BINDING CORPORATE RULES

THALES AS DATA PROCESSOR (BCR-P)

Public Version

THALES
Building a future we can all trust

TABLE OF CONTENTS

APPENDICES

1. INTRODUCTION

1.1 OBJECTIVES

Thales is a global technology leader investing in digital and deep tech innovations including connectivity, big data, artificial intelligence, cybersecurity and quantum technology. The company provides solutions, services and products that help its customers – businesses, organizations and states – in the defence, aeronautics, space and digital identity and security markets to fulfil their critical missions, while keeping human intelligence at the heart of the decision-making process.

As part of its activities, Thales processes a large amount of personal data and pays particular attention to their protection in compliance with applicable personal data protection legislation.

Such compliance needs to take into account an evolving legal environment, in particular, the European Union Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, adopted on 27th April 2016 and applicable since 25th May 2018 (the **"GDPR"**).

Thales' objectives are clear: providing a high level of protection to the Personal Data it processes and being able to demonstrate that commitment. Such obligation is also known as the accountability principle.

Moreover, it is important for Thales to document compliance with its commitments in order to comply with the requirements of the GDPR and other applicable data protection legislation.

This is the reason why Thales has adopted binding corporate rules (the **"BCR"**) which have been approved by the French data protection authority, the CNIL, by decisions No. 2023-144 and No. 2023-145 dated 21st December 2023.

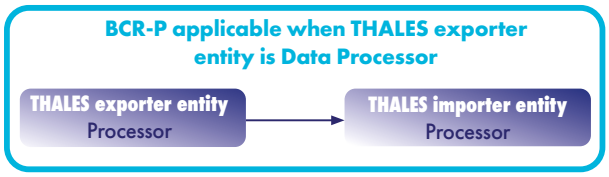
The BCR are designed to be used as Thales global data protection policy.

The French CNIL has approved two sets of BCR applicable whether Thales is data controller or data processor.

1.2 THE BCR-P (*"PROCESSOR"*)

The present BCR named **"BCR-P"** are applicable when a Thales Entity is acting as data processor under the instructions of an external data controller.

The BCR-P are suitable for framing transfer of personal data from a Thales entity acting as data processor and covered by the geographical scope of the GDPR pursuant to Article 3 GDPR to another Thales entity, acting as sub-processor and established in a third country that has not been recognized as providing an adequate level of protection pursuant to Article 45 of the GDPR.



Where the GDPR contains mandatory protective measures, the BCR-P describe how Thales will meet those measures. Where the GDPR contains principles, the BCR-P describe how Thales is to adhere to those principles. Local specificities outside of the scope of the GDPR are beyond the scope of the BCR-P.

Where local specificities apply, local policies may be implemented subject to the prior validation of the group data protection officer. Where the local legislation requires a higher level of protection for personal data, it will take precedence over the provisions of the BCR-P.

1.3 KEY DEFINITIONS AND ACRONYMS

"Agreement" refers to the contract concluded by Thales with the Client under which Thales acting as Data Processor is Processing Personal Data under instructions of the Client acting as Data Controller.

"Applicable Personal Data Protection Legislation" refers to any data protection regulation that may apply to the Processing of Personal Data by Thales and/or a Third Party and, in particular, (i) the GDPR, and (ii) any other applicable regulation relating to the Processing of Personal Data. For sake of clarity, with respect to Thales Entities established outside the EEA receiving Personal Data under the BCR-P, the Applicable Personal Data Protection Legislation shall be the one of the country of the Thales Entity established in the EEA exporting the relevant Personal Data.

"Competent DPA" refers to the EEA Data Protection Authority competent for the Thales Exporter Entity on the basis of the BCR-P.

"Data Controller" refers to 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.

"Data Processor" refers to a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

"Data Protection Authority" refers to the supervisory authorities as defined by the Applicable Personal Data Protection Legislation.

"Data Protection Correspondent" or **"DPC"** refers to the persons designated by Thales in accordance with Appendix 13.

"Data Protection Impact Assessment" or **"DPIA"** refers to the privacy impact assessment to be carried out by the Data Controller where a Processing is likely to result in a high risk to the rights and freedoms of Data Subjects.

"Data Subject" refers to an identified or identifiable natural person whose Personal Data are processed (e.g., Clients' employees, users of Thales products and services).

"EEA" refers to the European Economic Area.

"Group Data Protection Officer" or **"GDPO"** refers to the data protection officer of the Thales group, designated in accordance with Appendix 13.

"Lead Supervisory Authority" refers to the lead supervisory authority competent for the cross-border processing carried out by Thales, i.e. the *"Commission Nationale de l'Informatique et des Libertés"* (CNIL).

"Personal Data" refers to any information relating to a Data Subject, 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 Data Subject. Pseudonymized data remain Personal Data since it is still possible to retrieve the individual behind such pseudonymized data. On the contrary, anonymized data according to strict applicable standards making the anonymization irreversible would prevent the data from being qualified as Personal Data.

"Personal Data Breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"Personal Data Protection Organization" refers to the organization implemented by Thales in relation to the Personal Data protection as described in Appendix 13.

"Processing" refers to 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.

"Record" refers to the record of Processing activities of Thales.

"Sensitive Personal Data" refers to Personal Data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

"Standard Contractual Clauses" or **"SCC"** refer to the standard contractual clauses of the European Commission for the Transfer of Personal Data to Third Countries.

"Sub-Processor" refers to a Data Processor engaged by the Thales Entity acting as initial Data Processor for carrying out specific processing activities on behalf of the Data Controller. The Sub-Processor might by another Thales Entity or a Third-Party.

"Thales" (or **"Thales Entity(ies)"**) refers to Thales S.A. and/or Thales Affiliates bound by the BCR-P, as listed in Appendix 2.

"Thales Affiliate(s)" refers to any legal entity that is controlled either directly or indirectly by Thales S.A. For the purposes of this definition, "control" means Thales S.A. holding, either directly or indirectly, more than fifty percent (50%) of the economic rights or voting rights.

"Thales Client" or **"Client"** refers to any legal entity (except Thales or Thales Affiliates) acting as Data Controller i.e. on behalf of which Thales processes Personal Data in the context of an Agreement implying Personal Data Processing.

"Thales Exporter Entity" refers to any Thales Entity covered by the geographical scope of the GDPR pursuant to Article 3 GDPR and exporting Personal Data on the basis of the BCR-P to a Thales Importer Entity established in a Third Country i.e. a country outside the EAA that has not been recognized as providing an adequate level of protection pursuant to Article 45 of the GDPR.

