BINDING CORPORATE RULES

THALES AS DATA CONTROLLER (BCR-C)

Public Version

THALES
Building a future we can all trust

TABLE OF CONTENTS

1	INTRODUCTION	3
2	SCOPE OF APPLICATION	6
3	BINDING STATUS	7
4	BASIC PRINCIPLES WHEN PROCESSING PERSONAL DATA	8
5	PROCESSING OF SENSITIVE PERSONAL DATA	9
6	PERSONAL DATA BREACH	10
7	PROCESSING BY THIRD PARTIES OR BY INTERNAL DATA PROCESSOR	11
8	TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS	12
9	LIABILITY	14
10	DATA SUBJECTS' RIGHTS	14
11	DATA SUBJECTS REQUEST HANDLING PROCEDURE	16
12	DATA SUBJECTS COMPLAINT HANDLING PROCEDURE	16
13	PRIVACY BY DESIGN / PRIVACY BY DEFAULT	17
14	DATA PROTECTION IMPACT ASSESSMENT	17
15	RECORD OF PROCESSING ACTIVITIES	18
16	COOPERATION WITH DATA PROTECTION AUTHORITIES	19
17	TRANSPARENCY	19
18	TRAINING	21
19	AUDIT	22
20	PERSONAL DATA PROTECTION ORGANIZATION	22
21	UPDATE OF THE BCR-C	23

APPENDICES

1	LIST OF PURPOSES OF PROCESSING CARRIED OUT BY THALES AS DATA CONTROLLER	25
2	THALES ENTITIES BOUND BY THE BCR-C AND COUNTRIES OF REGISTRATION	29
3	THALES INTRA-GROUP AGREEMENT	31
4	THALES EMPLOYEES INFORMATION AND BINDINGNESS	31
5	AUDIT PLAN	31
6	THALES GROUP INFORMATION SECURITY POLICY	31
7	CRISIS MANAGEMENT CHECKLIST	32
8	TRANSFER IMPACT ASSESSMENT	32
9	DATA SUBJECTS' REQUEST HANDLING PROCEDURE	32
10	DATA SUBJECTS' COMPLAINT HANDLING PROCEDURE	32
11	DATA PROTECTION IMPACT ASSESSMENT	32
12	TRAINING PROGRAM	32
13	THALES PERSONAL DATA PROTECTION ORGANIZATION	32

1. INTRODUCTION

1.1 OBJECTIVES OF THE BCR

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 defense, aeronautics, space and digital identity and security markets to fulfill 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.

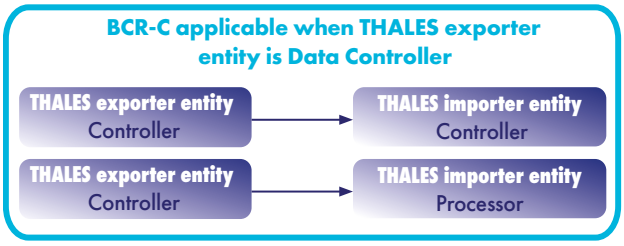
The BCR are designed to be used as Thales global data protection policy.

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

1.2 THE BCR-C ("CONTROLLER")

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

The BCR-C are suitable for framing transfer of personal data from a Thales Entity acting as data controller and covered by the geographical scope of the GDPR pursuant to its Article 3 to another Thales entity, acting as data controller or internal data 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-C describe how Thales will meet those measures. Where the GDPR contains principles, the BCR-C 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-C.

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-C.

1.3 KEY DEFINITIONS AND ACRONYMS

"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-C, 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-C.

"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., employees, providers' contact points).

"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.

"Intra-Group Agreement" refers to the intra-group agreement according to which the Thales Entities are bound by the BCR-C. A template of said Intra-Group Agreement is attached hereto in Appendix 3.

"Intra-Group Products and Services Agreement" refers to a specific intra-group agreement signed between Thales Entities for the supply of products and/or services and/or granting of license, as per Thales internal Intra Group Trading Rules (IGTR) template.

"Internal Client" refers to any Thales Entity acting as Data Controller, for which another Thales Entity processes Personal Data in the frame of an Intra-Group Products and Services Agreement implying Personal Data Processing.

"Internal Data Processor" refers to a Thales Entity acting as Data Processor on behalf and under the instructions of another Thales Entity acting as Data Controller.

"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.

