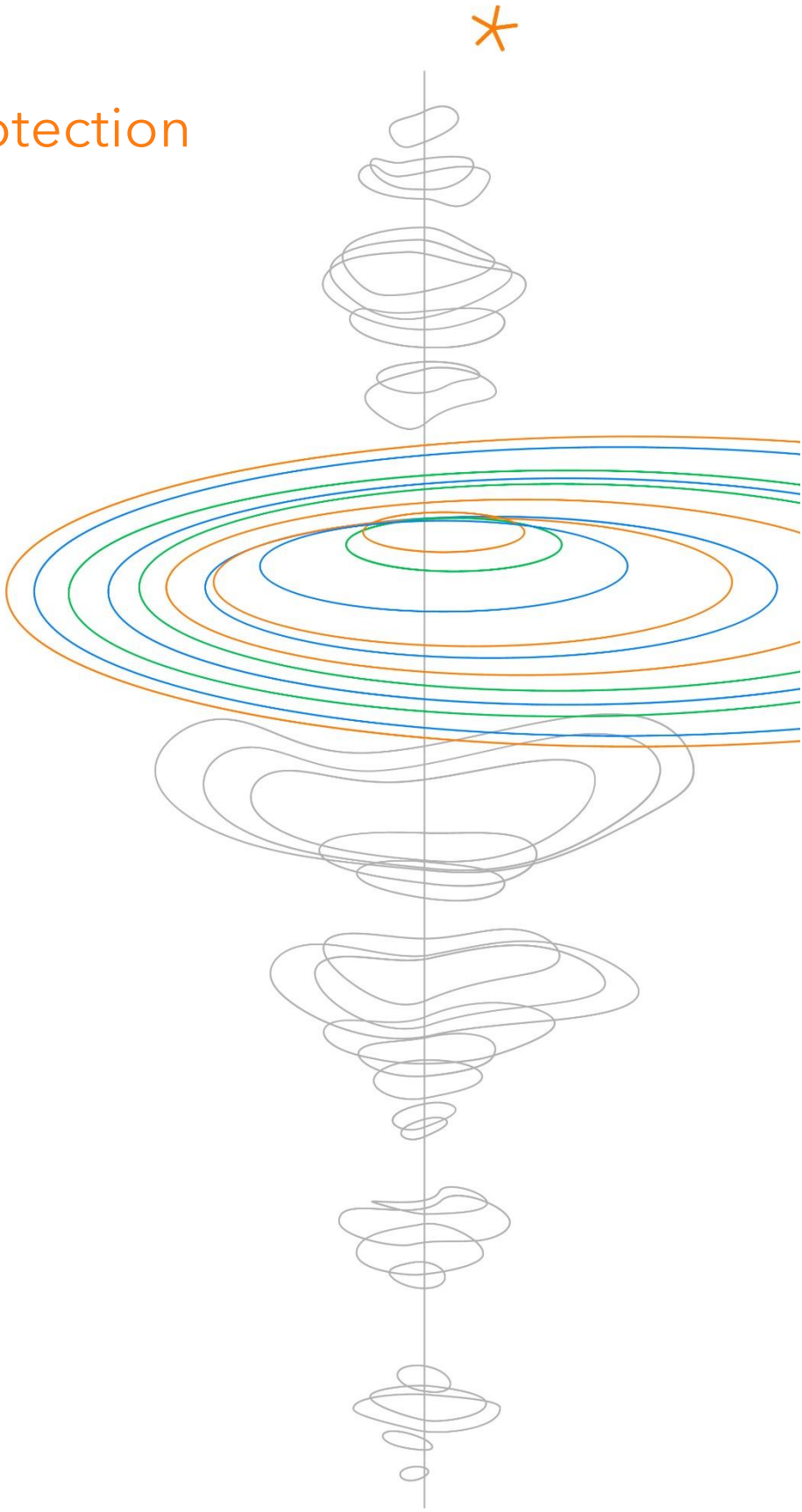
Personal Data Protection Policy



Introduction

In its everyday business TOBAM makes use of a variety of data about identifiable individuals, including data about:

- Current, past, and prospective employees;
- Customers/ Subscribers;
- Stakeholders;
- Counterparts ;
- Service providers.