"Thales Importer Entity" refers to any Thales Entity established in a Third Country that has not been recognized as providing an adequate level of protection pursuant to Article 45 GDPR, and receiving Personal Data from a Thales Exporter Entity on the basis of the BCR-P.

"Thales S.A." refers to Thales S.A., a French *"société anonyme"* with headquarters at 4, rue de la Verrerie, 92190 Meudon, France, with a share capital of EUR 630,630,420.00, registered with the Register of Trade and Companies of Nanterre under number 552 059 024.

"Third Country(ies)" means the country(ies) outside the EEA that have not been recognized as providing an adequate level of protection pursuant to Article 45 of the GDPR.

"Third Parties" refers to Thales' suppliers and subcontractors.

"Transfer" refers to a transfer or set of transfers of Personal Data, including material transfer or remote access to Personal Data by Thales Entities or Third Parties.

"Transfer Impact Assessment" or **"TIA"** refers to the assessment of the level of data protection in a Third Country and the need for the adoption of supplementary measures. A template of TIA is attached in Appendix 8 hereto.

2. SCOPE OF APPLICATION

2.1 EFFECTIVE DATE

The BCR-P shall apply from the date of coming into force of the Intra-Group Agreement, i.e. 15th May 2024.

2.2 MATERIAL SCOPE

2.2.1 The BCR-P shall apply when a Thales Entity is acting as a Data Processor on behalf of Clients and thus processes Personal Data according to the instructions of Clients (e.g., for the purpose of providing them with products and services).

Thales acknowledges that its status as Data Processor shall be based on how and why Personal Data are processed, Thales applying a fact-based procedure to determine its status.

2.2.2 The BCR-P apply to the Processing of Personal Data of all types, as follows:

- Identification data;
- Professional Information;
- Economic and financial data;
- Connection and traffic data;
- Cookies;
- Sensitive Personal Data (including data related to health and biometric data);
- Location data;
- Criminal convictions and offences;
- Data related to the use of interactive products and services.

Specific provisions relating to Sensitive Personal Data are set out under Section 5 of the BCR-P.

2.2.3 For sake of clarity, the following categories of Data Subjects shall be covered by the BCR-P:

- Clients' employees;
- Users of Client's/Thales products and services;
- Service Providers and suppliers' employees;
- External Data Subjects (for example in case of R&D experimentations and products & services' testing).

2.2.4 The list of purposes covered by the BCR-P is provided in Appendix 1. Appendix 1 may be updated from time to time according to Section 21 of the BCR-P.

2.2.5 The types of Personal Data Processing covered by the BCR-P are as follows:

- Collection;
- Access and communication;
- Consultation;
- Copy;
- Modification;
- Erasure;
- Hosting; and
- Archiving.

2.2.6 The countries of registration of the Thales Entities are listed in Appendix 2. This list includes the Third Countries, i.e. countries outside the EEA not benefiting from an adequacy decision and covered by Transfers under this BCR-P as per Section 8 hereafter.

2.3 GEOGRAPHICAL SCOPE

As mentioned above, Thales' objective is to ensure a consistent approach between Thales Entities when they Process Personal Data.

Those BCR-P are designed to be used as Thales global data protection policy applicable to all Thales Entities which Process Personal Data.

Regarding Transfers, the principles defined hereunder shall apply to Transfers of Personal Data from a Thales Exporter Entity covered by the geographical scope of the GDPR pursuant to Article 3 of the GDPR to a Thales Importer Entity established in a Third Country, as well as to their onward Transfers to other Thales Entities in a Third Country.

3. BINDING STATUS

3.1 BINDINGNESS AMONGST THALES ENTITIES

The BCR-P must be legally binding for Thales Entities irrelevant of their localization.

The list of Thales Entities bound by the BCR-P with their country of registration and contact details is specified in Appendix 2.

In practice, in order to be bound by those BCR-P, each Thales Entity shall sign an Intra-Group Agreement, a draft of which is attached in Appendix 3 hereto. By signing said Intra-Group Agreement, each Thales Entity commits to comply with the provisions of the BCR-P and to implement them within its own organization.

No Transfer can be made to a Thales Importer Entity in a Third Country on the basis of the BCR-P unless said Thales Importer Entity is effectively bound by the BCR-C and can deliver compliance.

3.2 BINDINGNESS AMONGST EMPLOYEES

Each Thales employee is bound by the same obligations as the ones defined under the BCR-P and can benefit from the rights granted under the BCR-P.

The BCR-P are to be respected by Thales employees and contractors in accordance with their employment contract and/or contract for services, the Thales employees general information notice and/or internal binding rules adopted by Thales and duly accepted by Thales employees as per Appendix 4 hereto.

Non-compliance with the BCR-P shall expose employees to disciplinary sanctions.

3.3 BINDINGNESS VIS-A-VIS THALES CLIENTS

Thales shall commit, vis-à-vis Clients, to respect the BCR-P. Thales shall ensure that a reference to the BCR-P is included in the Agreement entered into Thales and the Client together with a link to the public version of the BCR-P available on Thales website.

Without prejudice of the provisions of Section 9 of the BCR-P, Clients shall have the right to enforce the BCR-P (i) against any Thales Entity for breaches they caused, and, moreover, (ii) against the Thales Exporter Entity that has accepted liability (as provided for in Section 9) in case of a breach by the Thales Importer Entity of the BCR-P.

4. BASIC PRINCIPLES WHEN PROCESSING PERSONAL DATA

4.1 COMPLIANCE WITH CLIENTS' INSTRUCTIONS

Where it acts as Data Processor under the BCR-P, Thales is obliged to ensure that it Processes Personal Data only under the documented instructions of its Clients, including with regards to Transfers of Personal Data to a Third country, unless required to do otherwise by law. In such case, Thales shall inform the Client of that legal requirement before the Processing takes place, unless that law prohibits such information on important grounds of public interest.

In other cases, if Thales cannot comply with the Client's instructions, Thales shall promptly inform the Client of its inability to comply, in which case the Client will be entitled to suspend the Transfer of Personal Data and/or terminate the Agreement it has entered into with Thales.

Where Thales believes that an instruction of the Client infringes the Applicable Personal Data Protection Legislation, Thales, acting as Data Processor, shall immediately inform the Client.

As Data Processor, Thales shall Process Personal Data lawfully and in accordance with the Applicable Personal Data Protection Legislation and the Client's instructions.

An Agreement reflecting the Client's instructions and the requirements provided by Article 28 of the GDPR, must be agreed upon with the Client. If the instructions were to be modified by the Client, the modifications would have to be subject to an addendum to the Agreement.

