GEHC PRIVACY AND DATA PROTECTION APPENDIX

In the event of inconsistency or conflict between this appendix (hereinafter, “Appendix” or “PDPA”) and the Contract Document with respect to a Privacy and Data Protection subject covered by this Appendix, the provisions governed by this Appendix shall prevail. The requirements in this Appendix are in addition to any confidentiality obligations between GEHC and the Supplier under the Contract Document. This Appendix is also applicable to Supplier affiliates when required under Contract Document.

THE PARTIES HEREBY AGREE AS FOLLOWS:

1. **DEFINITION**

1.1 For the purposes of the PDPA,

(a) the terms "Controller", “Joint-Controller”, “Data Subjects”, “Processing”, "Personal Data", "Personal Data Breach", "Processor", “Sub-Processor” and “Supervisory Authority” will have the meaning given to them by Applicable Law.

(b) “**Affiliate**” means any entity, including, any individual, corporation, company, partnership, limited liability company or group, that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with GEHC.

(c) “**Applicable Law**” means all regional, national and international applicable laws , relating to the protection of individuals with regards to the processing of personal data or other requirements with similar effect of any governmental or data protection authority, each as updated from time to time which apply to the Parties in the circumstances governed by the Contract Document and that limit, restrict or otherwise govern the collection, use, access, security, storage, protection, and disclosure of personal data.

(d) “**Contract Document**” shall mean the agreement between GEHC and Supplier, which, for the avoidance of doubt, may include a signed agreement or purchase order, as applicable.

(e) “**GEHC**” shall mean GE HealthCare Technologies Inc. or any of its Affiliates or subsidiaries responsible for the protection of any of the Personal Data governed by this Appendix. GEHC or the applicable GEHC Affiliate responsible for the protection of any of the Personal Data governed by this Appendix may enforce the terms of this Appendix.

(f) “**Supplie**r” shall mean Supplier and Supplier affiliates, collectively.

(g) **“Supplier Personnel**” shall mean Supplier, its subcontractors and their respective employees, agents, sub-tier suppliers and representatives.

1.2 In this PDPA:

(a) the neuter gender shall include the masculine and the feminine;

(b) the singular number shall include the plural and vice versa;

(c) references to persons shall include individuals, bodies corporate, unincorporated associations and partnerships;

(d) the headings are inserted for convenience only and shall not affect the construction of this PDPA; and

(e) references to recitals, sections, appendixes and annexes and sub-divisions thereof, unless a contrary intention appears, are to the recitals and sections of and appendixes and annexes to this PDPA and sub-divisions thereof respectively.

2. COMPLIANCE WITH APPLICABLE LAWS

2.1 The Parties shall process Personal Data in accordance with all Applicable Laws.

2.2 In the event of a conflict between the provisions of an Applicable Law and the terms of this PDPA, then the Parties shall endeavour (as far as reasonably possible) to comply with the terms of this PDPA but without contravening the Applicable Law.

2.3 In the event of any conflict between the provisions of the Contract Document and this PDPA, then the provisions of this PDPA shall prevail.

2.4 Each Party represents and warrants that its performance under the Contract Document and this PDPA will not cause the other Party to be in violation of any Applicable Law. Each Party will promptly notify the other Party and cooperate with it if it believes that it may no longer be able to comply with any of the terms of this PDPA. In the event of any conflict between the provisions of the Contract Document and this PDPA, then the provisions of this PDPA shall prevail.

