GENERAL SALES TERMS AND CONDITIONS OF SALES FOR PROVISION OF SOLUTION SaaS

(Version April 2025)

This document is a Commercial Proposal and is subject to the signature of a **Thales agreement** ("***Agreement***"). Upon acceptance of the Commercial Proposal by the Customer, Thales shall send to Customer a draft Agreement reflecting the terms of this Commercial Proposal (including any addendums, changes and/or additions agreed upon), which shall be negotiated in good faith by the Parties. Notwithstanding the foregoing, the following legal terms and conditions together with the present Commercial Proposal shall apply to the Product(s) and/or Software(s) and/or Services(s) described herein and constitute an interim contract ("***Interim Contract***") for the Interim Period of time starting on acceptance of this Commercial Proposal and/or issuance of a purchase Order by Customer (whichever is the earlier) and ending upon signature of the Agreement.

1. Precedence

In the event of any conflict or inconsistency between the provisions of the present Legal Conditions and the other provisions of the Commercial Proposal or the Interim Contract (including provisions of Schedule Data Protection and Security Terms and Schedule Governing Law and Jurisdiction), the provisions of the Legal Conditions shall prevail. In no event shall any other terms and conditions accompanying purchase orders, invoices, reminders and other commercial documents or standard forms sent by Customer constitute any amendment to this Interim Contract irrespective of the date of such documents.

2. Provision of Services

As pre-requisite and for Customer to receive the Services, Thales will connect Customer to the Solution pursuant to a setup/connection process to be defined by Thales, to enable Customer to deliver or have delivered the Customer Data via a selected secure network connection. Once Thales considers that the connection process is completed, Thales will provide the Customer with an acceptance form, requesting acknowledgment that the connection of the Solution has been performed according to the Specifications (the "Acceptance Certificate"). The Customer shall have five (5) Business Days, from the date of the Acceptance Certificate, to sign it. Should the Customer refuse to sign the Acceptance Certificate, the Customer shall so notify Thales in writing by substantiating the non-conformities of the Solution with the Specifications, within the same five (5) Business Days period. Should the Customer fail to sign the Acceptance Certificate, within the five (5) Business Days period, without notifying Thales as per above, the connection of the Solution shall be considered as completed and the Acceptance Certificate shall be deemed signed by the Customer. Upon Acceptance, Thales will perform the Services. Customer acknowledges and agrees that the commercial use of the Solution (i.e., providing Services to End-Users) shall be deemed as a signature of the Acceptance Certificate.

Customer acknowledges that the performance of the Services is dependent upon the following conditions:

- Customer, during the connection/set up process, shall cooperate with Thales to implement the necessary integration required for the performance of the Services.
- The Customer shall (i) grant Thales' access to and use of the Customer's information and facilities reasonably necessary for the Services; (ii) have a representative present at all times during the installation and/or configuration; and (iii) provide ready access to the Network.
- Customer shall (a) ensure that its and its End Users' use of the Services complies with the Interim Contract; (b) prevent and terminate any unauthorized access or use of the Services; and (c) promptly notify Thales of any unauthorized use of, or access to, the Services of which Customer becomes aware; and (d) grant Thales access to and use of all information, data, and Network, as reasonably determined by Thales to be necessary for the connection of the Solution and performance of the Services.
- Customer shall grant or obtain and provide to Thales or the relevant Affiliate(s) all Required Consents.
- Customer shall be liable against and pay Thales any fees required or costs occurring in connection with and/or relating to obtaining all Required Consents.
- Customer shall be responsible for obtaining any necessary consents and providing any required notices to allow Thales to access, store, and process data provided by the Customer (including Customer Data, if applicable) under the Interim Contract.
- Customer shall have and maintain all necessary permits, consents and notices registrations, filings, and licenses necessary in order to receive the Services and, with respect to the Network, be responsible for the

implementation and maintenance at all times of external security, contingency and back-up procedures for reconstruction of lost or altered files, data, programs, if any, and for reconstructing any such material.
- Customer's full and timely cooperation with Thales and in particular fulfillment of its obligations detailed in the Commercial Proposal.
- The accuracy and completeness of any information and data Customer provides to Thales.

3. Rights Granted

During the Term of the Agreement, Thales grants Customer a limited, revocable, non-exclusive, non-transferable right to use the Services provided from the Solution, in accordance with the Documentation for the Term of the Agreement.- Customer grants to Thales a limited, non-exclusive, royalty-free, fully paid-up, revocable, world-wide license to process, as necessary to provide the Service, the Customer Data, and any proprietary information provided by Customer in connection with the provision of the Service.

4. Ownership and Restrictions

Customer shall retain all ownership and Intellectual Property Rights in and to Customer Data.
Thales or/and its licensors retain all ownership and Intellectual Property Rights to the Services and Thales Software if any. Thales shall retain all ownership and Intellectual Property Rights to anything developed and delivered under the Interim Contract.

Customer will not:

(a) make any Service(s) or Thales Data available to, or use any Service(s) or Thales Data for the benefit of, anyone other than Customer or its End-Users, (b) sell, resell, license, sublicense, distribute, rent or lease any Service(s) or Thales Data, or include any Service(s) or Thales Data in a Service bureau or outsourcing offering, (c) use any Service(s) to store or transmit infringing, libelous, or otherwise unlawful or tortuous material, or to store or transmit material in violation of third-party privacy rights, (d) use any Service(s) to store or transmit malicious code, (e) interfere with or disrupt the integrity or performance of any Service(s) or third-party data contained therein, (f) attempt to gain unauthorized access to any Service(s) or Thales Data or its related systems or networks, (g) copy any Service(s) or any part, feature, function or user interface thereof, (h) copy Thales Data except as permitted herein or the Documentation, (i) access any Service(s) or Thales Data in order to build a competitive product or Services.

Customer will not, and will not allow End Users to:

(a) copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any of the source code of the Solution and/or Software if any (except to the extent such restriction is expressly prohibited by applicable law); (b) sell, resell, sublicense, transfer, or distribute the Services; or (c) access or use the Services: (i) for High Risk Activities; (ii) in a manner intended to avoid incurring Fees; (iii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (iv) in a manner that breaches, or causes the breach of, Export Control Laws; or (v) in a manner that would not be consistent with, breaches, or cause the breach of the General Security Policy for Health Information Systems (PGSSI-S).

5. Services Suspension

Thales may suspend Services if: (a) necessary to comply with law (including governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority) or Customer or any End User’s use of the Services does not comply with Services described in the contract and it is not cured following notice from Thales.
If Thales Suspends Services, then: (a) Thales will provide Customer notice of the cause for suspension without undue delay, to the extent legally permitted; and (b) the suspension will be to the minimum extent and for the shortest duration required to resolve the cause for suspension.

6. Confidentiality

All information contained in this Commercial Proposal, and all information to be disclosed by Thales pursuant to the activities contemplated in the Interim Contract is confidential between Thales and Customer and shall not be duplicated, published or disclosed to any legal entity, organization or person in whole or part without the prior written consent of Thales.

The information and data contained in this document and any document or support of information supplied by Thales as part of this commercial Proposal or the Interim Contract shall remain Thales’s exclusive property along with all industrial

property rights and copyright attached thereto. Therefore, no right, title or interest is transferred to the Customer by this Commercial Proposal or by the Interim Contract in the names, trademarks, patents, pending patents, expertise, copyright and other intellectual property rights relating to the solution.

7. Personal data and security policy

General:
The terms and conditions covering the processing of Personal Data in the delivery of the Services are set forth in the Data protection provisions set forth in the Schedule “Data Protection and Security Terms” attached to the present Commercial Proposal.
Furthermore, to comply with transparency requirements, prior to entering into the Interim Contract with Customer, Thales has delivered to Customer a document called “Subject Matter and Details of the Data Processing” attached to this Commercial Proposal
Thales reserve the right to migrate the Solution to another data center located (i) in the European Economic Area (“EEA”) for Solution(s) initially hosted in EEA, (ii) in United States Area (“US”) for Solution(s) initially hosted in US. Thales will provide a minimum thirty (30) days notice to Customer detailing the technical plan accompanying the migration windows and the effect on the Availability of the Services.