4.2 SUBPROCESSING

The Thales Entity Processing Personal Data on behalf of a Client may subcontract said Client's Personal Data Processing to a Third Party and/or another Thales Entity only in accordance with Section 7 of the BCR-P.

In addition, Thales shall commit to cooperate and assist the Clients, where possible and within a reasonable period, in order to help and assist them to comply with Applicable Personal Data Protection Legislation, such as the duty to inform suppliers and subcontractors and have the Personal Data updated, corrected, anonymized or deleted upon Clients' request and according to their instructions.

Each Thales Entity will inform the other Thales Entities to whom Clients' Personal Data have been disclosed of any rectification, deletion or anonymization of Clients' Personal Data.

For any Personal Data Thales Processes as a Data Processor and, unless otherwise required as per Client's instructions, Thales will implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing as provided by Article 32 of the GDPR. Thales has a duty to implement technical and organizational measures which at least, meet the requirements of the Client's applicable law and any existing particular measures specified in the agreement concluded between Thales and the Client.

Taking into account the nature of Processing and information available to Thales, as a Data Processor, Thales will also have a duty to assist its Clients in ensuring compliance with the obligations as set out in the GDPR regarding the security of Personal Data (security of Processing, notification of a Personal Data Breach to the Data Protection Authority and communication of a Personal Data Breach to the Data Subject) and Data Protection Impact Assessment and related prior consultations.

Upon termination of the Agreement related to the Processing entered into with the Client, Thales (and any of its Sub-Processor) shall, at the choice of the Client, delete or return all the Personal Data to the Client and delete the copies thereof, and certify to the Client that it has done so, unless Applicable Personal Data Protection Legislation requires storage of the Personal Data Transferred. In that case, Thales (and any Sub-Processor) shall inform the Client and warrant that it will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore. For sake of clarity, Thales may keep Personal Data for the purpose of existing litigation or to bring or defend future claims, in accordance with Applicable Personal Data Protection Legislation.

It is the Client's sole responsibility, as a Data Controller, to ensure that the Processing it requests Thales to conduct is compliant with the Applicable Personal Data Protection Legislation and to communicate to Thales only Personal Data which have been collected and processed in accordance with the Applicable Personal Data Protection Legislation.

In addition to these elements and irrespective of the instructions received from the Client or as a result of Thales' contractual obligations, Thales, as a Data Processor, must comply with various obligations in particular in relation to:

- the Processing of Sensitive Personal Data as set out under Section 5;
- the management of Personal Data Breaches as specified under Section 6;
- the Processing of Personal Data by Sub-Processors as specified under Section 7;
- the Transfer of Personal Data outside the EEA as specified under Section 8;
- the management of Data Subjects' rights and the exercise thereof as specified under Sections 10, 11 and 12;
- the consideration of the requirement applicable to Personal Data protection by design and the implementation of a Data Protection Impact Assessment as specified under Sections 13 and 14;
- the maintenance of a Record of Processing activities as specified under Section 15;
- the cooperation with the Data Protection Authorities as specified under Section 16;
- the duty of transparency vis-à-vis Clients as specified under Section 17;
- training as specified under Section 18; and
- audit as specified under Section 19.

5. PROCESSING OF SENSITIVE PERSONAL DATA

The Processing of Sensitive Personal Data triggers additional obligations to the ones mentioned above. Hence, the obligations defined hereunder shall apply in addition to the ones defined above. Indeed, where Thales is required by a Client to process Sensitive Personal Data as Data Processor, the Client may require Thales to implement additional security measures.

It is Thales Client's responsibility to define what measures should be implemented in the Agreement entered into the Client and Thales, and, where it processes Sensitive Personal Data, Thales shall in no case be bound to ensure that the Processing relies on a legal basis.

In any event, Thales shall implement the adequate measures, as specified in the Agreement entered into with the Client, regarding the Processing of Sensitive Personal Data, and this in addition to the measures already specified under Section 4 here above.

6. PERSONAL DATA BREACH

Where Thales acting as Data Processor becomes aware of any Personal Data Breach, Thales shall inform the Client about such Personal Data Breach without undue delay and in accordance with the Agreement entered into with said Client.

In addition, Thales shall ensure that its Sub-Processors shall have the duty to inform Thales (and Thales commits to notify the Client) without undue delay after becoming aware of any Personal Data Breach.

Any Personal Data Breach shall be notified without undue delay to the Data Protection Correspondent(s) of the concerned Thales Entity(ies). The Data Protection Correspondent(s) shall immediately inform the Group Data Protection Officer and where appropriate Thales SA.

In any event, Thales shall comply with its Personal Data Breach policy as per Thales crisis management Checklist in Appendix 7.

Thales undertakes to document any such Personal Data Breach and to make the said documentation available to the Client upon request of the latter.

7. PROCESSING BY SUB-PROCESSORS

Although each Thales Entity is able to rely on its own resources and information system, a Thales Entity may also rely on Third Parties or on other Thales Entities to provide the Client with products and services.

Where a Thales Entity needs to rely on a Third Party or on another Thales Entity, acting as a Sub-Processor, it shall first obtain the prior informed specific or general written authorization of the Client according to the conditions defined under the Agreement entered into with said Client. Such Agreement will specify if a general prior authorization would be sufficient or if a specific authorization will be required for each new Sub-Processor. If a general authorization is given, the Client should be informed by Thales of any intended changes concerning the addition or replacement of a Sub-Processor in such a timely fashion that the Client has the possibility to object to the change or to terminate the Agreement before the Personal Data are communicated to the new Sub-Processor.

In addition, the Thales Entity relying on a Sub-Processor (whether a Third Party or another Thales Entity) shall enter into an agreement with said Sub-Processor which provides that adequate protection is ensured, as set out in the GDPR (Articles 28, 29, 32, and Chapter V relating to Transfers of Personal Data to Third Countries).

Same data protection obligations as set out in the Agreement between the relevant Thales Entity and the Client and in Sections 4, 6, 7, 10, 13, 14, 16, 17.2, and 17.3 of the BCR-P are imposed on the Sub-Processor, in particular by providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR.

8. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

8.1 APPROPRIATE SAFEGUARDS ON TRANSFERS TO A SUB-PROCESSOR

Where a Thales Exporter Entity established in a country in the EEA, acting as Data Processor, carries out a Transfer of Personal Data to a Thales Importer Entity established in a Third Country acting as Sub-Processor, such Transfer shall be framed by the provisions of the BCR-P.

Where a Thales Exporter Entity established in a country in the EEA, acting as Data Processor, carries out a Transfer of Personal to a Third Party established in a Third Country acting as Sub-Processor, such Transfer shall be framed by the European Union Standard Contractual Clauses adopted by the European Commission in accordance with the GDPR or by other appropriate safeguards in compliance with the Applicable Personal Data Protection Legislation.