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe which measures TOBAM is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation's information systems, including directors, employees, suppliers and other third parties who have access TOBAM systems.

The following policies and procedures are relevant to this document:

The General Data Protection Regulation principles

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that TOBAM carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is TOBAM's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

1. Definitions

The most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

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' means:

any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.

'controller' means:

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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

2. Principles Relating to Processing of Personal Data

There are several fundamental principles upon which the GDPR is based (Article 6).

These are as follows:

1. *Personal data shall be:*

   a) *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

   b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

   c) *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

   d) *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

   e) *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*

   f) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

TOBAM will ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

3. Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to delete
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within TOBAM that allow the required action to be taken. All requests will be taken care as soon as possible and without undue delay, respecting the maximum timescale defined by the CNIL and GDPR.

Data Subject Request	Articles	Maximum Timescale	Mean
The right to withdraw consent	7	Without undue delay	- Mean equivalent to the one used to obtain consent, preferably via the dedicated email address
The right to be informed	12, 13, 14	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)	- Any mean that is clear, transparent, understandable, and easily accessible.
The right of access	15	One month in case of simple request. Three months in case of complex request. (*)	- preferably via the dedicated email address - by mail - On site
The right to rectification	16	One month in case of simple request. Three months in case of complex request. (*)	- preferably via the dedicated email address - by mail
The right to delete	17	One month in case of simple request. Three months in case of complex request. (*)	- preferably via the dedicated email address - by mail
The right to restrict processing	18	Without undue delay	- via the dedicated email address
The right to data portability	20	One month in case of simple request. Three months in case of complex request. (*)	- via the dedicated email address
The right to object	21	- On receipt of objection if case of commercial prospection. - Within one month in case of personal data deletion from a database.	- preferably via the dedicated email address - by mail

(*) In any case, the individual must be informed **within one month**, that

- his/her request is taken care of, and
- if applicable, if the delay is postponed to three months.
- the dedicated email address is: dataprotection@tobam.fr
- the on site address / Mail is: TOBAM, Compliance officer, 49-53 avenue des Champs Elysées, 75008 Paris, France

Data Requests for Access and Transfer

Requests must include the data subject's identification details, proof of identity if necessary, and the exact need. TOBAM is entitled to ask further clarification about the request if a large quantity of information is processed.
All personal data disclosed in response to such request will be communicated by a method appropriate to the security and sensitivity of the information. Information containing sensitive personal data sent by email or via USB or other portable media will be encrypted. If personal data is sent via hardcopy, the envelope/package shall be marked as strictly private and confidential and preferably sent via letter with acknowledgement of reception.

Withdrawal of consent (article 7)

The data subject must be informed about his or her right to withdraw consent anytime. This will not affect the lawfulness of processing based on consent before its withdrawal.

Data updates, amendments, and erasure (Articles 16 and 17)

TOBAM has controls and procedures in place to allow personal data to be deleted or rectified (where and when applicable). TOBAM will make it a priority to keep personal data accurate and up to date. Requests will be communicated to the relevant team holding such data and will be dealt with accordingly. Upon the updates, amendment or erasure of such personal data, a notification will be sent to notify you regarding the completion of the process.

Right to restriction of processing (Article 18)

TOBAM has put in place controls and procedures to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing.
Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, TOBAM is permitted to store the personal data, but not use it.
This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Data portability (Article 20)

Individuals may request to be provided with their personal data in a structured, commonly used and machine-readable format for data obtained via consent or a contract only.

Right to object to processing (Article 21)

Data subjects have the right to object to certain types of processing such as direct marketing or where the legal basis of the processing is legitimate interests or necessary for a task carried out in the public interest. TOBAM has put in place controls and procedures to halt the processing of personal data where an individual has objected to the processing.

Data stored in a Secure Fortified Safe

Tapes will be held for an indefinite period in a safe at the home address of the President of TOBAM. The files in the safe are for storage purposes only and may be accessed on a case-by-case basis subject to the validation of the President or the Chief Operating Officer (COO) and in their absence, the Head of Compliance.

I. Lawfulness of Processing

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is TOBAM's policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief in the following sections.

Consent
TOBAM should always obtain explicit consent from a data subject to collect and process their data. This information will be provided in an accessible form, written in clear language and free of charge.