8. Warranty

Thales warrants that the Services comply with description thereof in the present Commercial Proposal.
If Thales receives written notice from Customer of any substantial non-conformance that impairs the functioning of the Service(s), Thales will use reasonable endeavors to remedy or cause to remedy such non-conformance after receipt of such notice, according to the “Thales Support policy and Incident Management”. Thales at its option may either correct or cause to correct such non-conformance or provide or cause to provide a work-around, which substantially remedies the non-conformance. The Customer's written notice will specify in reasonable detail the nature of such non-conformance.

Exclusions:
The obligations provided in paragraph “Warranty” above will not apply in the event of non-conformances resulting from:

1. software, hardware (including Devices), interfacing, or data not supplied by Thales under the Interim Contract, including but not limited to software, hardware, interfacing, supplies or services provided by a third Party;
2. the Network and/or the third party system;
3. improper use or operation of the Services or any portion thereof;
4. unauthorized use by the Customer of the Network and/or a third party system;
5. improper or inadequate maintenance of the Network and/or a third party system;
6. failure by the Customer to provide complete and/or accurate data necessary for Thales to provide the Services;
7. unavailability or inaccuracy of the GSMA device database.

All conditions, terms, representations (other than fraudulent representations) and warranties relating to the Service, whether implied by law or otherwise, which are not expressly stated in the Interim Contract including, without limitation, the implied warranty of satisfactory quality and fitness for a particular purpose are excluded to the fullest extent possible by law.

9. Indemnification

Thales will defend, at its expense, a third-party filed legal complaint, lawsuit or proceeding against Customer (“Claim”) to the extent such Claim is based upon an allegation that Services, as of their delivery date, directly and literally infringe in the country where Customer has its registered address valid Non- Essential Patent(s), or copyrights or misappropriate a third party’s trade secret (hereafter “IP Claim”). Always subject to the Section” Excluded Claims” set forth in the paragraph below, Thales will indemnify Customer for any final adverse judgment(s) by a competent court or an arbitration tribunal, settlements and reasonable attorney fees resulting from an IP Claim. The foregoing obligations are conditioned on Customer: (a) notifying Thales promptly in writing of the IP Claim; (b) giving Thales sole control of the defense thereof and any related settlement negotiations; and (c) cooperating and, at Thales’s request and expense, assisting in such defense. If the Services becomes, or in Thales’s opinion is likely to become, the subject of an IP Claim, then Thales may (at its option and expense) either: (a) procure for Customer the right to continue using the Services; (b) replace or modify the Services so that it becomes non-infringing or (c) terminate the Contract or any part thereof.

Excluded Claims:

Thales has no obligation under this Section "Indemnification" or otherwise with respect to an IP Claim based upon: (a) any use of the Services not in accordance with the Interim Contract or the related Documentation (b) any modification of the Services by any person other than Thales or its authorized agents, (c) use of the Services in combination with solution, product, process, data or equipment if the infringement was caused by such use or combination, regardless of whether or not the Services or elements of the Services are a material part of the infringement, (d) any content and/or materials introduced or made available in or through the Services by Customer, Customer's client(s), end users, and/or any third parties, (e) damages attributable to the value of the use of a non-Thales product, Services, data or business process, (f) the use of the Services(s) during any time period after Thales has notified Customer to discontinue use of the same, (sub-sections (a) to (f)) are hereafter collectively referred to as "Excluded Claim(s)"). Customer indemnifies Thales against all liability, damages and costs (including reasonable attorneys' fees) resulting from or related to an Excluded Claim.

In case a third party asserts that Services, as of their delivery date, directly infringe valid Standard Essential Patents ("SEP Claim"), and subject to Thales duty to confidentiality, Thales will provide Customer with information about the Standard Essential Patents under which Thales is licensed for its Services, if any. Thales at its own discretion may support Customer in the defense against or settlement of such SEP Claim provided that Customer immediately after the receipt of the SEP Claim informs Thales in writing hereof, grants Thales access to all communication and documents related to the SEP Claim and enables Thales to actively participate in the defense or settlement of the SEP Claims. For the avoidance of doubt, Thales shall not have any obligation to indemnify and shall not hold the Customer harmless from any SEP Claim regarding infringement of Standard Essential Patents by the Solution brought against Customer directly or indirectly by any third party.

Thales may enter into further Standard Essential Patent licenses during the Interim Contract. Thales may increase its prices to reflect increased royalty costs.

The foregoing states the entire liability of Thales and the exclusive remedy for Customer relating to IP Claims and SEP Claims. Except as expressly stated in this Section "Indemnification", any remedy for indemnification regarding such intellectual property rights shall become time-barred twelve (12) months after the delivery of the respective Services to Customer. All warranties of non-infringement of any intellectual property rights are hereby expressly disclaimed by Thales.

10. Limitation of liability

Entire Liability:

This Section sets forth the entire liability of Thales, and the Affiliates (including any liability for the acts and omissions of its employees, agents and contractors) to the Customer, its agents, employees and contractors whether in contract or in negligence in respect of (i) any breach of its contractual obligations arising under this Interim Contract; and (ii) any representation statement (other than fraudulent) or wrongful act or omission including negligence arising under or in connection with this Interim Contract.

Exclusions

Except for loss that arise as a result of a fraud perpetrated by a party; or claims for death or bodily injury (or any other liability which cannot be excluded or limited by law, In no event shall Thales be liable to Customer, its agents, employees, successors and assigns for any special, indirect and/or consequential damages of any kind, including, without limitation, loss of revenue or profit, loss of productivity, damage resulting from business disruption, damage to brand image, suffered by Customer arising out of or connected to this Interim Contract.

Notwithstanding anything set out in this Section "Limitation of liability", Thales and its Affiliates shall have no liability arising out of or in connection with:

- the availability, performance, non-performance, defective performance, and maintenance or otherwise of third-party systems, Customer' system and/or associated or supporting systems to use or otherwise access the Services, improper use or operation of the Services or any portion thereof;
- wrong, missing, delayed or incomplete information or data provided in connection with the Services by the Customer and/or a third-party;
- software, hardware (including but not limited to the Device), interfacing, not supplied by Thales and part of the Services;

- any failure to meet an obligation to this Interim Contract where such failure is caused (directly or indirectly) by Customer's failure or delay to meet any of its obligations pursuant to this Interim Contract.

Liability cap

Notwithstanding the foregoing, and to the extent permitted by law, Thales and its Affiliates total and aggregate liability to Customer for any kind of direct loss, damage or liability arising under or in connection with this Interim Contract, under any theory of liability, shall in no event exceed, as an aggregate, the total amount actually paid by Customer to Thales for the Services that is subject of the claim in the twelve (12) calendar months immediately preceding the occurrence of the event giving rise to such claim (less any amounts already paid out under the Interim Contract).

11. Termination

Either Party may terminate this Interim Contract, in whole or in part, if the other Party: (a) is in material breach of this Interim Contract where the breach is incapable of remedy; (b) materially breaches any material term or condition of this Interim Contract where the breach is capable of remedy and fails to cure such breach within ninety (90) calendar days after receiving written notice thereof; or (c) becomes insolvent or makes any assignment for the benefit of creditors or similar transfer evidencing insolvency, or suffers or permits the commencement of any form of insolvency or receivership proceeding, or has any petition under bankruptcy law filed against it, which petition is not dismissed within ninety (90) calendar days of such filing, or has a trustee, administrator or receiver appointed for its business or assets or any part thereof.

In the event of termination, Customer agrees to compensate Thales for any work performed or costs incurred up to the date of termination including the decommissioning fees.

Thales shall submit an invoice detailing the costs associated with the termination which shall be sent to Customer promptly upon termination. Customer agrees to make payment for the provisioned Product(s) and/or Software(s) and/or Services(s) and/or the costs associated with the termination, within 15 days of receiving the invoice from Thales.