In the absence of an adequacy decision or appropriate safeguards, Transfers may exceptionally take place if a derogation applies in line with the GDPR. The determination and implementation of the relevant safeguard or derogation where such Transfer of Personal Data takes place shall be defined by the relevant Thales legal department and/or the Data Protection Correspondent in consultation with the Client.

8.2 LOCAL LAWS AND PRACTICES AFFECTING THE TRANSFER TO A SUB-PROCESSOR

8.2.1 Transfer Impact Assessment (TIA)

Before carrying out Transfer of Personal Data to Third Countries, the Thales Exporter Entity and the Sub-Processor (whether a Thales Importer Entity or a Third-Party) shall conduct an assessment to ensure that they have no reason to believe that the laws and practices in the Third Country, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevent the Sub-Processor from fulfilling its obligations under the BCR-P (where the Sub-Processor is a Thales Importer Entity) or the Standard Contractual Clauses (where the Sub-Processor is a Third-Party).

This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23 (1) of the GDPR, are not in contradiction with the BCR-P.

When conducting the assessment mentioned above, the Thales Exporter Entity and the Sub-Processor shall take into account, in particular, the following elements:

- the specific circumstances of the Transfer, including the length of the Processing chain, the number of actors involved and the transmission channels used; the intended onward Transfers; the type of recipient; the purpose of Processing; the categories and format of the transferred Personal Data; the economic sector in which the Transfer occurs; the storage location of the data transferred;
- the laws and practices of the Third Country – including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the Transfer, and the applicable limitations and safeguards;
- any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the BCR-P or the Standard Contractual Clauses, including measures applied during transmission and to the Processing of Personal Data in the country of destination.

In carrying out this assessment, the Thales Importer Entity shall ensure to make its best efforts to provide the Sub-Processor with relevant information and shall continue to cooperate with the Thales Exporter Entity in ensuring compliance with the BCR-P or the Standard Contractual Clauses.

The Thales Exporter Entity and the Sub-Processor shall document the assessment mentioned above and make it available to the Competent DPA on request. A template of Transfer Impact Assessment to be documented for each Transfer is attached in Appendix 8 hereto.

8.2.2 Change in protection level / Transfer suspension

The Sub-Processor shall promptly inform the Thales Exporter Entity if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements of the first paragraph of this Section 8.1, including following a change in the laws of the Third Country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements of such first paragraph. The Thales Exporter Entity shall forward the notification to the Client. This information should also be provided to any liable Thales Entity as per Section 9 hereunder.

Following a notification pursuant to the above paragraph, or if the Thales Exporter Entity otherwise has reason to believe that the Thales Importer Entity can no longer fulfill its obligations under the BCR-P or the Standard Contractual Clauses, the Thales Exporter Entity and the concerned Data Protection Correspondent shall promptly identify appropriate measures (for example, technical or organizational measures to ensure security and confidentiality) to be adopted to remedy the situation. The Thales Exporter Entity shall suspend the Transfer of Personal Data if it considers that no appropriate safeguards for such Transfer can be ensured, or if instructed by the Client or the Competent DPA to do so, as well as all Transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or Transfer is ended.

Following such a suspension, the Thales Exporter Entity has to end the Transfer if the BCR-P cannot be complied with and compliance with the BCR-P is not restored within one (1) month of suspension. In this case, Personal Data that have been Transferred prior to the suspension, and any copies thereof, should, at the choice of the Thales Exporter Entity, be returned to it or destroyed in their entirety.

The concerned Thales Entities and the relevant Data Protection Correspondent or the Group DPO will inform all other Thales Entities of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of Transfers is carried out by any other Thales Entity or, where effective supplementary measures could not be put in place, the Transfers at stake are suspended or ended.

Thales Exporter Entities shall monitor, on an ongoing basis, and where appropriate in collaboration with Thales Importer Entities, developments in the Third Countries to which the Thales Exporter Entities have Transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such Transfers.

8.3 THIRD-COUNTRY COURTS AND AUTHORITIES DECISION

Any judgment of a court or tribunal and any decision of an administrative authority of a Third Country requiring a Thales Exporter Entity to transfer or disclose Personal Data may only be recognized or made enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting Third Country and the EEA or an EEA Member State, without prejudice to other grounds for Transfer pursuant to Chapter V of the GDPR.

8.4 DISCONTINUATION OF APPLICATION OF THE BCR-P TO A THALES IMPORTER ENTITY

A Thales Importer Entity, which ceases to be bound by the BCR-C may keep, return, or delete the Personal Data received under the BCR-C. If the Thales Exporter Entity and Thales Importer Entity agree that the Personal Data may be kept by the Thales Importer Entity, protection must be maintained in accordance with Chapter V of the GDPR.

The same commitments should apply to any copies of the Personal Data.

In case of local laws applicable to the Thales Importer Entity that prohibit the return or deletion of the Transferred Personal Data, the Thales Importer Entity should warrant that it will continue to ensure compliance with the BCR-C, and will only process the Personal Data to the extent and for as long as required under that local law.

9. LIABILITY

Any Thales Exporter Entity established in the EEA and exporting Personal Data outside the EEA on the basis of the BCR-P shall accept liability for any breaches of the BCR-P by a Thales Importer Entity established outside the EEA. The Thales Exporter Entity also agrees to take the necessary action to remedy these acts and to pay compensation for any material or non-material damages resulting from the violation of the BCR-P by the Thales Importer Entity. The Thales Exporter Entities confirm that they have sufficient assets to enable themselves to enforce such obligation.

In the event a Thales Importer Entity violates the provisions of the BCR-P, the courts or other competent authorities in the EEA shall have jurisdiction and the Data Subject shall have the rights and remedies against the Thales Exporter Entity as if the violation had been caused by it within the EEA Member State where it is established and not by the Thales Importer Entity.

If the Thales Exporter Entity can prove that the Thales Importer Entity is not responsible for the event giving rise to the damage, the Thales Exporter Entity may discharge itself from any responsibility.