2.5 **Covered Person Status and Restriction on Onward Transfers - U.S. Sensitive Personal Data**. Supplier represents and warrants that it is not a Covered Person or Country of Concern, as defined under 28 C.F.R. Part 202. Capitalized terms used in this Section 2.5 have the meanings afforded to them under 28 C.F.R. Part 202. Supplier further represents and warrants that it (i) will not disclose or otherwise provide Access to U.S. Sensitive Personal Data processed under the Contract Document to any Covered Person or Country of Concern, regardless of whether the U.S. Sensitive Personal Data is pseudonymized, anonymized, de-identified, encrypted, or otherwise subject to security measures, unless authorized in writing by GEHC; (ii) will not engage in any transaction involving Data Brokerage of U.S. Sensitive Personal Data processed under the Contract Document with any Covered Person or Country of Concern, regardless of whether the U.S. Sensitive Personal Data is pseudonymized, anonymized, de-identified, encrypted, or otherwise subject to security measures; (iii) will conduct reasonable due diligence to assess counter-party Covered Person status for compliance with this Section 2.5; (iv) will report violations of this Section 2.5 to GEHC within 24 hours of becoming aware of the same by providing the information listed in 28 C.F.R. § 202.302(b)(2)(ii), and promptly update such notice thereafter as appropriate; and (v) will provide information to and cooperate with GEHC as reasonably necessary to facilitate compliance with 28 C.F.R. Part 202. Supplier will indemnify, defend, and hold harmless GEHC and its subsidiaries, affiliates, officers, directors, and employees against third-party claims arising from Supplier's negligent or intentional non-compliance with this Section 2.5, which indemnification obligations shall not be subject to any limitation on liability provided in the Contract Document. If Supplier becomes a Covered Person during the term of the Contract Document, Supplier will immediately notify GEHC, and GEHC shall have the right to immediately terminate the Contract Document without further obligation to Supplier. Upon such termination, Supplier will fully cooperate with GEHC to wind-down the services or any terminated portion thereof for compliance with 28 C.F.R. Part 202. This Section 2.5 shall survive the expiration or termination of the Contract Document.

3. ALLOCATION OF ROLES AND RESPONSIBILITIES

3.1 The provisions of Section 4 shall apply in all cases where the Supplier is acting as a Processor and is Processing Personal Data on behalf of GEHC when GEHC is acting as a Controller.

3.2 The provisions of Section 5 shall apply in all cases where GEHC is acting as Processor and Supplier is acting as Sub-Processor of GEHC.

3.3 The provisions of Section 6 shall apply in all cases where both Parties are acting as Joint-Controllers.

3.4 The provisions of Section 7 shall apply in all cases where both Parties are acting as independent Controllers.

4. **OBLIGATIONS BETWEEN CONTROLLER AND PROCESSOR**

4.1 **Obligations of Processor**

(a) This Section concerns situations where Supplier is acting as Processor and GEHC is acting as Controller.

(b) Following Instructions of GEHC. Supplier shall carry out Processing activities on the Personal Data in accordance with the instructions of GEHC as set forth in this PDPA and as communicated in writing via letter, email, or other electronic means capable of visual display and retention from time to time. Where Supplier is required to carry out Processing activities on Personal Data by any Applicable Laws, regulations, or governmental authority and, therefore, is required to comply with a regulatory request for disclosure, Supplier shall notify GEHC in writing via email or other electronic means prior to complying with any such requirement, unless the Applicable Laws, regulations, or governmental authority prohibit the providing of such notice, and in such case Supplier shall comply with all reasonable directions of GEHC with respect to such Processing Activities. Supplier shall not assume any responsibility for determining the purposes for which and the manner in which Personal Data is processed.

(c) Supplier's Personnel. Supplier shall (i) take reasonable steps to ensure the reliability of any of its Supplier Personnel in charge of the processing under the authority of the Supplier, who will have access to the Personal Data; (ii) ensure that all of its Supplier Personnel who have access to the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (iii) ensure that none of its Supplier Personnel process Personal Data except on instructions from GEHC, unless they are required to do so by Applicable Law; and (iv) provide training as necessary from time to time to all of its Supplier Personnel with respect to its obligations in this PDPA and under Applicable Law to ensure that its staff are aware of and comply with such obligations.

(d) Processing Solely for the Purpose. Supplier shall carry out Processing Activities on the Personal Data solely for the purposes as set out in the Contract Document and in the manner specified by GEHC in the Appendixes, attached hereto. Supplier shall not carry out Processing Activities on Personal Data for any other purpose or in any other manner, nor shall Supplier carry out Processing Activities on more Personal Data than are necessary to fulfil the Purposes. Supplier will ensure that any Personal Data created by the Supplier on behalf of GEHC is accurate and, where appropriate, kept updated, and ensure that any Personal Data which is inaccurate or incomplete is erased or rectified in accordance with GEHC's instructions.