"Thales" (or **"Thales Entity(ies)"**) refers to Thales S.A. and/or Thales Affiliates bound by the BCR-C, 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 Exporter Entity" refers to any Thales Entity covered by the geographical scope of the GDPR pursuant to Article 3 of the GDPR and exporting Personal Data on the basis of the BCR-C to a Thales Importer Entity established in a Third Country i.e. a country outside the EEA 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 of the GDPR, and receiving Personal Data from a Thales Exporter Entity on the basis of the BCR-C.

"Thales S.A." refers to Thales SA, 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-C 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-C shall apply when a Thales Entity is acting as a Data Controller and thus processes Personal Data on its own behalf (when it determines the purposes and means of Processing of Personal Data).

The BCR-C shall also apply when a Thales Entity is acting as an Internal Data Processor on behalf and under the instructions of another Thales Entity acting as Data Controller.

Thales acknowledges that its status as Data Controller or Internal 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-C 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-C.

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

- Thales' employees, including Thales' salaried employees, representatives and officers, as well as Thales' former employees and family members of Thales employees;
- Thales' temporary workers and interns;
- Thales' job applicants;
- Employees and contact points of Thales' clients and prospects;
- Employees and contact points of Thales' partners, services providers, suppliers, distributors and subcontractors;
- Users and administrators of Thales applications;
- Users and administrators of Thales websites;
- Users of Thales' products and services; and
- Other natural persons (for example volunteers in case of R&D experimentations and products & services' testing, plaintiffs in case of litigation, visitors of Thales sites...).

2.2.4 The list of purposes covered by the BCR-C is provided in Appendix 1, with details on relevant categories of Data Subjects and Personal Data processed for each purpose. Appendix 1 may be updated from time to time according to Section 21 of the BCR-C.

2.2.5 The types of Personal Data Processing covered by the BCR-C 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 where Personal Data are Transferred to 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-C 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.

The BCR-C 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 another Thales Importer Entity in a Third Country.

3. BINDING STATUS

3.1 BINDINGNESS AMONGST THALES ENTITIES

The BCR-C are legally binding for Thales Entities irrelevant of their localization.

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

In practice, in order to be bound by the BCR-C, each Thales Entity shall sign the Intra-Group Agreement attached in Appendix 3 hereto. By signing said Intra-Group Agreement, each Thales Entity commits to comply with the provisions of the BCR-C 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-C 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-C, and can benefit from the rights granted under the BCR-C.

The BCR-C 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-C shall expose employees to disciplinary sanctions.

4. BASIC PRINCIPLES WHEN PROCESSING PERSONAL DATA

The GDPR defines a set of principles which shall be respected when Processing Personal Data. Each Thales Entity shall be responsible for and be able to demonstrate its compliance with the BCR-C. Therefore, the operational team in charge of the deployment of a Processing, with the help of the relevant Data Protection Correspondent, shall ensure that the principles below are complied with.

4.1 PURPOSE

Thales shall not process any Personal Data without a reason for doing so. Hence, prior to starting any Processing of Personal Data, Thales shall first ensure that it defines a purpose for such Processing. It means that Thales shall ensure that it does not process Personal Data without any reason or for prospective undefined reasons. Such purpose shall not only be defined, it shall as well be lawful and legitimate. In other words, Thales shall ensure that the Personal Data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The list of purposes covered by the BCR-C is provided in Appendix 1 which may be amended from time to time.

4.2 LEGAL BASIS

It is essential when Processing Personal Data to ensure that such Processing relies on a legal basis, as provided for by the GDPR.

Thus, subject to the specific principles applicable to Sensitive Data, as outlined in Section 5, Thales may process Personal Data only if one of the criteria defined below is met.

Where the Processing of Personal Data by Thales results from the performance of the contract concluded with the Data Subject (either an employment contract, a customer contract or another type of contract, for instance a supplier contract), the Processing would be deemed lawful.

Where the Processing does not result from the performance of a contract, the Thales Entity acting as Data Controller shall demonstrate that it has a legitimate interest in the Processing. To determine whether Thales can validly rely on the legitimate interest basis, it shall apply the so-called "balancing test" as specified by the European Data Protection Board in its recommendations. Thales must therefore demonstrate that the purpose is legitimate for Thales in light of its core business and of EEA or EEA Member State law, and shall also demonstrate that the said Processing does not have a negative impact on Data Subjects' privacy.