10. DATA SUBJECTS' RIGHTS

10.1 DATA SUBJECTS' RIGHTS

Each Data Subject benefits from the following rights:

- **Right of access:** right to obtain from the Data Controller confirmation as to whether or not Personal Data concerning him/her are being processed and, where that is the case, access to the Personal Data and information provided for by Article 15 of the GDPR;
- **Right to rectification:** right to obtain from the Data Controller (i) rectification of inaccurate Personal Data concerning him/her and (ii) that incomplete Personal Data be completed;
- **Right to erasure:** right to obtain from the Data Controller the erasure of Personal Data concerning him/her where one of the grounds provided for by Article 17 of the GDPR applies;
- **Right to restriction of Processing:** right to obtain from the Data Controller restriction of the Processing where one of the elements mentioned in article 18 of the GDPR applies;
- **Right to data portability:** right to receive the Personal Data concerning him/her, which he/she has provided to the Data Controller, in a structured, commonly used and machine-readable format, if the Processing is carried out by automated means and is based on the consent of the Data Subject or on a contract to which the Data Subject is party;
- **Right to object:** right to object at any time to Processing of Personal Data concerning him/her which is based on the legitimate interest pursued by the Data Controller or a Third Party. Thales shall then no longer process the Personal Data, unless Thales demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims. Where Personal Data are processed for direct marketing purposes, the Data Subject shall also have the right to object at any time to Processing of Personal Data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes;
- **Right not to be subject to decision based solely on automated Processing** (including profiling) which produces legal effects concerning him/her and which significantly affects him/her in accordance with the conditions laid down in Article 22 of the GDPR.

Where Thales acts as Data Processor and where it receives such requests of Data Subjects to exercise their rights, Thales shall communicate the requests without delay to the Data Controller, so that the latter can process the request. Thales shall only be responsible to comply with the Data Controller's instructions as to how to answer such request.

Where the Data Controller has disappeared factually or has ceased to exist in law or became insolvent and that no other entity has assumed the legal obligations of the Data Controller, Thales shall then handle such request directly, to the extent possible and in accordance with the procedure defined under Appendix 9.

10.2 THIRD-PARTY BENEFICIARY RIGHTS AND RIGHT TO LODGE A COMPLAINT

Data Subjects are able to enforce the provisions of the BCR-P, as listed hereinafter, as third-party beneficiaries, directly against the concerned Thales Entity acting as Data Processor where the requirements at stake are specifically directed to Data Processors in accordance with the GDPR:

- Sections 3, 4, 5, 8, 13 and 14 of the BCR-P: duty to respect the instructions from the Data Controller regarding the Personal Data Processing, including for Personal Data Transfers to Third Countries; duty to implement appropriate technical and organizational security measures; duty to cooperate with and assist the Data Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights;
- Section 6 of the BCR-P: duty to notify any Personal Data Breach to the Data Controller;
- Section 7 of the BCR-P: duty to respect the conditions when engaging a Sub-Processor whether the Sub-Processor is a Thales Entity or a Third Party;

- Sections 9 and 10 of the BCR-P: principles relating to liability, compensation and jurisdiction;
- Sections 11 and 12 of the BCR-P: right to complain through internal complaint mechanism;
- Section 16 of the BCR-P: duty to cooperate with Data Protection Authorities;
- Section 17 of the BCR-P: easy access to the BCR-P and national legislation preventing respect of the BCR-P.

Where Thales acts as Data Processor, Data Subjects shall in the first instance exercise their rights regarding the Processing of their Personal Data against Thales Client.

However, where the Client has factually disappeared or no longer exist in law or has become insolvent and that no other entity has assumed the legal obligations of the Client, Data Subjects shall be able to enforce the following sections of the BCR-P as third-party beneficiaries:

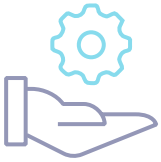
- Section 1: INTRODUCTION
- Section 2: SCOPE OF APPLICATION
- Section 3: BINDING STATUS
- Section 4: BASIC PRINCIPLES WHEN PROCESSING PERSONAL DATA
- Section 5: PROCESSING OF SENSITIVE PERSONAL DATA
- Section 6: PERSONAL DATA BREACH
- Section 7: PROCESSING BY THIRD PARTIES OR BY INTERNAL DATA PROCESSOR
- Section 8: TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS
- Section 9: LIABILITY
- Section 10: DATA SUBJECTS' RIGHTS
- Section 11: DATA SUBJECTS' REQUEST HANDLING PROCEDURE
- Section 12: DATA SUBJECTS' COMPLAINT HANDLING PROCEDURE
- Section 13: PRIVACY BY DESIGN / PRIVACY BY DEFAULT
- Section 14: DATA PROTECTION IMPACT ASSESSMENT
- Section 15: RECORD OF PROCESSING ACTIVITIES
- Section 16: COOPERATION WITH DATA PROTECTION AUTHORITIES
- Section 17: TRANSPARENCY
- Section 21: UPDATE OF THE BCR-P
- Appendix 1: LIST OF PURPOSES OF PROCESSING CARRIED OUT BY THALES AS DATA CONTROLLER
- Appendix 2: THALES ENTITIES BOUND BY THE BCR-P AND COUNTRIES OF REGISTRATION

In such a case, Data Subjects are invited to first submit their complaint to Thales within the framework of the amicable settlement procedure mentioned in Section 12 of the BCR-P. However, although Thales encourages amicable settlement, Data Subjects shall be entitled to lodge a complaint directly before the Competent DPA and/or before the competent court, as well as to obtain redress and, where appropriate, receive compensation for any material or non-material damages resulting from such breach.

Data Subjects shall be entitled to bring their claim before the Data Protection Authority of either: (i) the EEA Member State of his/her habitual residence; (ii) the EEA Member State of his/her place of work; or (iii) the EEA Member State where the alleged infringement took place. In addition, Data Subjects shall also be entitled to lodge a complaint before the competent court of the EEA Member State where the Thales Entity has an establishment.

Where a Thales Entity acting as Data Processor and a Data Controller involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from the Thales Entity acting as a Data Processor or from the relevant Data Controller.

11. DATA SUBJECTS' REQUEST HANDLING PROCEDURE



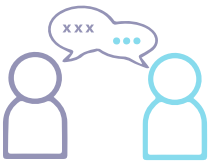
Where a Data Subject addresses a request directly to Thales, acting as Data Processor, but where, after consultation with the relevant department, it is confirmed that the Client has not ceased to exist in law, has not factually disappeared or has not become insolvent (or that another entity has assumed the legal obligations of the Client), the Data Subject's request shall be handled in accordance with the procedure specified in Appendix 9.

Thus, Thales shall have the duty to communicate the request without delay to the Client and Thales shall not take any further action until further instructed by the Client.

In any case, Thales will execute any appropriate technical and organizational measures, insofar as this is possible, when asked by its Client, for the fulfilment of the Client's obligations to respond to requests for exercising the data subjects rights including by communicating any useful information. Such assistance shall be handled by the relevant Data Protection Correspondent. Thales shall ensure that it communicates all relevant information it receives from the Data Subject to the Client and shall expressly inform the Client of its responsibility to handle such request.

