

THALES CYBERSECURITY AND DIGITAL IDENTITY

**Information notice for processing of personal data
for Internal Research & Development purpose**

1 / 8

Table of contents

1.	INTRODUCTION	2
2.	DATA CONTROLLER.....	4
3.	CATEGORIES OF PERSONAL DATA PROCESSED	4
4.	SOURCE OF THE PERSONAL DATA	5
5.	PURPOSE OF PROCESSING	5
6.	LEGAL BASIS FOR PROCESSING	5
7.	NATURE OF PROCESSING.....	6
8.	DATA RECIPIENTS.....	6
9.	DATA TRANSFERS	6
10.	DATA RETENTION	7
11.	DATA MINIMIZATION AND SAFEGUARDS	7
12.	YOUR RIGHTS.....	8
13.	UPDATES OF THIS NOTICE OF INFORMATION	8

THALES CYBERSECURITY AND DIGITAL IDENTITY

Information notice for processing of personal data for Internal Research & Development purpose

2 / 8

1. INTRODUCTION

1.1 THALES PERSONAL DATA PROTECTION POLICY

Thales places great importance on the protection of personal data and is committed to ensuring that such data is processed in a transparent, secure and lawful manner.

To this end, Thales has adopted Binding Corporate Rules (hereinafter the “**BCR**”).

The Thales BCR were approved by the French Data Protection Authority in deliberations No. 2023-144 and No. 2023-145 dated December 21, 2023.

The BCR constitutes the Thales Group's policy on the protection of personal data, defining the principles and procedures implemented by Thales in connection with any processing of personal data. You can access the Thales BCR by clicking [here](#).

1.2 PURPOSE OF THIS INFORMATION NOTICE

The activities of the Thales Cybersecurity and Digital Identity Global Business Unit (hereinafter referred to as “**CDI**”) are based on the development of products and services built on the design of algorithms and models, whether or not they involve artificial intelligence.

The performance, robustness and reliability of these algorithms and models directly depend on the quality, diversity, and representativeness of the datasets used for their development and training as well as for testing validation and improvement of related products and services.

Those datasets may contain personal data, including biometric data, collected from internal (e.g. collection of Thales employees' personal data) or external sources.

When re-using datasets originating from third parties (e.g. universities, national institutes, research laboratories, data providers) or publicly available sources, for internal research and development purpose, it may not always be possible to contact each individual concerned directly (e.g. where only images or biometric samples are available to Thales CDI).

This is why this notice is made publicly available on www.thalesgroup.com website in accordance with Article 14 of the General Data Protection Regulation (“**GDPR**”) in order to inform the individuals whose personal data are collected indirectly and processed by CDI entities, as described below.

THALES CYBERSECURITY AND DIGITAL IDENTITY

Information notice for processing of personal data for Internal Research & Development purpose

3 / 8

1.3 DEFINITIONS

The following definitions are essential for a good understanding of the scope of application of this information notice.

“Biometric Data”	means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
“Binding Corporate Rules” or “BCR”	means the Thales Binding Corporate Rules which have been approved by decision No. 2023-145 dated 21 st December 2023 of the French supervisory authority and which are applicable where Thales is acting as Data Processor or Data Controller. The Thales Binding Corporate Rules are accessible on the Thales public website .
“Data Controller”	means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
“Data Subject”	means any individual whose Personal Data is collected or processed under this information notice.
“Legitimate Interest Balancing Test”	means the assessment required when relying on Article 6(1)(f) GDPR, aimed at verifying that the Data Controller’s legitimate interest is lawful and specific, that the Processing is necessary to achieve it, and that the Data Subjects’ rights and freedoms do not override this interest. The Legitimate Interest Balancing Test documents this balance and supports compliance with the accountability principle.
“Personal Data”	means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, fingerprints, DNA...).
“Process” or “Processing”	means any operation or set of operations which is performed on Personal Data or 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.