12. Anti-corruption and Influence Peddling

1- The Parties shall always act in accordance with national and foreign laws and regulations applicable to the prevention and detection of risks of corruption and influence-peddling. In compliance with law, Thales performs due diligence on all parties with whom it enters into business relationships. In the event this due diligence were to reveal material ethical risks which in Thales' reasonable opinion cannot be adequately mitigated, Thales may rescind this Commercial Proposal and Interim Contract without liability or penalty.

2- The Parties shall always act in accordance with the national and foreign laws and regulations applicable to the prevention and detection of risks of corruption and influence-peddling, and in particular French law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and the modernization of the economy (the "Sapin II Law").

Whether directly or via third parties, neither Party shall propose to any person, or shall accept from any person, any offer, promise, donation, gift or benefit of any kind which would be linked to a misuse that would be made by that person, or that has already been made by that person, of his/her real or supposed influence with a view to obtaining, for itself or for others, a distinction, a job, a contract or any other favorable decision.

Neither Party shall solicit or accept for itself any offer, promise, donation, gift or benefit of any kind, for the purpose of misusing its influence with a view to making or obtaining any favorable decision.

Each of the Parties declares that it has implemented a compliance program that meets the requirements of the Sapin II Law, insofar as it is subject to it.

3- Each of the Parties hereby represents and warrants that none of its legal representatives is, or has been for the last three years, or will be at any time during the term of the Interim Contract, a Politically-Exposed Person who might, thanks to his/her function or mission, influence the position to be taken by him/herself or the end-customer within the frame of the performance of the Interim Contract. In case where, during the term of the Interim Contract, either Party would become aware of any circumstance likely to put into question this representation and warranty, it would have to promptly inform the other Party thereof.

In the meaning of the foregoing provision:
"**Legal representative**" means any of the directors and managing officers of either Party, of the company (or companies) controlling that Party and of the ultimate beneficiaries of that Party.

"**Politically Exposed Person**" (or "PEP") means any natural person who is either an "Initial PEP" or, by extension, a "Relative" to an Initial PEP:

(i) an Initial PEP is a person who cumulatively fulfils the following two criteria:

- on the one hand, is a ‘’Public Official’’ or a senior official of a state-owned enterprise or publicly-owned company or of a political party, in the Customer’s / end-customer’s country, who is currently exercising his/her functions or who has held such a position in the last three (3) years;
- and on the other hand, this person, by virtue of his/her function or mission (past or current), is able to influence the Customer’s / end-customer’s final decision regarding the award of a contract, or is able to influence the position to be taken by the Customer or the end-customer within the frame of the performance of a contract.

(ii) A Relative of an Initial PEP is any one of the following people:

- parents, brothers and sisters, children of the Initial PEP, as well as the spouse(s), recognized partner(s) or companion(s) of these children;
- spouse, recognized partner or companion of the Initial PEP, as well as the ascendants and descendants of this spouse, recognized partner or companion of the Initial PEP;
- persons closely associated with the Initial PEP, that is to say any person who is widely and publicly known to have close links, in particular business links, with the Initial PEP, including the beneficial owner of a legal entity, of a legal person or of a legal device held jointly with the Initial PEP or known to have been established for the benefit of the Initial PEP.

“**Public Official**” means any natural person who cumulatively fulfils the following two criteria:

(i) On one hand, this person:

- holds a legislative mandate or occupies an administrative, military or judicial position in the Customer’s / end-customer’s country, whether by appointment or by election, on a permanent or temporary basis, with or without remuneration; or
- exercises a public function, as a public official or as a public agent, at any hierarchical level whatsoever, including within a public company or a national or international public body; or
- provides a public service or acts as a public official, depending on the meaning that the law in force in the Customer’s / end-customer’s country gives to these terms;

(ii) And on the other hand, this person:

- is or appears to be, by virtue of his/her function or mission (past or current), able to influence the Customer’s / end-customer’s final decision regarding the award of a contract, or
- is able to influence the position to be taken by the Customer or the end-customer within the frame of the performance of a contract.

4- Any violation by the Parties of any provision of this Article shall be deemed a material breach by it of its contractual obligations, and shall entitle the non-defaulting Party either to suspend the performance of the Interim Contract as long as the breach is not satisfactorily remedied or to terminate the Interim Contract immediately, and this without prejudice to any other remedy to which it may be entitled as per contractual provisions and/or at law.

13. Force Majeure

Thales shall not be in default if performance of any of its obligations under the Interim Contract is partially or wholly delayed or prevented by reason of Force Majeure.
The occurrence of a Force Majeure event shall automatically suspend performance of the Interim Contract and the dates of the contractual schedule shall be postponed for the time period required to overcome the effects of the Force Majeure, and in any case for a period at least equivalent to the duration of the Force Majeure event.
If Thales’ performance of any obligation under the Interim Contract is delayed in whole or in part by reason of Force Majeure for a period exceeding six (6) months, either Party may request termination of the Interim Contract, in whole or in part, in accordance with article 1.10 “Termination”, and the Parties shall mutually agree upon a liquidation settlement. In case of disagreement, it shall be deemed to be a dispute which shall be settled in accordance with the provisions of article 1.13 “Governing Law & Dispute resolution”.
The termination shall not affect the debts due between the Parties at the date of the termination, in particular for the Products, Software and/or Service in production or execution at the said date.

14. Governing Law and Dispute Resolution

Applicable Laws: The governing law of the Commercial Proposal and the Interim Contract shall be determined, based on the Thales entity submitting the present Commercial Proposal, in accordance with the table set out in the Schedule "Governing Law and Jurisdiction". The Commercial Proposal and the Interim Contract shall not give effect to any conflicts of law principles. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Interim Contract.

Dispute Resolution: The Parties shall attempt to resolve any dispute arising out of or in connection with this Interim Contract, including regarding its validity, execution, performance, breach, expiry or termination (including non-contractual disputes or claims) amicably by mutual agreement.

Any dispute or claim that may arise in connection with the Interim Contract, shall be first referred to proceedings under the International Chamber of Commerce (ICC) mediation rules. If the dispute has not been settled pursuant to the said rules within sixty (60) Days following the filing of a request for mediation or within such other period as may be agreed in writing, such dispute shall thereafter be finally settled under the rules of arbitration of ICC by one or more arbitrators appointed in accordance with the said rules of arbitration.

The place of arbitration shall be determined, based on the Thales entity submitting the present Commercial Proposal, in accordance with the table set out in the Schedule "Governing Law and Jurisdiction

The language to be used in the arbitral proceedings shall be English, unless otherwise agreed by the Parties.

The arbitration proceedings shall be confidential.

15. Trade Compliance

The Parties shall comply with all applicable export controls and economic sanctions ("Export Laws"), including, as applicable, the Export Administration Regulations maintained by the U.S. Department of Commerce ("EAR"), trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control ("OFAC"), export controls and restrictive measures maintained by the U.K. Government, the European Union (the "EU") and by any EU member-state, as well as any embargo and trade control regulation.

Customer shall not sell, export or supply Services to any individuals or legal entities that are the subject of sanctions or of blocking or asset-freeze measures applicable in the United States of America, in any EU member-state (whether resulting from EU regulations or from a governmental decision) or in the United Kingdom. This shall apply, without limitation, to individuals and legal entities that are on the OFAC List of Specially-Designated Nationals and Blocked Persons, the national list of any EU member-state or the EU Consolidated List.

The Parties agree to maintain full, true, and accurate records of exports, re-exports, and transfers of Services purchased and distributed or resold for at least five (5) years following the respective dates of such exports, re-exports, or transfers, and agree to provide such export-related records to the other upon request.

The Customer commits to verify that its distributors, resellers and their own customers (as well as their respective directors) are not subject to the above-mentioned sanctions or blocking or asset-freeze measures.
The Customer agrees to flow-down the requirements resulting from the provisions of this Article to its own distributors, resellers and their own customers in order to prevent any risk of breach of Export Laws.