However, where the Client has factually disappeared or no longer exist in law or has become insolvent and that no other entity has assumed the legal obligations of the Client, Thales shall handle requests from Data Subjects, to the extent possible, without undue delay and in any event within one month of receipt of the request. Taking into account the complexity and number of the requests, that one (1) month period may be extended at maximum by two (2) further months, in which case the Data Subject should be informed accordingly within one (1) month of receipt of the request, together with the reasons for the delay. In this respect, Thales shall apply the procedure defined under Appendix 9.

12. DATA SUBJECTS' COMPLAINT HANDLING PROCEDURE



Without prejudice to Section 10 above, Data Subjects may lodge their complaint directly before Thales.

In such case, Thales, acting as Data Processor, commits to handle such complaints without undue delay, with particular care and attention and in any event within one (1) month of receipt of the request, as identified under an internal handling procedure described in Appendix 10. Taking into account the complexity and number of the requests, that one (1) month period may be extended at maximum by two (2) further months, in which case the Data Subject shall be informed accordingly within one (1) month of receipt of the request, together with the reasons for the delay.

Data Subjects are duly informed of the complaint handling procedure and how to file a complaint through the BCR-P and privacy information notices published by Thales on the Thales website, the Thales intranet, the concerned application and/or any other media defined by Thales.

The procedure by which a Data Subject may file a complaint is set out as follows:

- preferably by sending an e-mail to the specific data protection mailbox which address is mentioned in the privacy notice applicable to the concerned processing tool, application, intranet or internet site or by filling in the specific form made available by Thales if any;
- alternatively, by sending an e-mail to the dedicated data protection mailbox set up by the Group Data Protection Officer at dataprotection@thalesgroup.com.

The Group Data Protection Officer and the Thales S.A. Data Protection team are in charge of supervising the handling of complaints by Data Subject(s). They are granted an appropriate level of independence to advise the relevant Thales Entities and deal with such complaints.

Regardless of whether the internal complaint process has been exhausted or not and if the Data Subject remains unsatisfied, the Data Subject has the right to lodge a claim before the before the Competent DPA and/or competent court as per Section 10.2 hereabove.

If the complaint is justified, Thales will implement the relevant measures it deems adequate to remedy the failure.

13. PRIVACY BY DESIGN / PRIVACY BY DEFAULT

As demonstrated by the commitments taken under the BCR-P, Thales is committed to provide a high level of protection to the Personal Data it processes.

Where it is acting as Data Processor, Thales shall assist its Client in implementing appropriate technical and organizational measures to comply with the principles of "Privacy by Design" and "Privacy by Default".

14. DATA PROTECTION IMPACT ASSESSMENT

Where it acts as Data Processor, Thales may be required by the Client to cooperate and provide relevant information to enable the Client to conduct a Data Protection Impact Assessment. Whilst respecting any contractual commitments taken vis-à-vis Clients, Thales shall make sure that it provides reasonable assistance to the Client.

15. RECORD OF PROCESSING ACTIVITIES

For the Processing subject to the GDPR, Thales commits to maintain a Record of Processing activities carried out on behalf of its Clients, up to date, in line with the requirements of the GDPR.

Where Thales is acting as Data Processor, the Record shall include all of the following:

- the name and contact details of the Thales Entity acting as Data Processor and of the Group Data Protection Officer;
- the name and contact details of each Client acting as Data Controller on behalf of which Data Processor is acting;
- the name and contact details of any Sub-Processor;
- the categories of Processing carried out on behalf of each Client;

- the Transfers of Personal Data to any Third Country outside the EEA or to an international organization, including the identification of that Third Country or international organization and the documentation of suitable safeguards;
- where possible, a general description of the technical and organizational security measures referred to in the GDPR.

Thales shall be responsible for making sure that any new Processing is recorded in the Record with relevant information regarding the context of Processing.

The Record is maintained in electronic form, and shall be made available to the Competent DPA on request.

16. COOPERATION WITH DATA PROTECTION AUTHORITIES

Thales is committed to maintain good relationships with Data Protection Authorities. For this purpose, Thales shall cooperate with and accept to be audited by the Competent DPA, take into account its opinions and comply with its formal decisions on any issue related to the BCR-P.

Thales undertakes to provide the Competent DPA, upon request, with any information about the Processing covered by the BCR-P.

When Data Protection Authorities conduct investigations within one or several Thales Entities, Thales' internal guidelines shall apply. In accordance with these guidelines, where such investigations take place, the Group Data Protection Officer shall be immediately informed, in particular to coordinate any investigations with the Competent DPA.

Any dispute related to the Competent DPAs' exercise of supervision of compliance with the BCR-P will be resolved by the courts of the Member State of that Competent DPA, in accordance with that Member State's procedural law. The Thales Entities agree to submit themselves to the jurisdiction of these courts.

17. TRANSPARENCY

17.1 REGARDING DATA SUBJECTS

By willing to adopt an approach to compliance when Processing Personal Data, Thales expressly intends to communicate about its approach. In this context, Thales shall publish a public version of these BCR-P and commits to communicate them (as well as any other specific policies related to Personal Data protection applicable to relevant products and services) to the Data Subjects whose Personal Data are processed by Thales and to make them easily accessible by publishing them on the intranet for Thales employees and on its website for other Data Subjects.

In any event, the public version of the BCR-P available on Thales website will contain the following Sections of the BCR-P:

- Section 1: INTRODUCTION
- Section 2: SCOPE OF APPLICATION
- Section 3: BINDING STATUS
- Section 4: BASIC PRINCIPLES WHEN PROCESSING PERSONAL DATA
- Section 5: PROCESSING OF SENSITIVE PERSONAL DATA
- Section 6: PERSONAL DATA BREACH
- Section 7: PROCESSING BY THIRD PARTIES OR BY INTERNAL DATA PROCESSOR

- Section 8: TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS
- Section 9: LIABILITY
- Section 10: DATA SUBJECTS' RIGHTS
- Section 11: DATA SUBJECTS' REQUEST HANDLING PROCEDURE
- Section 12: DATA SUBJECTS' COMPLAINT HANDLING PROCEDURE
- Section 13: PRIVACY BY DESIGN / PRIVACY BY DEFAULT
- Section 14: DATA PROTECTION IMPACT ASSESSMENT
- Section 15: RECORD OF PROCESSING ACTIVITIES
- Section 16: COOPERATION WITH DATA PROTECTION AUTHORITIES
- Section 17: TRANSPARENCY
- Section 18 : TRAINING
- Section 19: AUDIT
- Section 20: PERSONAL DATA PROTECTION ORGANISATION
- Section 21: UPDATE OF THE BCR-P
- Appendix 1: LIST OF PURPOSES OF PROCESSING CARRIED OUT BY THALES AS DATA CONTROLLER
- Appendix 2: LIST OF THE REGISTERED COUNTRIES OF THE THALES ENTITIES BOUND BY THE BCR-C