THALES CYBERSECURITY AND DIGITAL IDENTITY

Information notice for processing of personal data for Internal Research & Development purpose

4 / 8

2. DATA CONTROLLER

The Data Controllers which are Processing your Personal Data under this information notice are the following Thales CDI entities, acting as separate data controllers:

- THALES DIS FRANCE SAS
- THALES DIS ESPANA SA
- THALES DIS ITALIA S.P.A
- THALES DIS ROMANIA SRL
- THALES DIS CZECH REPUBLIC S.R.O
- THALES DIS PTE. LTD
- THALES DIS USA, INC
- THALES DIS MAROC
- THALES DIS INDIA PRIVATE LIMITED
- THALES DIS MEXICO SA DE CV
- THALES DIS BRASIL CARTÕES E SOLUÇÕES DE TECNOLOGIA LTDA.

The above-mentioned entities may share your Personal Data with other Thales entities under the rules described in Section 8 and 9 hereunder in compliance with the Thales CDI instructions published on the Thales documents repository.

3. CATEGORIES OF PERSONAL DATA PROCESSED

Personal Data within the scope of this information notice may include:

- Facial image or images distinguishing features such as tattoos or other physical marks issued from photographs or video frames;
- Identity documents related Personal Data, including copies or images of identity documents;
- Biometric Data (e.g. facial images, fingerprints images, iris images or derived templates) as defined in Section 1 hereabove;
- Associated identification data (where available);
- Associated metal data (e.g. technical or contextual information linked to datasets).

THALES CYBERSECURITY AND DIGITAL IDENTITY

Information notice for processing of personal data for Internal Research & Development purpose

5 / 8

4. SOURCE OF THE PERSONAL DATA

Personal Data within the scope of this information notice may originate from third parties such as:

- Customers in the context of projects or solution testing and validation;
- Third-party providers (e.g. datasets suppliers, research institutions, laboratories, universities...).

Those datasets may be purchased, licensed for free to Thales CDI or publicly available.

Thales CDI systematically assesses the lawfulness of the initial collection of Personal Data and the conditions of reuse before any Processing.

5. PURPOSE OF PROCESSING

Personal Data within the scope of this Information Notice are processed exclusively for Thales CDI's internal research and development purpose.

Such internal research & development purpose may include:

- machine learning;
- performance testing;
- product and services' validation and improvement.

All Processing activities are strictly limited to development, learning, test and validation phases. Personal Data are not used in a production phase for direct commercial purpose nor for operational deployment.

Thales CDI does not sell your Personal Data to third parties.

6. LEGAL BASIS FOR PROCESSING

Processing is based on:

- Legitimate interest of Thales CDI (Article 6(1)(f) GDPR), consisting in internal research and development purpose as described in Section 5 hereabove. A Legitimate Interest Balancing Test is systematically carried out to ensure that Thales CDIs' interests do not override the rights and freedoms of Data Subjects.
- Where applicable for Biometric Data, one of the exemptions under Article 9 GDPR, including in particular:
 - processing necessary for scientific research purposes (Article 9(2)(j) GDPR);
 - explicit consent (Article 9(2)(a) GDPR);
 - data manifestly made public by the data subject (Article 9(2)(e) GDPR); or
 - other applicable legal grounds depending on the use case.

THALES CYBERSECURITY AND DIGITAL IDENTITY

Information notice for processing of personal data for Internal Research & Development purpose

6 / 8

7. NATURE OF PROCESSING

Processing may include:

- Collection and ingestion of datasets;
- Organization, structuring and storage;
- Analysis and transformation (e.g. feature extraction, template generation);
- Training and testing of algorithms;
- Generation of synthetic or derived data;

Depending on the use case, Personal Data may be used:

- without identification purpose (e.g. identity verification or authentication), in which case Article 9(1) GDPR does not apply; or
- with identification purpose, in which case additional safeguards and legal bases are implemented.

All Processing activities are subject to internal governance, ethical review processes and security controls.