TOBAM does not request consent from prospects as they are belonging to business entity which TOBAM wants to deal with and relies on legitimate interest's principle. They will have nevertheless have the option to refuse to continue to be part of the mailing list they are included in and to ask TOBAM to delete their information.

All other personal information that TOBAM could collect are based on the below:

Performance of a Contract
Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question.

Legal Obligation
If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example or information provided within TOBAM's relationship with regulators.

Legitimate Interests
If the processing of specific personal data is in the legitimate interests of TOBAM and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing.

Vital Interests of the Data Subject
In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. TOBAM will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used in aspects of Health care.

Tasks Carried Out in the Public Interest
Where TOBAM needs to perform a task that it believes is part of an official duty then the data subject's consent will not be requested.

Certain limitations that can be placed on data subjects' rights
Under Article 23 it is allowed for the CNIL to restrict the scope of rights as provided in Articles 12 to 22 and Article 34 of the GDPR. Also, the reach of Article 5 GDPR concerning the principles of data processing can be restricted if its provisions correspond to the rights and obligations found in Articles 12 to 22 GDPR.

These restrictions must respect the essence of the fundamental rights and freedoms and be in line with the requirements of the EU Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. In addition, they are required to constitute necessary and proportionate measures in a democratic society meaning that there must be a pressing social need to adopt these legal instruments and that they must be proportionate to the pursued legitimate aim. In addition, they must safeguard certain important interests. They are required to be necessary and proportionate and must protect various interests such as:

- Relating to national security, defence and public security (when the State engages in intelligence gathering activities in the field of national security and process personal data).
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties fall under these important interests and they include safeguarding against threats to public security and preventing them.
- Relating to important economic or financial interests of both the Union or its Member States, which include monetary, budgetary and taxation matters, public health and social security.
- The protection of judicial independence and judicial proceedings and the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, such as lawyers and doctors.
- In order to protect the data subjects or the rights and freedoms of others and to enforce civil law claims (when there is a necessity to protect public health or to respond to humanitarian crises).

TOBAM will act pursuant to an Article 23 instruction only in respect of the foregoing.

II. Privacy by Design

TOBAM has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including if needed the completion of one data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

III. Contracts Involving the Processing of Personal Data

TOBAM will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR.

IV. International Transfers of Personal Data

Transfers of personal data outside the European Union will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR.

Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

V. Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, TOBAM does not require a Data Protection Officer to be appointed.
The IT administrator will be TOBAM's information Security Manager with a dedicated focus on information security and related issues.
The compliance of TOBAM will be the data controller which ensure that the principles relating to GDPR are adhered to and who is able to demonstrate compliance with them.

VI. Data Protection Impact Assessment

To comply with the article 35 of GDPR, Companies must establish a data Protection impact assessment when:
a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The protection impact assessment is in particular required in the case of:

- *systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*

- *processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*

- *a systematic monitoring of a publicly accessible area on a large scale*

Currently TOBAM does conduct any sensitive activities as described in article 35 so there is no need to do an assessment of the impact of the data protection.

VII. Breach Notification

With respect to Article 32 of the GDPR: If you notice any breach to this procedure, please follow the incident reporting procedure G:\Compliance\Procedures\Procedures - Compliance\ Incident Reporting Procedure.

Notification to CNIL, if necessary, will be performed in accordance to the Incident Reporting Procedure.

VIII. Addressing Compliance to the GDPR

The following actions are undertaken to ensure that TOBAM always complies with the accountability principle of the GDPR:

- All staff involved in handling personal data understand their responsibilities for following good data protection practice.
- Training in data protection is provided to all staff once a year and relevant employees will have to fill the personal Data inventory TOBAM-wide Personal Data Inventory [Department] .xlsx

- The following documentation of processing activities is recorded:
  - Purposes of the personal data processing
  - Categories of individuals and personal data processed
  - Categories of personal data recipients
  - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
  - Relevant technical and organisational controls in place

- All employees have the following main responsibilities:
  - Report any processing activities to the IT administrator,
  - Report any actual or potential security breaches,
  - Contribute to data protection impact assessment where required.

- Duplication of records:
  - The regular update of inventories will avoid any unnecessary duplication of records.
  - The data access procedure is designed to avoid any unregulated duplication of records.