Besides, the Processing of Personal Data could be legitimized by the mere fact that Thales shall comply with a legal obligation in EEA or EEA Member State law it is subject to (Health, Safety, and Environmental requirements, billing requirements...).

Where the Processing contemplated by Thales would not fall under one of the above listed legal basis, Thales could seek to obtain Data Subjects' prior consent, provided that it respects the cumulative conditions for a valid consent. It means that consent shall be:

- given by a clear affirmative act;
- freely given; and
- a specific, informed and unambiguous indication of the Data Subject's agreement to the Processing of Personal Data relating to him/her.

It should be noted that Processing of Personal Data by Thales is also lawful where the Processing is necessary to save the vital interest of the Data Subject (e.g., when Personal Data need to be communicated to the rescue department when an employee has a problem at the office).

4.3 PERSONAL DATA MINIMISATION

Thales shall ensure that it will collect and retain only the Personal Data strictly necessary in relation to the purposes for which they are processed.

4.4 PERSONAL DATA QUALITY

Thales shall make sure that, during the entire life cycle of a Processing, the Personal Data remain accurate and up to date. Thales has implemented an audit plan as further described under Section 19 and Appendix 5.

4.5 PERSONAL DATA LIMITED STORAGE PERIODS

Thales shall ensure that it does not keep the Personal Data for longer than strictly necessary for the purpose for which the Personal Data are collected. Thales shall first determine the Personal Data's storage period required for such purpose and further conduct a balancing test between:

- the time during which the Personal Data are necessary for Thales' interest;
- the period after which keeping such Personal Data may have an impact on Data Subjects' rights to be forgotten; and
- other legal obligations which may impose minimum Personal Data storage period.

Thales shall determine the balanced Personal Data's storage period before implementing the Processing in order to ensure that deletion occurs in a timely manner in accordance with Applicable Personal Data Protection Legislation. Thales has in place a Personal Data's retention policy and guidelines in the various jurisdictions to support the operational team in determining the appropriate storage period and such storage periods are communicated accordingly in the relevant information notices.

4.6 SECURITY MEASURES

As further described under Thales internal Group Information security policy in Appendix 6, Thales has implemented security measures to protect its information system. When Processing Personal Data, particular attention needs to be paid and appropriate technical and organizational measures are needed to ensure that Personal Data are not unlawfully accessed and/or processed. The Thales above mentioned security policy specify the security requirements to be implemented for any Personal Data Processing.

Where the security measures are breached or where a Personal Data Breach occurs, Thales shall comply with its Personal Data Breach's procedure, as further described under Section 6 of the BCR-C.

4.7 LAWFULNESS, FAIRNESS AND TRANSPARENCY

Thales commits to process Personal Data lawfully, fairly and in a transparent manner.

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.

Thales will process Sensitive Personal Data in very limited cases, in particular in relation to its employees.

Where it intends to process Sensitive Personal Data on its own behalf, Thales shall ensure that:

- the Data Subject has given his/her explicit consent; or
- where the Data Subject is not in a position to give his/her consent (e.g. medical emergency), the Processing is necessary to protect the vital interests of the Data Subject or of another person; or
- the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by European Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject; or
- the Processing is necessary for the purposes of preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or management of health or social care systems and services on the basis of EEA or EEA Member State law or pursuant to a contract entered into with a health professional (e.g., medical examination in the context of a recruitment); or
- the Data Subject has already manifestly placed the concerned Sensitive Personal Data in the public domain; or
- the Processing is essential for the purpose of establishing, exercising or defending legal claims, provided that there are no ground to assume that the Data Subject has an overriding legitimate interest in not having the Personal Data processed; or
- the Processing is necessary for reasons of substantial public interest, on the basis of European Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject; or
- the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR based on European Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject; or
- the Processing is otherwise explicitly permitted by Applicable Personal Data Protection Legislation.

6. 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 shall immediately inform the Group Data Protection Officer and where appropriate Thales S.A.

Unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons, the Group Data Protection Officer shall notify such Personal Data Breach to the Competent DPA, without undue delay and, where feasible, not later than 72 (seventy-two) hours after Thales becomes aware of it, in accordance with the Thales crisis management checklist in Appendix 7.

In such case, Thales shall also determine whether it needs to communicate the Personal Data Breach to the Data Subjects affected. If the assessment leads to the conclusion that the breach is likely to result in a high risk to the Data Subjects' rights and freedoms, Thales shall communicate such breach to the Data Subjects, without undue delay, in accordance with the procedure defined under the Thales crisis management checklist in Appendix 7.

