant, necessary, and proportionate to the stated objectives.

It may be processed only for a particular and legitimate purpose consistent with the stated objectives; it may not be used in a manner inconsistent with the purpose for which it was collected.

## 3.2. Prohibited and sensitive data

The CABINET does not collect, for any reason whatsoever (other than regulatory requirements), data relating to:

- racial or ethnic origin,
- political, philosophical or religious views,
- trade union membership,
- sexual orientation, and
- generally any data that may be discriminatory or defamatory.

**Medical data**

In the course of our business, in particular in the provision of health and death and disability cover, but also in the case of physical injury, we need to collect and handle medical data.

This data is particularly sensitive and, as such, should be afforded special attention and is subject to medical confidentiality.

For further information on this point, please contact your entity's consulting physician,

**Social Security number (or equivalent)**

For the health, retirement or death and disability side of our business, we may be allowed to collect and use social security numbers: you must therefore ensure that your legislation permits you to use this number and in what context.

**Financial data**

The collection and retention of financial data must be handled very carefully, as it is obviously of great interest to those who would seek to misuse it.

Special care must be taken (truncation, encryption, etc.) in such areas as collection, retention, and communication of personal bank details (account number, credit card number, etc.).

## 3.3. Strict compliance with our legal obligations

If your entity is subject to such obligations, the procedure implemented should comply fully with them.

Please note the following important points, depending on the legal circumstances:

- If there is an obligation to inform people as to the reasons for the collection of data and/or their rights, the physical documents must be compliant but electronic forms completed via an intranet or extranet should not be forgotten. Moreover, for online enrolments, other precautions should be taken, in particular a requirement for the user to actively acknowledge and accept the terms and conditions.
- With respect our contracts signed with sub-contractors who handle personal data on behalf of our group (or a group entity), it is essential to insert a standard clause in the contract specifying that:
    - the sub-contractor complies with the legislation in force and agrees to implement all necessary measures or procedures to ensure legal compliance with respect to their handling of data,
    - they agree not to release or disclose this data to third parties without our prior agreement.
- Video surveillance also falls under the heading of collection of personal datat as it can have an impact on privacy. Depending on the legislation in force in each country, particular precautions should be taken with regard to the use of information.
    - Recording of telephone conversations with clients: depending on the obligations in force in this regard, it will be necessary to review the possibility to inform the client that the conversation may be recorded. In this case, it will also be necessary to think about the retention period of records (for destruction).

## 3.4. The principle of security and confidentiality of data

All necessary measures should be taken to ensure the confidentiality of data and to prevent disclosure to unauthorized persons, whether internal and external.

Personal data should only be used or accessed by duly authorized persons. These principles should be applied to the physical and logical systems. There are a number of resulting implications, such as:

- that internal and external authorizations should be clearly defined in terms of "who can handle this type of data (creation/modification) and who has read-only access",
- that files containing sensitive information are protected and restricted, that the methods of collection of sensitive data are secure,
- that our external communications are well controlled.

For example, it is not appropriate to hold an individual's username and password together, because in the event of interception by a third party, this third party will have access to a secure and confidential online space which is not theirs.

Determine the identity of a person before supplying them with any personal information.

This also means truncating certain types of information, such as the account details on bank statements, or encrypting certain types of highly sensitive information if it is being disclosed externally (such as credit card numbers). Finally, vulnerability testing should be carried out regularly in order to test the level of protection of our data and to identify potential vulnerabilities of our privacy systems.

For further information, discussion or advice o the monitoring and implementation of this policy, please contact:

Judith GOLDNADEL
President of A.R.T.
+33 1 44 20 95 04
judith.goldnadel@art-assurance.com