In application of Council Regulations (EU) No 833/2014 and 765/2006, the Customer shall not sell, export or re-export, directly or indirectly any goods and/or technologies supplied under this Interim Contract to :

i) the Russian Federation, the Belarus or for use in the Russian Federation or in the Belarus and in the Ukrainian territories controlled by the Russian Federation, or

ii) any individual or entity subject to EU sanctions or restrictive measures, as well as to any entity owned by, controlled by or acting for individuals or entities subject to EU sanctions or restrictive measures.

The Customer undertakes to immediately report in writing to Thales any suspicion of, allegation of or actual violation of these restrictive measures set forth in items i) and/or ii) above and shall immediately cease any such sale, export or re-export of goods and/or technologies supplied by Thales.

Any violation of this article shall be deemed a material breach by the Customer of its contractual obligations thereby entitling Thales without incurring any liability whatsoever, whether for payment of damages, by way of an indemnity, for costs or otherwise, to either :

-stop the negotiation and withdraw the Commercial Proposal, without incurring in any payment of damages, indemnity or costs, and/or

-suspend the performance of this Interim Contract as long as the breach is not satisfactorily remedied, and/or

-terminate this Interim Contract with immediate effect and without incurring in any payment of damages, indemnity or costs.

The above being without prejudice to any damages or remedy Thales may be entitled to claim under the Interim Contract or any applicable legal provisions.

Notwithstanding Article “Confidentiality” above, Thales is allowed to disclose the content of this article and the information exchanged between the Parties in relation with this article if required by virtue of a court order, a legal obligation or an external audit.

16. Definitions

Affiliates: means any corporation, partnership, or other entity that, directly or indirectly, owns, is owned by, or is under common ownership with, such Party hereto, for so long as such ownership exists. For the purposes of the foregoing, "own," "owned," or "ownership" shall mean ownership of more than fifty percent (50%) of the stock or other equity interests entitled to vote for the election of directors or an equivalent governing body.

Business Day(s) : means any day other than a Saturday, Sunday or any day designated as a public holiday for the team managing the Services .

Business Hours: means 9 am to 5 pm Monday to Friday (Business Days).

Confidential Information: The term "Confidential Information" shall mean any confidential information or data disclosed by either Party to the other, pursuant to this Proposal and/or Interim Contract, in whatever form either in writing or in machine-readable form or orally, subject to the conditions set forth in this Agreement, and including without limitation any written or printed documents, samples, models, or any information or data disclosed through any means that the Parties may elect to use during the term of this Agreement.

Customer Data: means data (including Personal Data) controlled by Customer and transmitted to the Solution.
Documentation*:* means the documentation produced by Thales and supplied to the Customer specifying how the Solution should be used.

End-User: means the Customer’s clients who can use the Services provided by the Solution.

Force Majeure: means any event beyond reasonable control of the victim Party, including but not limited to: governmental or public authority decision, act or omission, war (whether declared or not), hostilities, insurrection, act of terrorism, sabotage, fire, flood, explosion, epidemics, quarantine restriction, disruption in the supply of supplies from normally reliable sources (including but not limited to electricity, water, fuel and similar supplies), strikes, plant closures and labor disputes, suspension or revocation of any license, permit or authorization, embargoes, storms, earthquakes, delay of a subcontractor due to Force Majeure as defined above.

Group: means collectively or individually Thales and Affiliates of Thales.

High Risk Activities: means activities where the failure of the Services could lead to death, serious personal injury, or severe environmental or property damage.

Indemnified Liabilities means any (i) settlement amounts approved by the indemnifying party, and (ii) damages and costs finally awarded against the indemnified party and its Affiliates if relevant by a court of competent jurisdiction.

Intellectual Property Rights: mean all patents, patent applications, including with respect to patents and patent rights granted upon any reissue, division, continuation or continuation-in-part applications now or hereafter filed, utility models issued or pending, registered and un-registered design rights, copyrights (including the copyright on software in any code), trade secrets, know-how, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, neighboring rights and other similar statutory intellectual property or industrial rights (registered or unregistered), as well as applications for any such rights.

Network: means any network infrastructures fixed and radio used by the Customer and not provided by Thales.

Personal Data: means (i) data which relate to a living individual (whether in personal or family life, business or profession) who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, as well as (ii) information that can be utilized to identify or trace an individual's identity including but not limited to name, address, social security number, biometric data, date of birth, etc.

Required Consents: means any consents or approvals required to give the right to access the network or third Parties' facilities or third Party Services provider trusted Services manager or license to use, execute, reproduce, display, perform, distribute copies of, and modify software and/or otherwise use any intellectual property rights, Services, products, equipment, programs, materials, to the extent necessary for the purpose of the delivery of the Services.

Services(s): means the Thales Services described in this Commercial Proposal.

Solution: means the solution used to perform the Services as described in the present Commercial Proposal.

Specifications: means the Customer Requirement Specifications agreed between the Parties and the Supported Specifications.

Suspend or Suspension means disabling access to or use of the Services or components of the Services.

Thales Data: all data generated, stored or collected by the Services and/or Solution which is not Customer Data. Thales Data includes, but is not limited to, clicks, impressions, page views, interaction data, and any data stored or collected by the Services and/or Solution.

DATA PROTECTION CLAUSE WHEN THALES IS PROCESSING PERSONAL DATA ON BEHALF OF ITS CUSTOMERS
-
(THALES ACTING AS PROCESSOR AND CUSTOMER AS CONTROLLER)

"**Applicable Data Protection Legislation**"	means any Personal Data protection regulation, law, order, standard and other text that applies in the context of the performance of the Interim Contract, in particular (i) the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) howsoever incorporated into national laws and (ii) any other laws or regulations relating to the Processing of Personal Data.
"Binding Corporate Rules" or "BCR"	means the Thales Binding Corporate Rules which have been approved by decision No. 2023-145 dated 21st December 2023 of the French supervisory authority and which are applicable where Thales is acting as Data Processor. The Thales Binding Corporate Rules are accessible by clicking on the following link: https://www.thalesgroup.com/en/binding-corporate-rules.
"Customer"	means the entity receiving the Commercial Proposal
"Customer Personal Data"	means any Personal Data provided or made available to Thales by Customer and Processed by Thales under this DPA.
"**Data Controller**"	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
"Data Processing Agreement" or "DPA"	means this data processing agreement and its appendices.
"**Data Processor**"	means the entity acting on behalf of the Data Controller.
"**Data Subject**"	means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
"**EEA**"	means the European Economic Area.
"**Personal Data**"	means any information relating to a Data Subject.

“**Personal Data Breach**”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
“**Processing” or “Processed**”	means 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.
“Processing Activities”	means the Processing activities described in a document called “Subject Matter and Details of the Data” attached to the Commercial Proposal.
“Purpose”	Means the purpose for which Customer Personal Data is Processed by Thales as detailed in a document called “Subject Matter and Details of the Data” attached to the Commercial Proposal.
“Sub-Processors”	means a Data Processor of subsequent rank engaged by the Data Processor.
“Thales”	means Thales entity issuing the Commercial Proposal
“Thales Company”	means Thales SA, a French limited company having its registered office at 4, rue de la Verrerie, 92190 Meudon, France, registered with the Register of Trade and Companies of Nanterre, France, under number 552 059 024 and/or any legal entity that is controlled either directly or indirectly by Thales SA. For the purpose of this definition, "control" means Thales SA holding, either directly or indirectly, more than fifty percent (50%) of the economic rights or voting rights of the concerned legal entity.
“Third Country”	means a country outside the combined territories of the EEA and the UK as listed in a document called “Subject Matter and Details of the Data” attached to the Commercial Proposal which list may be amended from time to time.
“UK”	means the United Kingdom.

1. PURPOSE OF THE DPA

The DPA defines the terms and conditions applicable to the Processing of Customer Personal Data by Thales for the Purposes described in a document called “Subject Matter and Details of the Data” attached to the Commercial Proposal.