In any event, in case of a Personal Data Breach, Thales undertakes to document any such Personal Data Breach and to make the said documentation available to the Competent DPA on request of the latter.

7. PROCESSING BY THIRD PARTIES OR BY INTERNAL DATA PROCESSOR

Although each Thales Entity is able to rely on its own resources and information system, Thales Entities may also rely on a Thales Internal Data Processor or a Third Party.

Where communication of Personal Data to an Internal Data Processor or to a Third Party takes place, a contract relating to Personal Data Processing (or provisions relating to Personal Data protection to be inserted in the contract) shall be entered into, specifying the respective obligations of the stakeholders taking part to the Processing. Where a Thales Entity acting as Data Controller relies on another Thales Entity acting as Internal Data Processor, such contract or clauses shall be included in an Intra-Group Products and Services Agreement signed between both Thales Entities.

In such case, the Thales Entity acting as Data Controller shall make sure that it relies on a template of Personal Data protection clause it has adopted and shall negotiate any amendment to these clauses taking into account the following commitments.

Where Thales acts as Data Controller and needs to rely on a Third Party acting as Data Processor or any other Thales Entity acting as Internal Data Processor, Processing Personal Data on behalf of Thales, Thales shall ensure that the Third Party acting as Data Processor or the concerned Thales Entity acting as Internal Data Processor:

- implements procedures to ensure that it complies with the Thales Entity acting as Data Controller's instructions, notably regarding the deletion and/or restitution of Personal Data;
- maintains a Record of all categories of Processing activities carried out on behalf of Thales Entity acting as Data Controller in accordance with the BCR-C and the Applicable Personal Data Protection Legislation;
- commits to have its personnel and its providers comply with Applicable Personal Data Protection Legislation, with the same obligations as the ones defined hereunder and with reinforced confidentiality obligations by ensuring that they enter into specific confidentiality agreement;
- implements organizational and technical measures to ensure that Personal Data are not unlawfully accessed and/or processed;
- commits to have its personnel and the personnel of its sub-processors duly trained on their obligations when Processing Personal Data;
- implements a procedure to ensure that it informs Thales Entity acting as Data Controller without undue delay about Data Subjects' requests and/or complaints it may receive in relation to the Processing of Personal Data. In any case, the Third Party or the concerned Thales Entity Processing Personal Data on behalf of Thales shall refrain from reverting to Data Subjects without Thales prior written consent;
- allows Thales to perform Personal Data protection audits in relation to the Processing of Personal Data carried out in the context of the agreement entered into between Thales and the Third Party or the Internal Data Processor – such audit shall be carried out by Thales or by an independent inspection body composed of independent members duly appointed by Thales in accordance with the terms stated in the agreement entered into between Thales and the Third Party or the Internal Data Processor;
- commits to audit on a regular basis its providers acting as sub-processors in relation to the Processing of Thales' Personal Data. The Third Party or Internal Data Processor shall then provide to Thales a complete report of the conducted audit to demonstrate that Personal Data are actually processed in accordance with the terms defined and approved by Thales in the agreement entered into with the Third Party or the Internal Data Processor, and in accordance with Thales' instructions;
- actively cooperates with Thales to enable Thales to assess and document the compliance of the Processing of Thales Personal Data as a result of the agreement entered into with the Third Party or Internal Data Processor.

In addition, Thales undertakes to reflect all other information required as set out in Article 28 of the GDPR in its Personal Data Processing agreements concluded with any Third Party or any Internal Data Processor.

Compliance with the above mentioned obligations shall be monitored and implemented by the relevant Thales procurement department, with the help of the relevant Data Protection Correspondent and/or the local legal department.

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

8.1 LOCAL LAWS AND PRACTICES AFFECTING COMPLIANCE WITH THE BCR-C

8.1.1 Transfer Impact Assessment

Before carrying out Transfer of Personal Data to Third Countries, the Thales Exporter Entity and the Thales Importer Entity 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 Thales Importer Entity from fulfilling its obligations under the BCR-C. 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-C.

When conducting the assessment mentioned above, the Thales Entities 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; 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-C, 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 Thales Exporter Entity with relevant information and shall continue to cooperate with the Thales Exporter Entity in ensuring compliance with the BCR-C.