8. DATA RECIPIENTS

Access to personal data is strictly limited to:

- Authorized and duly trained Thales CDI personnel within the Thales CDI entities listed in Section 2;
- Authorized employees of other Thales Group entities involved in research and development activities;
- Authorized employees of service providers acting on behalf of Thales CDI, it being specified that Personal Data are never shared with external third parties for their own purposes.

Thales CDI may be required to disclose your Personal Data to public, governmental and/or judicial authorities by law or in the context of litigation, legal proceedings or any other request from such an authority. In such cases, Thales CDI ensures that only strictly necessary data is disclosed.

9. DATA TRANSFERS

When your Personal Data is transferred by a Thales CDI entity established in the European Economic Area (hereinafter “the EEA”) or in the United Kingdom (hereinafter “the UK”) to a Thales Group entity established outside the EEA or the UK, in a country that has not been recognized as offering an adequate level of protection by an adequacy decision of the European Commission or the UK, this transfer is based on the Binding Corporate Rules (hereinafter the “BCR”) adopted by Thales.

Thanks to the Thales BCR, wherever your Personal Data is processed within the Thales Group, it benefits from the same standard of protection.

THALES CYBERSECURITY AND DIGITAL IDENTITY

Information notice for processing of personal data for Internal Research & Development purpose

7 / 8

Where Thales CDI uses external suppliers and service providers, Thales CDI ensures that the third-party concerned which processes Personal Data on behalf of Thales CDI, in compliance with Thales CDI's instructions and implements appropriate protection measures.

When your Personal data is transferred by a Thales CDI entity established in the EEA to a third-party established outside the EEA, in a third country that has not been recognized as offering an adequate level of protection by an adequacy decision of the European Commission, the exporting Thales CDI entity relies on Standard Contractual Clauses as adopted by the European Commission (hereinafter the "SCC"). You can obtain a copy of the SCC signed by Thales by clicking [here](#).

When your Personal Data is transferred by a Thales CDI entity established in the UK to a third-party established outside the UK in a third country that has not been recognized as offering an adequate level of protection by the UK, the concerned Thales CDI entity relies on the International Data Transfer Agreement (IDTA) or the International Data Transfer Addendum to the SCC issued by the Information Commissioner's Office.

10. DATA RETENTION

Personal data are retained only for as long as necessary for the research and development purposes pursued.

In particular:

- Biometric samples are kept only for the duration necessary to train the relevant models;
- Derived data (e.g. templates) are retained for a limited period aligned with the project needs.

The relevance and necessity of retaining the data are regularly reassessed, taking into account:

- the nature of the Processing performed,
- the research, technological and study needs,
- the legal and regulatory requirements.

When use of Personal Data is no longer necessary, they are securely deleted or irreversibly anonymized, where appropriate.

11. DATA MINIMIZATION AND SAFEGUARDS

Thales CDI implements appropriate technical and organizational measures, including:

- Data minimization and purpose limitation;
- Pseudonymization and/or de-identification where possible;
- Encryption of data at rest and in transit;
- Strict access control limited to authorized and duly trained personnel;
- Secure storage in controlled environments.

Where feasible, Thales CDI prioritizes the use of de-identified, anonymized or synthetic datasets.

THALES CYBERSECURITY AND DIGITAL IDENTITY

Information notice for processing of personal data for Internal Research & Development purpose

8 / 8

12. YOUR RIGHTS

You have the right to access your Personal Data.

You may also request the correction or deletion of your Personal Data.

You also have the right to withdraw your consent or to object to the Processing of your Personal Data and to request that such Processing be restricted.

Finally, you can request your Personal Data to be sent to you in a structured and standard format.

To exercise your rights or make a complaint, please use the dedicated form by [clicking here](#).

You may also contact the Thales Group Data Protection Officer by sending an e-mail to dataprotection@thalesgroup.com.

In all cases, you have the right to lodge a complaint with the competent data protection authority.

13. UPDATES OF THIS NOTICE OF INFORMATION

This notice may be updated from time to time to reflect legal, technical or organizational changes.

Last update: August 2026