(e) Disclosure to Third Parties. Supplier shall not disclose or transfer Personal Data to any third party other than a Sub-Processor pursuant to Section 4.2 of this PDPA without the prior permission in writing or via email, or other electronic means of GEHC.

(f) Exercise of Data Subjects' Rights. Supplier shall notify GEHC within five (5) business days of any communication received from any individual relating to that individual's rights such as to access, modify or correct Personal Data relating to him or her and shall comply with all instructions of GEHC in responding to such communications. In addition, Supplier shall provide any and all assistance required by GEHC to respond to any communication received

by either GEHC or Supplier from any individual relating to that individual's rights on Personal Data relating to him or her.

(g) Security. Supplier shall adopt technical and organisational measures necessary to ensure the security of the Personal Data to prevent the carrying out of unauthorized Processing Activities on or unauthorised access to them and to prevent their alternation or loss. These technical and organisational measures shall have regard to the state of the art, the nature of the Personal Data, and the risks to which the Personal Data are exposed by virtue of human action or the physical or natural environment. For avoidance of doubt, Supplier shall implement the security measures according to current GE HealthCare Third Party Cyber Security Requirements (available at https://www.gehealthcare.com/about/suppliers/terms-and-conditions) and comply with the security requirements set forth in the Applicable Laws to which Supplier is subject. Supplier shall inform GEHC immediately, but not later than forty-eight (48) hours after the discovery of any Personal Data Breach. Supplier shall, without undue delay, make available to GEHC details of the Personal Data Breach and shall use commercially reasonable efforts to investigate and prevent the recurrence of such Personal Data Breach. The details provided by Supplier to GEHC shall at least include:

(1) A description of the type of the Personal Data Breach including, the time and date of the security incident, and if possible, the categories and approximate number of individuals affected by said Personal Data Breach and the categories and the approximate amount of Personal Data records in question;

(2) The name and contact details of the data privacy officer of the Supplier from whom further information can be obtained;

(3) A description of the likely consequences of the Personal Data Breach;

(4) A description of the measures taken to remedy the Personal Data Breach, including, where appropriate, measures to mitigate any negative consequences.

The notification must be sent to 3PS.GEHCSECURITY@gehealthcare.com.

GEHC, at its sole discretion, shall determine whether and when to notify any individuals or persons (including governmental authorities) regarding any Personal Data Breach. Supplier shall co-operate with GEHC's defence relating to any Personal Data Breach processed by Supplier.

(h) Transfers. Supplier warrants to adopt appropriate safeguards before performing any international data transfers, where it is required by Applicable Law, including the execution of additional agreements required by Applicable Law.

(i) Compliance with the Applicable Laws. Supplier shall comply with all provisions of the Applicable Laws applicable to it.

(j) Privacy Impact Assessment. Supplier shall assist GEHC carrying out any privacy impact assessments ("**PIA**") on the protection of Personal Data required by the Applicable Law and with respect to any prior consultation of a competent Supervisory Authority, if the Processing is likely to result in a high risk to the rights and freedoms of the Data Subjects concerned.

(k) Return or deletion of the Personal Data. Upon GEHC's request, upon the termination or expiration of the Contract Document or whenever Supplier no longer needs to retain all or part of Personal Data in order to perform the obligations under the Contract Document, Supplier shall, at GEHC's option, immediately return or destroy that Personal Data. In the event that GEHC opts to have Supplier to destroy that Personal Data, Supplier shall destroy

it using a final, secure and complete method that will render that Personal Data permanently unrecoverable. Upon GEHC's request, Supplier shall certify in writing that it has completed the destruction of that Personal Data. If Applicable Laws to which Supplier is subject prevents Supplier from returning or destroying all or part of the Personal Data, Supplier warrants that it will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore, and will guarantee the return and/or destruction of the Personal Data as requested by GEHC when the legal obligation to not return or destroy the information is no longer in effect.