17.2 REGARDING LAWS PREVENTING RESPECT OF THE BCR-P AND GOVERNMENT ACCESS REQUESTS

Where a Thales Entity acting as Data Processor has reasons to believe that the legislation applicable to it is likely to prevent it from fulfilling the instructions received from the Data Controller or its obligations under the BCR-P or under the Agreement entered into with the Client, it will promptly inform (i) the Data Controller which will be then entitled to suspend the Transfer of Personal Data and/or terminate the Agreement in accordance with the terms of said Agreement, (ii) the Group Data Protection Officer and, where appropriate, the relevant Data Protection Correspondent(s) (ii) Thales S.A, (iv) the Competent DPA for the Data Controller, and (v) the Competent DPA for the Data Processor.

Any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body shall be communicated to the Data Controller, unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the Data Protection Authority competent for the Data Controller and the Data Protection Authority competent for the Data Processor should be expressly informed about the request, including information about the Personal Data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited).

If, in specific cases, the suspension and/or notification are prohibited, the concerned Thales entity, acting as Data Processor, shall use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate it did so.

If, in the above cases, despite having used its best efforts, the Thales entity is not in a position to notify the competent Data Protection Authorities, it shall annually provide to the competent Data Protection Authorities general information on the requests it received (e.g., number of applications for disclosure, type of Personal Data requested, requester if possible).

In any case, Transfers of Personal Data by a Thales Entity to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

17.3 REGARDING CLIENTS

Where it is acting as Data Processor, Thales shall provide its Clients with relevant information which shall enable the Clients to provide an information notice to Data Subjects.

In addition, Thales shall ensure that the BCR-P are part of the Agreement concluded with Thales Clients, by means of a reference or a link granting electronic access thereto.

18. TRAINING

Thales ensures that the BCR-P are effectively applied within the organization. For this purpose, Thales has adopted a data protection training program which aims to ensure that Thales' employees are aware about the principles and procedures defined by the BCR-P.

The training program aims at providing Thales' employees with:

- a common core of knowledge regarding the applicable principles when Processing Personal Data;
- a good understanding of the existing procedures and when and how they shall apply;
- a specific training adapted to the different functions within the organization.

This training program will, in particular, aim at ensuring that proper training is provided to the employees that have permanent or regular access to Personal Data or that are involved in the collection of Personal Data or in the development of tools used to process Personal Data.

In addition, Thales is also committed to maintain the culture of Personal Data protection within the organization. For this purpose, some specific actions, such as providing webinars on specific key topics or guidelines, will be implemented.

The proposed training program is further developed under Appendix 11 of the BCR-P.

19. AUDIT

Thales commits to perform audits in relation to Personal Data protection, on a regular basis, by internal or external accredited auditors, or at the express request of the Group Data Protection Officer or, where appropriate, Data Protection Correspondents, in order to verify that Personal Data protection complies with the BCR-P.

Scheduled global audits (on site or remote), including audits with respect to the general compliance of Thales with the BCR-P shall be performed on a regular basis (every 3 years for Processing carried out by the Thales Entities).

For this purpose, Thales has implemented an audit plan that covers all aspects of the BCR-P, including methods to ensure the implementation of corrective measures.

The audit plan defines:

- a reasonable calendar according to which audits shall be carried out;
- the proposed scope of audits;
- the team in charge of audits.

The results of the audit shall be communicated to the Group Data Protection Officer (and, where appropriate, to the members of the Personal Data Protection Organization), to the board of the relevant Thales Entity and, where appropriate, to the board of Thales S.A. Corrective measures shall be defined with a prioritization enabling the Group Data Protection Officer and, where appropriate, the members of the Personal Data Protection Organization to determine a schedule for the implementation of such measures.

The Competent DPA can have access to the results of the audit upon request.

The audit plan referred to under this Section is further described under Appendix 5.

20. PERSONAL DATA PROTECTION ORGANIZATION

The implementation of the BCR-P requires that all Thales Entities and employees are involved in the compliance with requirements in terms of Personal Data protection. Thales shall ensure that it relies on an organized Personal Data protection community, gathering Thales' employees which shall be responsible for the effective implementation of the BCR-P.

In this context, Thales has implemented a Personal Data Protection Organization and has appointed, in particular, a Group Data Protection Officer, relying on a network of Data Protection Correspondents and Data Protection Referees, as further described under Appendix 12. The Group Data Protection Officer directly reports to the highest management level.

The main responsibility of the Group Data Protection Officer is to monitor that Thales Entities comply with the provisions of the BCR-P and with the Applicable Personal Data Protection Legislation. The Group Data Protection Officer shall enjoy the highest management support in exercising this function.

More specifically, the Group Data Protection Officer is in charge of:

- defining the Thales group's general data protection policy, the procedures to be met and the control measures to be implemented for the efficient protection of Personal Data;
- regularly informing senior management as to the status of and the compliance with the BCR-P;
- responding to requests and complaints made by Data Subjects and assessing the collection and use of Personal Data by Thales Entities in terms of potential risks relating to data protection;
- determining and implementing procedures to handle situations of non-compliance;
- setting up an effective organization to notify the Competent DPA of any Personal Data Breach, as well as the Data Subjects, and defining the action plan;
- permanently monitoring the correct application of internal rules, procedures and guidelines relating to the protection of Personal Data;
- centralizing the results of monitoring and audits regarding the implementation of the BCR-P in order for the Competent DPA to access them in the event of investigations;
- being the dedicated point of contact for the Data Protection Authorities on matters relating to Processing carried out by Thales.

The Group Data Protection Officer does not bear any tasks that can result in conflict of interests. The Group Data Protection Officer is not in charge of carrying out Data Protection Impact Assessments, neither he is in charge of carrying out the BCR-P audits if such situations can result in a conflict of interests. However, the Group Data Protection Officer can play a very important and useful role in assisting the Thales Entities, and the advice of the Group Data Protection Officer should be sought for such tasks.

The Group Data Protection Officer can directly be contacted by sending an e-mail at **dataprotection@thalesgroup.com**. This e-mail address is mentioned in all Thales privacy notices.

21. UPDATE OF THE BCR-P

The BCR-P have to be kept up-to-date in order to reflect the current situation (for instance to take into account modifications of the regulatory environment, European Data Protection Board Recommendations, or changes to the scope of the BCR-P).