2. QUALIFICATION AND ROLES OF THE PARTIES

Within the context of the DPA, Customer shall act as Data Controller and Thales shall act as Data Processor.

Acting as Data Processor, Thales shall carry out the Processing of Personal Data received from Customer only on Customer’s documented instructions, including with regard to transfers of Customer Personal Data to a Third Country or an international organization, unless required to do so by applicable law to which Thales is subject. In such case, Thales shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

The Parties shall comply with their respective obligations under Applicable Data Protection Legislation.

3. THALES OBLIGATIONS

Thales shall implement technical and organizational measures to ensure the security of Customer Personal Data against Personal Data Breaches. In assessing the appropriate level of security, Thales shall take due account of the state of the art, the costs of implementation, the nature, scope, context and Purpose of Processing and the risks involved for the Data Subjects

The security measures designed and defined by Thales are described in Appendix A to the DPA “*Security Measures”* and Customer has confirmed their appropriateness to the above mentioned criteria.

Thales shall also:

- ensure that Thales’ personnel authorized to carry out Processing of Customer Personal Data are committed to confidentiality obligations;
- assist Customer, insofar as this is possible, taking into account the nature of the Processing Activities, for responding to requests from Data Subjects to exercise their rights laid down in the Applicable Data Protection Legislation;
- taking into account the nature of the Processing Activities and the information available to Thales, provide reasonable assistance to Customer in ensuring compliance with Customer’s obligations set out in Applicable Data Protection Legislation, in particular :
    - the obligation for Customer to carry out a data protection impact assessment where the Processing is likely to result in a high risk to the rights and freedoms of the Data Subjects;
    - the obligation for Customer to consult the competent supervisory authority/ies prior to Processing where the data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken to mitigate the risk;
    - the obligation for Customer to ensure that Personal data is accurate and up to date for which Thales shall inform Customer if it becomes aware that such Personal Data it is Processing is inaccurate or has become outdated;
- immediately inform Customer in writing if it believes that a Customer’s instruction with respect to the Processing of Customer Personal Data infringes the Applicable Data protection Legislation; and

Finally, upon termination or expiration of the Interim Contract, Thales shall, at the choice of Customer, delete all Customer Personal Data and certify to Customer that it has done so, or, return all Personal Data to Customer and delete existing copies, unless otherwise required by applicable laws.

4. PERSONAL DATA BREACH

In the event of a Personal Data Breach concerning Customer Personal Data Processed by Thales, Thales shall notify Customer without undue delay after Thales having become aware of the Breach.

Such notification shall contain, at least:

- a description of the nature of the Personal Data Breach;
- the details of a Thales contact point where more information concerning the Personal Data Breach can be obtained;
- its likely consequences and the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

Thales shall provide Customer with necessary information to assess and document the Personal Data Breach as well as to notify supervisory authorities and/or Data Subjects of a Personal Data Breach under Applicable Data Protection Legislation.

5. AUDIT

Customer's right to audit. Upon request and subject to Thales security requirements, Thales shall allow Customer to perform audits of compliance by Thales with its obligations in relation to the Processing of Customer Personal Data, as required under Applicable Data Protection Legislation.

Thales shall contribute to such audits by providing Customer with the information and assistance reasonably necessary to demonstrate compliance with the present DPA and with Applicable Data Protection Legislation.

Choice of auditor. The audit may be carried out by Customer or by an independent third party appointed by Customer and approved by Thales.

In case Customer appoints a third party auditor to conduct the audit, Customer shall execute a written confidentiality agreement with said third-party auditor including confidentiality obligations substantially similar to those contain in the applicable confidentiality agreement between Thales and Customer, or otherwise be bound by a statutory confidentiality obligation before conducting the audit.

Terms and conditions of the audit. Except in case of a Personal Data Breach, audits may not be carried out more than every two (2) years.

Audits shall not interfere in any way with Thales business activities and shall be conducted during regular business hours at the applicable facility or remotely, subject to the agreed final audit plan and Thales Security requirements as above mentioned. Furthermore, unless otherwise provided by applicable laws, audits shall not permit access, in particular intrusive access (e.g. penetration tests) to the information systems and applications of Thales and/or its service providers.

Thales and Customer shall discuss and agree in advance on a reasonable start date for the audit with a minimum thirty (30) calendar days' previous notice from Customer's request to carry out an audit.

If the requested audit scope has already been addressed in a similar audit report issued by a qualified third-party auditor within the prior twelve (12) months and Thales provides such report to Customer confirming there is not any known material change in the audited check points, Customer agrees to accept the findings presented in the third-party audit report in lieu of requesting an audit of the same check points as the ones covered by the report.

Audit report. Customer shall send a copy of the audit report to Thales. The audit report shall be considered as confidential information. Customer shall use the audit reports only for the purposes of meeting its regulatory audit obligations.

Audit Fees. Audits shall be carried out at Customer's costs. Thales is not responsible for any costs incurred by Customer or any fees charged by any third-party auditor in connection with an audit except in the case where the audit would reveal that Thales has failed to comply with the DPA and/or Applicable Data Protection Legislation. In the latter case, Thales shall reimburse Customer with all costs incurred by Customer for performing the audit, upon presentation of proof thereof.

Thales' Sub-Processors. Unless otherwise provided by applicable laws, this audit clause shall not apply to the audit of Thales' Sub-Processors. Thales shall, ensure that Thales has substantially similar audit rights towards its Sub-processors.

6. SUB-PROCESSORS

Customer hereby gives a general authorization to THALES to share Customer Personal Data with Sub-Processors, for the sole purpose of performing the Processing Activities, it being understood that THALES shall inform Customer of any changes of Sub-Processors by any means (including by email), thereby giving CLIENT the opportunity to object to such changes in writing , by sending an e-mail to mcsdataprivacy@thalesgroup.com, for legitimate reasons and within thirty (30)

calendar days from the date of Thales' notification. In the absence of an objection within this thirty (30) calendar days' period, the change shall be deemed approved.

THALES commits to have its Sub-Processors comply with Applicable Data Protection Legislation, on the same terms as those set out in this Data Processing Agreement.

THALES shall remain fully liable to CLIENT for the performance of the Sub-Processors' obligations.

7. TRANSFERS OF PERSONAL DATA OUTSIDE THE EEA

Customer acknowledges that Thales may transfer Customer Personal Data out of the EEA to the Third Country(ies) specified in a document called "Subject Matter and Details of the Data" attached to this Commercial Proposal which list of may be amended by Thales from time to time by informing Customer as described in Article 6 above.

Where Customer Personal Data is transferred by a Thales Company established in the EEA or in the UK to another Thales Company established in a Third Country that has not been recognized as providing an adequate level of protection by an adequacy decision of the European Commission or the UK Parliament, as appropriate, such transfer shall be based on Thales BCR.

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

Where Customer Personal Data is transferred by a Thales Company established in the EEA to a third-party established in a Third Country that has not been recognized as providing an adequate level of protection by an adequacy decision of the European Commission, such transfer is framed by the European Union Standard Contractual Clauses (SCC) adopted by the European Commission or by other appropriate safeguards, in compliance with the Applicable Data Protection Legislation.

Where Personal Data is transferred by a Thales Company established in the UK to a third-party established in a Third Country that has not been recognized as offering an adequate level of protection by the UK Parliament, such transfer relies on either the International Data Transfer Agreement (IDTA) or the SCC as amended by the International Data Transfer Addendum issued by the Information Commissioner's Office to facilitate the transfer.

8. PROCESSING OF CONTACT DETAILS FOR THE ADMINISTRATIVE MANAGEMENT OF THE COMMERCIAL PROPOSAL & INTERIM CONTRACT

In the context of the Interim Contract, the Parties shall process personal data for the purpose of administrative management and exchange of information relating to the performance of the Interim Contract.