(l) Audit of Supplier's Processing Activities by GEHC. Supplier agrees that GEHC, or a third-party inspector designated and paid for by GEHC, may inspect, with reasonable notice and during normal business hours, Supplier's carrying out of Processing Activities on the Personal Data. Supplier shall furnish GEHC or such third-party inspector with all materials, documents and other information necessary for GEHC to confirm that Supplier has complied with its obligations under this PDPA, provided that GEHC shall only use such information for the Purposes specified in this Section 4 and for no other purpose. GEHC reserves the right to conduct its own security and vulnerability assessment if relevant information provided are not sufficient to confirm Supplier's compliance with GEHC security requirements. Supplier further agrees to respond promptly to all reasonable enquiries from GEHC regarding the carrying out of Processing Activities on the Personal Data.

(m) Audit Remediation. If during an audit a security vulnerability is discovered, GEHC and Supplier shall work expeditiously and in good faith to agree on a plan to remediate such security vulnerability ("**Remediation Plan**"). Once the Parties agree on a Remediation Plan, Supplier shall execute and complete the Remediation Plan without unreasonable delay and notify GEHC when that Remediation Plan is complete. Notwithstanding anything to the contrary elsewhere in the Contract Document, GEHC may conduct a follow-up inspection within six (6) months of Supplier's notice of completion of the Remediation Plan. To the extent that an audit identifies any material security vulnerabilities, Supplier shall remediate those vulnerabilities within fifteen (15) days of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

4.2 **Sub-Processors**

(a) Engaging Sub-Processors. Supplier may engage a Sub-Processor to assist it in fulfilling its obligations, provided that it complies with the provisions set out in this Section 4.2 and imposes provisions in a contract executed with the Sub-Processor that are not less stringent than those detailed in Section 4. Supplier will remain fully liable to GEHC for the performance of the Sub-Processor's obligations. Supplier will provide a list of its Sub-Processors to GEHC. In case of modifications to this list, it will inform GEHC promptly so that GEHC can indicate whether it objects to the modifications to the list of Sub-processors.

(b) Transfer of Data to Sub-Processors. If Supplier wishes to transfer Personal Data to a Sub-Processor, it shall be permitted to do so, provided that, (i) it has adopted appropriate safeguards before performing any international data transfers, where it is required by Applicable Law, (ii) it notifies GEHC, in accordance with clause 11, of the name and contact details of the Sub-Processor and that it enters into a sub-processing data processing agreement, which shall be in line with the provision of this PDPA. Supplier shall be permitted to grant sub-processing rights to the Sub-Processor; provided that if such Sub-Processor engages itself a sub-processor (a "**Sub-Sub-Processor**"), it shall respect the obligations set forth in this Section 4.2.

(c) Assumption of Obligations. If a Sub-Processor fails to fulfil the obligations set forth in its written data processing agreementwith Supplier, then Supplier shall assume and be liable for those obligations. It is also the Supplier's responsibility to ensure that the Sub-Processor provides sufficient guarantees as to the implementation of appropriate technical and organisational measures to ensure that the Processing meets the requirements of the Applicable Laws.

(d) Revocation of powers. GEHC may at any time revoke the powers granted to Supplier under this Section 4.2 if Supplier breaches this Section 4.2 or if any necessary regulatory approvals have not been obtained or have been, or will be, revoked (as the case may be).

4.3 **Obligations of Controller**

(a) Responding to Inquiries. GEHC shall respond in a reasonable time and to the extent reasonably possible to inquiries from any Supervisory Authority relating to the carrying out of Processing Activities on the Personal Data by Supplier, and to any inquiries from any individual concerning the carrying out of Processing Activities on Personal Data relating to him or her by Supplier.

(b) Providing Instructions. GEHC shall provide Supplier with instructions relating to the Purpose and the Processing of Personal Data. These instructions shall be sufficiently clear to allow Supplier to meet its obligations under this PDPA. Beyond issuing instructions to Supplier necessary to fulfilling the Purposes, GEHC's instructions will not otherwise materially alter the way by which Supplier performs its activities beyond what is necessary to protect Personal Data in accordance with Applicable Laws. In particular, GEHC's instructions may govern the use of Sub-Processors, the disclosure of Personal Data and other obligations of Supplier pursuant to Section 4.2.