The Group Data Protection Officer shall keep a fully updated list of the Thales Entities bound by the BCR-P, keep record of any updates to the BCR-P, and provide the necessary information to Data Subjects, and, upon request, to Competent DPAs.

Where a modification to the BCR-P would possibly be detrimental to the level of the protection offered by the BCR-P or significantly affect them (e.g. changes to the binding character), it must be communicated in advance to the Competent DPAs, via the Lead Supervisory Authority, with a brief explanation of the reasons for the update. In this case, the Competent DPAs will also assess whether the changes made require a new approval.

Once a year, the Competent DPAs should be notified via the Lead Supervisory Authority of any changes to the BCR-P or to the list of the Thales Entities, with the brief explanation of the reasons for the changes. The Competent DPAs should also be notified once a year in instances where no changes have been made.

The annual update or notification should also include the renewal of the confirmation regarding assets as per Section 9 here above.

Amendments which would possibly affect the level of protection offered by the BCR-P or significantly affect the BCR-P (i.e. changes to the binding character) must also be promptly communicated:

- to each Thales Entity bound by the BCR-P (including Internal Clients);
- to Thales' employees;
- to Data Subjects in relation to which Thales is acting as Data Controller.

Communication regarding such changes shall be made to enable Data Subjects to acknowledge such amendment and take necessary actions where required.

It remains the responsibility of the Group Data Protection Officer to keep the BCR-P up-to-date and in compliance with Article 47 GDPR and the EDPB Recommendations.

APPENDIX 1
LIST OF PURPOSES OF PROCESSING CARRIED OUT BY THALES AS DATA PROCESSOR

1. Collection and processing of license plates in order to provide a service intended to calculate journey times pursuant to a contract under which Thales acts as a Data Processor or to calculate parking times in order to enable payment.

2. Data collection and processing by Thales on behalf of its customers in order to have contact details to use in case of emergency.

3. Data collection and processing in order to implement a tracking application of carried items.

4. Data processing within the framework of outsourcing, hosting and administration of IT systems, security and cloud services provided by Thales to its customers.

5. Data processing relating to the placing of convicted persons under electronic monitoring in accordance with a contract Thales is part of.

6. Data collection and processing resulting from photographs and reports made within the framework of air surveillance programs.

7. Data processing resulting from development, technical support and maintenance operations carried out on behalf of customers pursuant to a contract.

8. Processing in order to provide technical support and maintenance services to customers of monitoring and navigation systems.

9. Processing intended to ensure the organization, follow-up and performance of training sessions provided by Thales to its customers as a Data Processor.

10. Processing for surveillance, protection and incident prevention purposes implemented on behalf of customers.

11. Data collection and processing by Thales on behalf of its airline customers in order to provide services to such airlines.

12. Data collection and processing by Thales on behalf of its airlines customers in order to provide personalized services to the end customers.

13. Data collection and processing by Thales on behalf of its customers implying aggregation and redistribution of data to its customers or to third parties designated by its customers.

14. Processing for the purpose of adapting and setting up products in accordance with the customers' needs.

15. Processing of personal data for digital payment and banking services' management.

16. Processing of personal data for ID verification and biometric recognition.

17. Processing of personal data for identity, authentication, access and risk management.

18. Processing of personal data to connect devices to cellular networks.

19. Processing of personal data for software licensing solutions.

20. Processing of personal data for supply and personalization of government issued documents, health cards, banking cards, digital cards and smart cards.

21. Processing of personal data to provide device location services.

22. Processing of personal data to remotely administrate subscriber's SIM cards and customers' devices in a secure manner.

23. Processing of personal data to make marketing campaigns towards end-users.

24. Data processing resulting from the production of document management products.

APPENDIX 2
THALES ENTITIES BOUND BY THE BCR-P AND COUNTRIES OF REGISTRATION

Appendix 2.1 : List of Thales Entities

Click here to access the list of Thales Group locations.

Appendix 2.2 : List of countries where Thales Entities bound by the BCR are established

Countries in the European Economic Area	Countries outside the European Economic Area
Austria	Algeria
Belgium	Argentina
Czech Republic	Australia
Denmark	Bahrein
Finland	Bolivia
France	Brazil
Germany	Cameroun
Greece	Canada
Hungary	Chile
Italy	China
Luxembourg	Colombia
Netherlands	Egypt
Norway	Hong-Kong
Poland	India
Portugal	Indonesia
Romania	Israel
Spain	Ivory Coast
Sweden	Japan
	Kazakhstan
	KSA
	Lebanon
	Malaysia

Countries in the European Economic Area	Countries outside the European Economic Area
	Mauritius
	Mexico
	Morocco
	New-Zealand
	Nigeria
	Oman
	Pakistan
	Philippines
	Qatar
	Russia
	Senegal
	Singapore
	South Africa
	Switzerland
	Taiwan, Province de Chine
	Thailand
	Turkey
	United Arab Emirates
	United Kingdom
	United States
	Venezuela

APPENDIX 3
THALES INTRA-GROUP AGREEMENT

This document is a confidential document for Thales internal use only.

APPENDIX 4
THALES EMPLOYEES INFORMATION AND BINDINGNESS

This document is a confidential document for Thales internal use only.

APPENDIX 5
AUDIT PLAN

This document is a confidential document for Thales internal use only.

APPENDIX 6
THALES GROUP INFORMATION SECURITY POLICY

This document is a confidential document for Thales internal use only.

APPENDIX 7
CRISIS MANAGEMENT CHECKLIST

This document is a confidential document for Thales internal use only.

APPENDIX 8
TRANSFER IMPACT ASSESSMENT

This document is a confidential document for Thales internal use only.

APPENDIX 9
DATA SUBJECTS REQUEST HANDLING PROCEDURE

This document is a confidential document for Thales internal use only.

APPENDIX 10
DATA SUBJECTS COMPLAINT HANDLING PROCEDURE

This document is a confidential document for Thales internal use only.

APPENDIX 11
TRAINING PROGRAM

This document is a confidential document for Thales internal use only.

APPENDIX 12
THALES PERSONAL DATA PROTECTION ORGANIZATION

This document is a confidential document for Thales internal use only.

LOG OF CHANGES

Revision	Date	Modification
001	05/2024	Update as per request of French Lead Supervisory Authority in its decision of approval No.2023-145 dated 21st December 2023.
002	10/2024	Update of Appendix 2 "*Thales entities bound by the BCR-P*".
003		

THALES

Building a future we can all trust

Thales
Campus Meudon
4 rue de la Verrerie
92190 Meudon
France

thalesgroup.com