The Thales Exporter Entity and the Thales Importer Entity 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.

8.1.2 Change in protection level / Transfer suspension

The Thales Importer Entity 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. 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-C, the Thales Exporter Entity along with any other liable Thales Entity as per Section 9 hereunder 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 by the Thales Exporter Entity and/or by the Thales Importer Entity to address 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 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-C cannot be complied with and compliance with the BCR-C 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.

8.2 APPROPRIATE SAFEGUARDS ON ONWARD TRANSFERS

Where a Thales Entity, acting as Data Controller (or as Internal Data Processor), carries out an onward Transfer of Personal Data as referred to in Section 2.3 to another Thales Entity established in a Third Country and acting itself as Data Controller (or as Internal Data Processor), such Transfer shall be framed by the provisions of the BCR-C.

Where a Thales Entity, acting as Data Controller (or as Internal Data Processor), carries out an onward Transfer of Personal Data that have been transferred under the BCR-C to a Third Party acting as Data Controller or Data Processor, established in a Third Country, 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, onward 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 onward Transfer of Personal Data takes place shall be defined by the relevant Thales legal department and/or the Data Protection Correspondent.

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 an EEA Member State, without prejudice to other grounds for Transfer pursuant to Chapter V of the GDPR.

8.4 NON-COMPLIANCE

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 exporting Personal Data to a Thales Importer Entity established in a Third Country on the basis of the BCR-C shall accept liability for any breaches of the BCR-C by said Thales Importer Entity. 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-C 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-C, 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 is 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 defense 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.

Thales shall make sure that it handles such requests without undue delay and in accordance with the request handling procedure defined under Section 11.

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

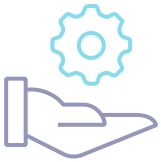
As third party beneficiaries, Data Subjects are conferred rights to enforce the following Sections of the BCR-C:

- 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-C
- Appendix 1: LIST OF PURPOSES OF PROCESSING CARRIED OUT BY THALES AS DATA CONTROLLER
- Appendix 2: THALES ENTITIES BOUND BY THE BCR-C AND COUNTRIES OF REGISTRATION

Where Data Subjects consider that Thales has breached the above listed Sections of the BCR-C, 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-C. 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 the EEA Member State where the Data Controller or Internal Data Processor has an establishment.

11. DATA SUBJECTS' REQUEST HANDLING PROCEDURE



Data Subjects' requests to exercise their rights shall be handled by Thales in accordance with the internal procedure defined under Appendix 9.

As described in Appendix 9, Data Subjects are duly informed of the exercising of rights' request handling procedure and how to file a request through the 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 request for exercising its rights 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**.

Thales commits to handle such requests without undue delay and in any event within one (1) month of receipt of the request, by a department or person with an appropriate level of independence in the exercise of his/her functions, as identified under Appendix 9, with particular care and attention. Taking into account the complexity and number of requests, that period may be extended by two (2) further months at the utmost and Thales shall inform the Data Subject accordingly within one (1) month of receipt of the request, together with the reasons for the delay.

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, 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-C 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 Competent DPA and/or competent court as per Section 10.2 here above.

If the complaint is justified, the concerned Thales Entity 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-C, Thales is committed to provide a high level of protection to the Personal Data it processes.

In order to ensure that the principles defined under the BCR-C are effectively taken into account and reflected in the different Processing activities carried out by Thales, Thales shall ensure that Personal Data protection issues are considered prior to the beginning of any new project. In practice, this means that the principles and obligations defined hereunder shall be integrated into the design of the project. The overall objective is to ensure that the requirements applicable in terms of Personal Data protection defined under the BCR-C and under applicable law have been taken into account.

The GDPR provides for obligations related to "Privacy by Design" and "Privacy by Default". In order to comply with these obligations, Thales has adopted the following approach regarding Personal Data protection:

- anticipate Personal Data protection requirements and embed such requirements from the design phase of any project or process and where relevant from the tender phase;
- ensure that any Personal Data protection requirements are embedded into the project in an easy way and that any recommendation made with regard to Personal Data protection remains business oriented;
- make sure that the Personal Data protection implication of a project are clearly defined and identified to facilitate the compliance of the requirements, as well as to ensure full transparency towards Data Subjects;
- ensure that the Personal Data protection requirements can be complied with during the entire life cycle of the product or system or during the Personal Data storage period if the latter is longer.