Those personal data include contact details of employees and/or third parties involved in the performance and/or administrative management of the Commercial Proposal and the Interim Contract, such as their surname, first name, professional identifier, position, professional e-mail address, place of work and telephone number.

The Parties respectively determine the purpose and means of the aforementioned processing, each in its capacity as data controller.

The Parties shall comply with the applicable data protection legislation.

The Parties shall only process personal data which is strictly necessary for the fulfilment of the above mentioned purpose.

The Parties shall inform the aforementioned data subjects of the processing of their personal data.

To this end, the information notice for processing of contact details under Thales agreements is available online by clicking on the following link: https://www.thalesgroup.com/en/information-notice-processing-contact-details-under-thales-agreements.

Appendix A - Security Measures

1 Technical and Organizational measures to ensure the security of the data

Thales security program aims at ensuring that in the current context of our international activities, Thales follows the data protection laws and regulations in the jurisdictions in which we are conducting business.
Thales security program aims at:

- identifying through risk analysis, potential threats to Customer information;
- implementing security solutions (both processes and tools) to limit risks to our systems;
- training our employees and third-party service providers to implement our security program;
- monitoring the security of our systems and processes in operation;
- providing clear information on the processing of Customer information;
- responding to Customer queries and request on the protection of their information;
- preparing ourselves in case of crisis

The following paragraphs describe in more details our security program that is split in two chapters:

(1) the common security corpus applicable to all transfers;

(2) the technical and organizational measures which may not be applicable to all transfers.

1.1 Common applicable security measures

Thales security program governance is:

- Based on the several policies applicable to all Thales' affiliated entities as well as to all Thales employees, employees of third-party services providers and external people servicing or dealing with our Information System.
- Under the responsibility of the Security Department and IT department and locally under the management of designated security and IT manager.
- Periodically reviewed and its application is checked during local and central security audits. Furthermore, technical security audits are undertaken at central and local level. The frequency of such audits varies in light of the security level, sensitivity and vulnerability of the system.

Thales security program concentrates on the following elements:

Reference	Description
PII_Classif	**Personal Information Identification and Classification** The purpose of the personal information identification and classification policy is to establish a system of priorities for protecting information and assets, in order to ensure that protection levels are commensurate with the value of the information or system being protected throughout their lifecycle, from elaboration to destruction. The use of classification levels allows the organization to focus protection costs on information of the highest value. This policy covers the following main elements: • Establish Thales rules for the management of information, in respect with its sensitivity; • Protection of the area where information is located is in adequacy with the information classification level; • Restricted logical access to computers and networks follow the same rules as physical access restrictions; • Recording of the reception of physical media containing confidential information; • Rules for the transmission of information; • Rules for physical, electronic and media storage; • Rules for destruction; • Clean desk policy rule.

PHY_policy	**Physical and Environmental Security Policy** Setting the primary means of defence against theft or misuse of products and services supplied by Thales and are required to protect our know-how. They are also a protection for our personnel. This policy covers the following main elements: Applicable to all Thales sites. A site is a physical location where Thales employees are based or where Thales operations are conducted; Each Thales site must comply with defined minimal security features in accordance with their domains of activity and the identified risks of their processes; Each Thales site is subject to regular audit performed by the Central Security Team to verify compliance with the policy; Each Thales site has a security manager; Each Thales site is organized in different zone levels classified according to the security services they offer.
CMSS_policy	**Configuration Management System Security Policy** Designed to establish Thales security rules for the management of software during their development and when they are delivered. This policy covers the following main elements: Major security topics: confidentiality, integrity, availability, accountability and traceability; Software management through an IT tool called a Configuration Management System (CMS); Applicability to all Thales DIS employees, consultants, or contractors working within Thales facilities or connected via networks or remote access; Implementation of this policy is checked during local and central security audits; Roles and responsibilities in the application of this policy is allocated to a wide number of Thales's employees, comprised of security personal and personal involved in the development and management of software; Rules setting restricted access to the room where sensitive software is stored; Rules addressing the use of encryption to assure confidentiality; Integrity of the software files is of the utmost importance.
SEC_rules	**Security Rules for Sub-contracting Software development** In addition to the Configuration Management System Security Policy, Thales has designed a policy addressing the acquisition of third parties software development services. This policy aims at assuring the confidentiality of the information provided to the service provider. This policy covers the following main elements: Defining security levels establishing a level of risk in light of the software security sensitivity; Complying with our approach on security by design framework for any development; Validation by Thales security personnel of the service provider's physical and logical configurations; The information made available to the service provider is previously classified by Thales in accordance with the personal information identification and classification policy. Based on such classification the service provider is bound to implement the applicable Thales' rules.
Key Management	**Keys management** *Encryption keys and certificates are used to protect communications and sensitive application data and are also used inside the access control system.* *The encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and are considered robust* *They are managed by a very limited number of people, operating according to a rigorous process providing a high level of integrity. This ensures very detailed tracking of the keys' lifecycle and anticipates their expiration dates and renewal. Keys are stored securely. Certificates are delivered by an external public or internal public key infrastructure (PKI) system depending on the usage.* The security of the key management is ensure during the whole life cycle (generation, usage, storage, renewal and deletion) of the key & certificates.

IS_Sec_Controls	**1.2.1 Information System ("IS") Security Controls in Operation** Designed to (a) enlighten the IS security principles are valuable for key strategic elements, such as the stakes, the referential, the business security needs and miscellaneous threats and (b) ensure that our security requirements are in accordance with our customers' requirements. These controls cover the following main elements: • **Information system user access** Access to the information systems follows a principle of "need to access" and implies the user fulfills a series of obligations regarding access rules, compliance with access limits and/or privileges, use of information processing resources, etc. Depending on their role and area of work, users may have restricted access to outside communication. Account creation is validated by management according to a process handling the full lifecycle of the account, depending on user status: employee, subcontractor or outsourcer staff. Thales follows a strong access control policy which is based on separation of duties, strong password policy and least privilege. • **System administration** The administration functions and privilege accesses are granted according to dedicated, restrictive rules. Any usage of an administration function is individually accountable with no repudiation mechanism and is planned with the Production Manager in order to protect service delivery continuity. Any generic privilege accounts (root, Administrator) is using in dual control with split of password principle (one IT team member and one security team member). Remote administration is done through a Jump Gateway with two-factor authentication. • **Audit logs management** All administrative, privileges access (Data base administration) and users activities done across any of the solution interfaces (login attempts, accounts management, failed activities, granting privileges etc.) and all activities affecting personally identifiable information (PII), are recorded in log files. Audit logs are designed and collected in order to allow consistent monitoring of the information security of multiple solution components. • **Penetration testing** Penetration tests are performed against the whole solution (infrastructure, core services, product and customization, including interfaces to customer back-end and various communication channels). They are directed according to known and maintained attack schemes coming from industry and from our security expertise. Penetration testing take place as soon as a solution is integrated and are performed again when it is deployed in a production environment within operational infrastructure configuration and settings. They are done before the commercial launch and then periodically after that (Some tests impact the service). Where a change is applied inside a sensitive component of the operated solution, penetration tests are rerun to insure the security level is maintained. • **Vulnerability management** Software vendors consider that around 65% applications are patched to fix vulnerabilities within a few days of the alert being raised. The vulnerabilities of IT infrastructure component, common middleware, open source components and software from serious software vendors are monitored and fixed. Alerts are raised with patch notifications. The same approach is performed internally by Thales DIS R&D for shared software components. Identification of components used by all solutions is essential to target and control security patch deployment. An organization inside the central security department makes the bridge between alerts and solutions to be patched. Production Managers are accountable to maintain the relevant security patch level.