The effective implementation of the provisions of this Section 13 shall be respected by each Thales' employee involved in the Processing of Personal Data, with the support of the Data Protection Correspondent and the Group Data Protection Officer.

14. DATA PROTECTION IMPACT ASSESSMENT

It is Thales' responsibility to monitor Personal Data Processing compliance with Applicable Personal Data Protection Legislation. In this respect, Thales has implemented a Data Protection Impact Assessment procedure which enables Thales to:

- identify Processing which present specific risk for the protection of Personal Data;
- assess the level of compliance of the Processing it carries out; and
- determine the corrective measures to be implemented in order to ensure that Personal Data are finally processed in compliance with Applicable Personal Data Protection Legislation.

Thales shall carry out a Data Protection Impact Assessment for Processing on Personal Data that are likely to result in a high risk to the rights and freedoms of natural persons as per Article 35 of the GDPR.

Where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk, Thales shall consult the Competent DPA prior to implementing the concerned Processing.

The internal procedure to be followed by Thales in order to assess the impact of a project on the protection of Personal Data is further described in Appendix 11.

15. RECORD OF PROCESSING ACTIVITIES

For the Processing subject to the GDPR, Thales commits to maintain a Record of Processing activities, up to date, in line with the requirements of the GDPR.

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

- the name and contact details of the Data Controller and, where applicable, the joint controller, the Data Controller's representative and the Group Data Protection Officer;
- the purposes of the Processing;
- the categories of Data Subjects;
- the categories of Personal Data;
- the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in Third Countries or international organizations;
- the Transfers of Personal Data to any Third Country or to an international organization, including the identification of that Third country or international organization and the documentation of suitable safeguards;
- the retention period of the different categories of Personal Data;
- where possible, a general description of the technical and organizational security measures referred to in the GDPR.

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

- the name and contact details of the Thales Entity acting as Internal Data Processor and of the Group Data Protection Officer;
- the name and contact details of each Thales Entity acting as Data Controller on behalf of which the Internal Data Processor is acting;
- the name and contact details of any sub-processor;
- the categories of Processing carried out on behalf of each Data Controller;
- 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 mandatory 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-C.

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

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-C 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 the BCR-C and commits to communicate this public version of the BCR-C (as well as any other specific policies related to Personal Data protection applicable to employees and 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 employees and on its website for other Data Subjects.

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

- 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-C
- 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

Besides, where it is acting as Data Controller, Thales commits to provide Data Subjects with the relevant information and, as a minimum, with the following information:

- the identity and the contact details of the Thales Entity acting as Data Controller;
- the contact details of the Group Data Protection Officer;
- the purposes of the Processing, as well as the legal basis it relies upon;
- if the information is not obtained from the Data Subject, the categories of Personal Data processed and the source from which the Personal Data originate;
- whether the provision of Personal Data is a statutory or contractual requirement, or necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such data;
- the categories of recipients of the Personal Data;
- where applicable, the existence of Transfers of Personal Data out of the EEA, the countries where the Personal Data are transferred and the measures implemented to ensure an adequate level of protection as well as the means to obtain a copy thereof or accessing them;
- the Personal Data's storage period or, if that is not possible, the criteria used to determine that period;
- the rights of the Data Subjects as defined under Section 10 above;
- where Processing is based on consent, the right to withdraw consent at any time;
- the right to lodge a complaint before the Data Protection Authority;
- if the Processing is based on Thales' legitimate interest, description of the said legitimate interest;
- as the case may be, the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
- the third party beneficiary rights of the Data Subjects with regard to the Processing of their Personal Data and the means to exercise those rights;
- the Sections of the BCR-C relating to liability;
- the Sections of the BCR-C relating to data protection principles.

Thales shall ensure that such information is provided in full and in an easily understandable form and that it is made easily accessible to Data Subjects. For this purpose, Thales shall use its standard information notices which shall be adapted to each Processing depending on its context and characteristics.

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

Where a Thales Entity has reasons to believe that the legislation applicable to it is likely to prevent it from fulfilling its obligations under the BCR-C or has substantial effect on the guarantees provided by the BCR-C, it will promptly inform Thales S.A., the Group Data Protection Officer and, where appropriate, the relevant Data Protection Correspondent(s), unless otherwise prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

This includes any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body.