	Thales DIS's vulnerability watch process ensures that alerts are recorded and security patches deployed on the solutions. Installation and infrastructure hardening rules are defined and applied. Applications configuration applies guidelines to restrict the accesses and the permissions to who it is strictly required. • **Computer Emergency Response Team (CERT)** Thales has set-up a centralized organization to reinforce the prevention and protection against Cyber security risks. The Computer Emergency Response Team (CERT) from Thales is an organization that reinforces the prevention and protection against Cyber security risks. The Thales CERT is made of several experts in Cyber defense, Cyber criminality and Incident Response, encompassing forensics, network investigations and penetration testing. Our experts are certified: GIAC Forensics, Malware Reverse Engineering, Ethical Hacking, depending on their scope of responsibilities. This organization operates according to RFC2350 which specifies the expectations for Computer Security Incident Response. Thales CERT RFC2350 Thales CERT is recognized and accredited by Trusted Introducer consortium.
Monitoring	**Monitoring** The auditlogs are analyzed both manually and in an automated way based on patterns characterizing suspicious behavior. This later analysis is performed in near real time and raises alarms. Audit logs also provide first level investigation capabilities which are completed by other methods in case forensics are needed. The reports are automatically generated on request on a weekly and monthly basis to control and detect suspicious behaviors. This task is performed both at the infrastructure level with a dedicated team and at the application team with the project team.
Maintenance	**Maintenance** Policies and procedures ensure that any maintenance of IT system hosting personal data are not leaving the controlled premises without the proper management of the stored data (external maintenance resources are under constant surveillance, maintenance company is binding by contract to respect the Thales rules…).

1.2 Technical Controls applicable depending on the concerned transfer

In that section out of the main security of the security program and the associated controls, a complimentary list of technical controls are detailed as relevant for the provided Solutions and Services.

Reference	Description
IS_MFA	**1.2.1 Information system user access specific to application** Application is using strong authentication based on Multi-Factor Authentication or split password under dual control.
Auth_Transit_App	**1.2.2 Application has limited access to protected resource based on token (authentication, authorization)** Authentication / authorization controls apply at the application level to obtain limited access to a protected resource, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and an authorization service, or by allowing the application to obtain access on its own behalf.
ENC_Transit_Com A	**1.2.3 Encryption in Transit at communication level (A)** All personal data in transit is protected by transport layer security (TLS) configured as state of the art for all the HTTP protocol, and provide effective protection against active and passive attacks with resources known to be available to the public authorities of these third countries in line with the EDPB's recommendations. The encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into

	account the resources and technical capabilities (e.g., computing power for brute-force attacks). The management of the keys & certificate is defined in subsection "Keys management" above.
ENC_Transit_Com B	**1.2.4 Encryption in Transit at communication level (B)** A secure communication channel is set upped when possible (depend on the use case) between the trusted actors/ components to exchange the personal data. It can be done applying a VPN based on IPSEC standard or through a TLS mutual authentication protocol. The encryption algorithm and its parameterization follow the same principle as mentioned above.
ENC_Transit_App	**1.2.5 Encryption in Transit at application level** Out of the encryption in transit implemented, a complimentary encryption layer is applied at the application level. The personal data is processed using strong encryption before transmission. The encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks). The management of the keys & certificate is defined in subsection "Keys management" above. Furthermore the strength of the encryption and key length take into account the specific time period during which the confidentiality of the encrypted personal data is preserved. The decryption key associated is in the sole custody of Thales and its affiliates which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organization for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured, The identity of the exporter and the importer are verified.
ENC_Rest_Infra	**1.2.6 Encryption at Rest at infrastructure level** Once the data is transferred to be store, an encryption mechanisms of Customer personal data including backups is applied using cryptographic keys that remain under our control. Thales uses FIPS 140-2-approved cryptographic devices managed by CSP Key Management Service (KMS) so as to handle the full life cycle of the key under Thales's control. All cryptographic keys generated by the CSP for Thales in the EEA remain and are usable solely in the EEA. The encryption algorithms and their parameterization conform to the state-of-the-art and are implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified in line with the EDPB's recommendations. The management of the certificate is defined in subsection "Keys management" above.
ENC_Rest_App (A)	**1.2.7 Encryption at Rest at application level (A)** Out of the encryption at rest implemented at the infrastructure level a complimentary encryption layer is applied at the application level. The feature permits to protection the customer personal data within the solution and applied with regard to the nature of the personal data. It's then enabling the encryption at rest. The personal data are then encrypted end-to-end (E2E) on the application layer using state-of-the-art encryption methods in the sense of EDPB.

	Thales uses FIPS 140-level 2 cryptographic devices managed solely by Thales Key Management Service (KMS) so as to handle the full life cycle of the key and the hardware associated under Thales's control. All cryptographic keys generated in the EEA remain and are usable solely in the EEA. The encryption algorithms and their parameterization conform to the state-of-the-art and are implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified in line with the EDPB's recommendations. The management of the keys is defined in subsection "Keys management" above.
ENC_Rest_App (B)	**1.2.8 Encryption at Rest at application level (B)** Out of the encryption at rest implemented at the infrastructure level a complimentary encryption layer is applied at the application level. The feature permits to protection the customer personal data within the solution and applied with regard to the nature of the personal data. It's then enabling the encryption at rest. The personal data are then encrypted end-to-end (E2E) on the application layer using state-of-the-art encryption methods in the sense of EDPB. Thales uses cryptographic software managed solely by Thales Key Management Service (KMS) so as to handle the full life cycle of the key and the application under Thales's control. All cryptographic keys generated in the EEA remain and are usable solely in the EEA. The encryption algorithms and their parameterization conform to the state-of-the-art and are implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified in line with the EDPB's recommendations. The management of the keys is defined in subsection "Keys management" above.
ENC_Rest_App (C)	**1.2.9 Encryption at Rest at application level (C)** Out of the encryption at rest implemented at the infrastructure level a complimentary encryption layer is applied at the application level. The feature permits to protection the customer personal data within the solution and applied with regard to the nature of the personal data. It's then enabling the encryption at rest. The personal data are then encrypted end-to-end (E2E) on the application layer using state-of-the-art encryption methods in the sense of EDPB. Thales uses FIPS 140-2-approved cryptographic devices managed by CSP Key Management Service (KMS) to protecting the encryption key involved at the application level so as to handle the full life cycle of the key under Thales's control. All cryptographic keys generated in the EEA remain and are usable solely in the EEA. The encryption algorithms and their parameterization conform to the state-of-the-art and are implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified in line with the EDPB's recommendations. The management of the keys is defined in subsection "Keys management" above.
Pseudonymization	**Pseudonymization** Thales for such personal data is able to apply the pseudonymization where the personal data are processed in such a manner that the personal data can no longer be attributed to a specific data subject. Such feature can be ensuring thanks to masking mechanisms or hash mechanisms where respectively the look-up table or the cryptographic key involved are not accessible by the supporting maintenance team located in the data importer country thanks to access control restriction in line with the EDPB's recommendations.

1.3 Organizational Controls applicable depending on the concerned transfer

In that section out of the main security of the security program and the controls associated, a complimentary list of organizational controls are detailed as relevant for the provided Solutions and Services.

Reference	Description
Governance	**Governance** For data governance, several practices are in place: • Guidelines, policies and standards are available to support privacy requirements; • Data and data processing activities are cataloged; • Data lifecycle is managed; • Data access and usage are defined and monitored
Awareness	**Privacy awareness** Every user of the IS has to be trained in information security practices relevant to their use of Thales information and systems. Testing of user knowledge is tracked. Human Resources department is responsible for orientation of all new employees in basic information security principles. Direct managers are responsible for informing each employee, through awareness programs, about information security policy, standards and procedures. IT managers are responsible for job specific technical training of IT team. Security department is responsible for training, certification and tracking of information security practices. Specific eLearning is in place to train all the Thales employees on the privacy rules in line with the GDPR including the knowledge of what is a personal data what are the controls to protect, what to do in case of data breach or in case of particular public authority request...
Audit	**Internal Audit** An internal audit plan is setup to ensure the regular check as part of Thales DIS governance. Several controls are done; among them, some are covering the active data protection process, the logical and the physical accesses to personal data, the incident management process. The compliance to the policies is verified.
Data Minimization (A)	**Data Minimization (A)** The data access to limited at few records for performing the support. The Access Control List is Role Based Access Control and restricts the access to a subset of information according the profile of the person performing the support. The audit trail of the access is kept, see "Audit logs management chapter" above. A process of audit to verification the proper implementation of the data minimization is also in place.
Data Minimization (B)	**Data Minimization (B)** Out of the standard data minimization mentioned above some complimentary data minimization are implemented. The remote access to EEA data, such as in support cases, is done with restricted access instead of full access to avoid full export to database. Furthermore, by design, the collected data are limited to the strict number of items relevant to the query for ensuring the service to the customer.
Data Minimization (C)	**Data Minimization (C)** Out of the standard data minimization mentioned above some complimentary data minimization are implemented . In order to limit exchange of potential personal data on the ticketing system using free text, a pre-selected entry filed is defined.
Retention	**Data Retention** In the context of data processing taking place for the performance of a contract (i.e. provision of a service), it is important to distinguish between two types of data before defining their respective retention periods: • commercial and transactional data: those data can be retained in an active database for the full duration of the contract. At the end of the contract, they can be archived physically (on a separate medium: DVD,

	etc.) or logically (by authorization management) in the event of possible litigation. Thereafter, at the end of the statutory limitation periods, the data are deleted or anonymized; • usage data: usage data can be classified as raw data and aggregated data. As stated above, if possible, data controllers or processors should not process raw data. If it is necessary, raw data are kept only as long as they are required to elaborate the aggregated data and to check the validity of that aggregation process. Aggregated data are kept as long as it is necessary for the provision of the service or otherwise requested by a Union or Member State law.
Transparency	**Transparency and accountability measures** The requests for access received from public authorities and the response provided are recorded, alongside the legal reasoning and the actors involved (e.g. if the exporter has been notified and its reply, the assessment of the team in charge of dealing with such requests, etc.). These records are made available to the data exporter, who is in charge to provide them to the data subjects concerned. For transparency, the publication of reports or summaries regarding governmental requests for access to data are regular, including the kind of reply provided, insofar publication is allowed by local law.

SCHEDULE GOVERNING LAW AND JURISDICTION

Country	Contracting Thales Entity	Governing Law	Place of Arbitration
Argentina	THALES ARGENTINA SA	Argentina	Buenos Aires - Argentina
Australia	THALES DIS AUSTRALIA PTY LTD	State of New South Wales - Australia	Sydney - Australia
Brazil	Thales DIS Brasil Cartões e Soluções Tecnológicas Ltda	Brazil	Sao Paulo - Brazil
Canada	THALES DIS CANADA, Inc	Province of Ontario - Canada	Toronto - Ontario
China	THALES DIS (SHANGHAI) Co, Ltd	People's Republic of China	Shangai - China
Colombia	THALES COLOMBIA SA	Colombia	Bogota - Colombia
Denmark	THALES DIS DANMARK A/S	Denmark	Copenhagen - Denmark
Finland	THALES DIS FINLAND OY	Finland	Helsinki Finland
France	THALES DIS FRANCE SAS	France	Paris - France
Germany	THALES DIS DEUTSCHLAND GmbH	Germany	Munich - Germany
Hong Kong	THALES DIS HONG KONG LIMITED	Hong Kong Special Administrative Region	Hong Kong
India	THALES DIS INDIA PRIVATE LIMITED	India	Delhi - India
Indonesia	PT THALES DIS INDONESIA	Indonesia	Singapore
Italy	THALES DIS ITALIA S.p.A	Italy	Milan - Italy
Japan	THALES DIS JAPAN KK	Japan	Tokyo - Japan
KSA	GEMALTO ARABIA LTD	KSA	Riyadh - KSA
Malaysia	THALES DIS (MALAYSIA) SDN BHD	Malaysia	Singapore
Mexico	THALES DIS MEXICO SA DE CV	Mexico	Mexico City - Mexico
Netherlands	GEMALTO BV	The Netherlands	Amsterdan - the Netherlands
New Zealand	GEMALTO (NZ) LIMITED	New Zealand	Auckland - New Zealand
Norway	THALES DIS NORGE AS	Norway	Oslo - Norway
Poland	THALES DIS POLSKA Sp. Z.o.o	Poland	Warsaw - Poland
Singapore	THALES DIS (SINGAPORE) PTE LTD	Singapore	Singapore
South Africa	GEMALTO SOUHTERN AFRICA PTY LTD	South Africa	Johanesburg - South Africa
Spain	THALES DIS ESPANA SPAIN SA	Spain	Madrid - Spain
Sweden	THALES DIS SWEDEN AB	Sweden	Stockholm - Sweden
Switzerland	Thales DIS Schweiz AG	Switzerland	Aarau - Switzerland
Thailand	THALES DIS (THAILAND) LTD	Thailand	Singapore
UAE	THALES DIS MIDDLE EAST FZ LLC	UAE	Dubai - UAE
UAE	GEMALTO GENERAL TRADING LLC	UAE	Dubai - UAE
UK	THALES DIS UK LIMITED	England	London - England
USA	THALES DIS USA, INC	State of New York - USA	New York - USA

Country	Thales Entity	Governing Law	Place of Arbitration
Argentina	THALES ARGENTINA SA	Argentina	Buenos Aires - Argentina
Australia	THALES DIS AUSTRALIA PTY LTD	State of New South Wales - Australia	Sydney - Australia
Brazil	Thales DIS Brasil Cartões e Soluções Tecnológicas Ltda	Brazil	Sao Paulo - Brazil

Canada	THALES DIS CANADA, Inc	Province of Ontario - Canada	Toronto - Ontario
China	THALES DIS (SHANGHAI) Co, Ltd	People's Republic of China	Shangai - China
Colombia	THALES COLOMBIA SA	Colombia	Bogota - Colombia
Denmark	THALES DIS DANMARK A/S	Denmark	Copenhagen - Denmark
Finland	THALES DIS FINLAND OY	Finland	Helsinki Finland
France	THALES DIS FRANCE SAS	France	Paris - France
Germany	THALES DIS DEUTSCHLAND GmbH	Germany	Munich - Germany
Hong Kong	THALES DIS HONG KONG LIMITED	Hong Kong Special Administrative Region	Hong Kong
India	THALES DIS INDIA PRIVATE LIMITED	India	Delhi - India
Indonesia	PT THALES DIS INDONESIA	Indonesia	Singapore
Italy	THALES DIS ITALIA S.p.A	Italy	Milan - Italy
Japan	THALES DIS JAPAN KK	Japan	Tokyo - Japan
KSA	GEMALTO ARABIA LTD	KSA	Paris - France
Malaysia	THALES DIS (MALAYSIA) SDN BHD	Malaysia	Singapore
Mexico	THALES DIS MEXICO SA DE CV	Mexico	Mexico City - Mexico
Netherlands	GEMALTO BV	The Netherlands	Amsterdan - the Netherlands
New Zealand	GEMALTO (NZ) LIMITED	New Zealand	Auckland - New Zealand
Norway	THALES DIS NORGE AS	Norway	Oslo - Norway
Poland	THALES DIS POLSKA Sp. Z.o.o	Poland	Warsaw - Poland
Singapore	THALES DIS (SINGAPORE) PTE LTD	Singapore	Singapore
South Africa	GEMALTO SOUHTERN AFRICA PTY LTD	South Africa	Johanesburg - South Africa
Spain	THALES DIS ESPANA SPAIN SA	Spain	Madrid - Spain
Sweden	THALES DIS SWEDEN AB	Sweden	Stockholm - Sweden
Switzerland	Thales DIS Schweiz AG	Switzerland	Aarau - Switzerland
Thailand	THALES DIS (THAILAND) LTD	Thailand	Singapore
UAE	THALES DIS MIDDLE EAST FZ LLC	France	Paris - France
UAE	GEMALTO GENERAL TRADING LLC	France	Paris - France
UK	THALES DIS UK LIMITED	England	London - England
USA	THALES DIS USA, INC	State of New York - USA	New York - USA