In case of Transfer, the Thales Importer Entity will promptly notify the Thales Exporter Entity and, where possible, the Data Subject (if necessary with the help of the Thales Exporter Entity) if:

- it receives a legally binding request by a public authority under the laws of the country of destination, or of an another Third Country, for disclosure of Personal Data Transferred pursuant to the BCR-C; such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;
- it becomes aware of any direct access by public authorities to Personal Data Transferred pursuant to the BCR-C in accordance with the laws of the country of destination; such notification will include all information available to the Thales Importer Entity.

If, in specific cases, the notification is prohibited, the Thales Entity to which the request has been communicated 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.

The Thales Importer Entity will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.

The Thales Importer Entity will, under the same conditions, pursue possibilities of appeal.

When challenging a request, the Thales Importer Entity will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

The Thales Importer Entity shall provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

The Thales Importer Entity shall provide the Thales Exporter Entity, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Thales Importer Entity is or becomes partially or completely prohibited from providing the Thales Exporter Entity with the aforementioned information, it will, without undue delay, inform Thales Exporter Entity accordingly.

The Thales Importer Entity will preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the BCR-C, and shall make it available to the Competent DPA upon request.

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.

18. TRAINING

Thales ensures that the BCR-C 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-C.

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 12 of the BCR-C.

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-C.

Scheduled global audits (on site or remote), including audits with respect to the general compliance of Thales with the BCR-C 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-C, 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-C 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-C.

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 13. 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-C 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-C;
- 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-C 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-C 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-C

The BCR-C 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 (EDPB) recommendations, or changes to the scope of the BCR-C).

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

Where a modification to the BCR-C would possibly be detrimental to the level of the protection offered by the BCR-C 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-C or to the list of the Thales Entities, with the brief explanation of the reasons for the changes. This includes any changes made in order to align the BCR-C with any updated version of the EDPB recommendations. 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-C or significantly affect the BCR-C (i.e. changes to the binding character) must also be promptly communicated:

- to each Thales Entity bound by the BCR-C (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-C up-to-date and in compliance with Article 47 of the GDPR and the EDPB recommendations.

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

CATEGORIES OF PROCESSING	IDENTIFIED PURPOSES
IS-IT / IS security/ Telephony	1.Management of the Information System and phone network, control of access to the Information System as well as to various IS/IT tools (software, applications, printers, etc.), management of authorizations and of the appointments of IS/IT administrators related thereto, user authentication and management of their profiles, monitoring of the actions they carry out (e.g., modification of database)
	2. Implementation of an e-mailing system
	3. Monitoring and auditing connections to certain IT tools and databases in order to determine the use rate and calculate the cost of related licenses, analysis of websites browsing by users to understand their use and improve the concerned website(s)
	4. Implementation of IS/IT security audits, management and monitoring of security breaches/incidents, implementation of procedures for data back-up and business continuity in the event of incidents impacting the Information System
	5. Management and follow-up of IS/IT assistance requests submitted by users to the Helpdesk
	6. Management of phones and associated phone networks available to employees
	7. Management of collaborative tools
	8. Management of IT activity planning
Security	9. CCTV
	10. Reception of visitors, implementation of control measures to ensure the security of access to sites and monitoring of the security incidents on site
	11. Management of the authorizations of employees, suppliers, partners and customers, processing of biometric data of employees and visitors for obtaining the accreditations and / or authorizations necessary to access certain sites, documents and/or applications considered as sensitive
	12. Follow-up of employees on business trip to ensure their security
HR	13. Recruitment of employees and follow-up of applications
	14. Workforce administration, employees profiles, management of organizations, reporting and data analytics
	15. Management of: • performance, remuneration, financial or non-financial benefits • career and skills development

CATEGORIES OF PROCESSING	IDENTIFIED PURPOSES
HR	16. Management of pay, administrative file of employees (presence, absence, sick leave, retirement, transfers, etc.) and work-time follow-up
	17. Management of professional training
	18. Management of employee on international assignment (follow-up of their mission, support measures, family situation)
	19. Management and monitoring of the fleet of professional vehicles used by employees. Checking of the driving license of the concerned employees, including training in the field of driving where necessary (e.g., significant mileage). Follow-up of infractions and complaints in the event of violations
	20. Occupational health
	21. Organization of professional elections, management of employee representative bodies meetings, follow-up of trade union mandates and of the provisions of the Thales agreement on union rights
	22. Management of the workload, organization and monitoring of projects and activity
	23. Management of employee surveys
	24. Management of the employment policy of disabled workers
Technical	25. Follow-up of inventions notifications in the context of activities relating to intellectual property
	26. Performance of R&D (Research & Development) projects
	27. Management of experimentations and tests of the Thales' solutions, products and services
Compliance	28. Creation and management of insiders list as well as management of anti-corruption declaration, due diligence procedure in relation to partners, the management of the whistle-blowing, internal investigation and conflicts of interests procedures
	29. Monitoring compliance in terms of trade compliance and protection of personal data
	30. Management of directors and shareholders including in order to comply with the legal obligations
	31. Lobbying

CATEGORIES OF PROCESSING	IDENTIFIED PURPOSES
Operations	32. Processing for environmental health and safety reporting purposes
	33. Document management
	34. Management of employees' feedbacks and of their satisfaction, follow-up of suggestions submitted by them (e.g., suggestion box)
	35. Management of employees and providers clearances for the purpose of obtaining the accreditations and/or clearances necessary (i) to validate the conformity of data, documents, products or services with norms, standards or regulations or (ii) to carry out verifications or audits.
	36. Management and monitoring of occupational risk, accidents or diseases, as well as exposure to them for prevention and statistical purposes
	37. Management, follow-up and inventory of the real estate portfolio of the group
	38. Processing of personal data for the purpose of preparation and operational support of site survey, deployment and operation of Thales systems on customer sites.
	39. Management and follow-up of Thales sites occupancy.
	40. Processing of personal data of operators in the production room to ensure the protection of electronic devices from electrostatic phenomena.
	41. Processing of personal data for the purposes of traceability of production tools and knowledge of their usage rate.
Litigation and insurance	42. Management and follow-up of employees' claims or solicitations for indemnity, management of the relationships with insurers in this respect
	43. Study and resolution of third-party claims, solicitations for indemnity, litigation and pre-litigation, and for the determination of counsel assisting Thales in litigation and pre-litigation procedures
Communication/ Events	44. Processing for events organization and communication purposes
	45. Implementation of corporate network, including social corporate netork
Customers/ Suppliers/ Partners	46. Relationship management with customers, partners and prospects
	47. Management of mergers and acquisitions operations
	48. Management of the relationships with the suppliers and subcontractors, involving in particular the management of the purchases and the monitoring of the contractual relationships

CATEGORIES OF PROCESSING	IDENTIFIED PURPOSES
Customers/ Suppliers/ Partners	49. Management of booking, purchase, evaluation and provision of training by Thales for the benefit of its internal and/or external clients
	50. Submission of applications in the context of calls for tenders initiated by potential customers, involving in some cases exchanges of data with bidding partners and/or the customers
	51. Follow-up and management of the use of interactive platforms and networks made available to end customers and of purchases made by the latter on the said interactive platforms and networks
	52. Processing for the purpose of adapting and setting up products in accordance with the customers' needs
	53. Managing incidents on products and systems and incident reports made by THALES employees
	54. Data processing intended to ensure the organization, follow-up and performance of training sessions provided by Thales for its customers
	55. Data processing resulting from technical support and maintenance operations carried out for Thales customers
	56. Processing for participating in and/or implementing research projects
	57. Processing for obtaining grants
	58. Management of the electronic signature
	59. Management of travels, booking and payment of travel documents, as well as reimbursement to employees of travel expenses, follow-up and management of expenses submitted by employees, gifts and hospitality that employees may consider accepting or offering and of professional credit cards
	60. Access to online applications or services
Strategy	61. Personal data collection and processing for regulatory and economic watch as well as strategic intelligence
Accounting/Tax	62. Accounting and tax management as well as controlling financial operations
Audit	63. Implementation of internal audits within the group and follow-up of the actions resulting therefrom

APPENDIX 2
THALES ENTITIES BOUND BY THE BCR-C 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 (federation)
	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
DATA PROTECTION IMPACT ASSESSMENT

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

APPENDIX 12
TRAINING PROGRAM

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

APPENDIX 13
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.2023-144 dated 21st December 2023.
002	10/2024	Update of Appendix 1 "*List of purposes of processing*" and update of Appendix 2 "*Thales entities bound by the BCR-C*".
003		

THALES

Building a future we can all trust

Thales
Campus Meudon
4 rue de la Verrerie
92190 Meudon
France

thalesgroup.com