(c) Providing Information about Applicable Laws. Supplier shall inform GEHC about all amendments to its national data protection law and related statutory instruments, regulations, orders, and similar instruments that are of relevance to the Processing performed by Supplier under this PDPA and provide information on how Supplier is complying with such amendments.

5. **OBLIGATIONS BETWEEN PROCESSORS**

5.1 This Section concerns situations where GEHC is acting as Processor and Supplier is acting as Sub-Processor of GEHC.

5.2 Obligations of Supplier as Sub-Processor. In these situations, the obligations mentioned in Sections 4.1 and 4.2 of the PDPA applies to Supplier.

5.3 Transfers. Supplier shall not transfer Personal Data to any non-adequate country or make any Personal Data accessible from any such non-adequate Country without the prior written consent of GEHC.

5.4 Compliance with the Applicable Laws. Both GEHC and Supplier shall comply with all provisions of the Applicable Laws applicable to it.

6. **OBLIGATIONS BETWEEN JOINT-CONTROLLERS**

6.1 This Section concerns situations where both GEHC and Supplier are acting as Joint-Controllers.

6.2 Purposes and Means of the Processing. GEHC and Supplier jointly determine the purposes and means of the Processing. Each of them is responsible for Processing Personal Data under the scope of this PDPA in accordance with the requirements set out in the Applicable Laws.

6.3 Information of Data Subjects. The Supplier is responsible for providing the Data Subjects with the information required by Applicable Law and commits to provide such information in compliance with Applicable Law.

6.4 Data Subjects' rights. Both GEHC and Supplier are responsible for fulfilling the rights of Data Subjects regarding the Processing of their Personal Data. Each of them shall designate a data protection point of contact for Data Subjects. In case one of them has information necessary to answer a Data Subject's request, it shall provide the other without undue delay the necessary information to answer this Data Subject's request under the defined terms as per Applicable Law.

6.5 Security. It is the responsibility of both GEHC and Supplier to process Personal Data falling under the scope of this PDPA. Both GEHC and Supplier shall implement appropriate technical and organizational measures to ensure an appropriate level of data security.

6.6 Cooperation between Joint-Controllers. GEHC and Supplier shall assist each other in complying with requests or complaints of Data Subjects or data protection authorities regarding compliance with the obligations under the Applicable Law. They will notify each other of any requests, enquiries, monitoring activities and similar measures undertaken by Supervisory Authorities regarding the Processing. They shall further notify each other of actual or potential errors, irregularities, omissions or suspected infringements of provisions relating to the protection of Personal Data under the scope of this PDPA.

6.7 Notification of Personal Data Breach. In case of a Personal Data Breach, the Controller, either GEHC or the Supplier, under whose responsibility the Personal Data Breach occurred must report it to the other Controller. If necessary, the concerned Controller is responsible for reporting the Personal Data Breach to the competent data protection authority and/or the affected Data Subjects in compliance with Applicable Law. Where it may be unclear under which Controller's responsibility the Personal Data Breach occurred, GEHC and Supplier shall assess the situation in good faith and cooperate and determine the next steps together.

6.8 Privacy Impact Assessment. GEHC and Supplier shall assist each other to carry out any privacy impact assessments ("PIA") on the protection of Personal Data required by the Applicable Law and with respect to any prior consultation of a competent Supervisory Authority if the Processing is likely to result in a high risk to the rights and freedoms of the Data Subjects concerned.

6.9 Processing or Disclosure Required by Applicable Law. Where one Controller, either GEHC or Supplier, is required to carry out Processing Activities on Personal Data or to disclose Personal Data by any Applicable Laws, regulations, or governmental authority, it shall notify the other Controller in writing via letter, email, or other electronic means prior to complying with any such requirement, unless the Applicable Laws, regulations, or governmental authority prohibit the providing of such notice.

6.10 **Transfers**. GEHC and Supplier shall adopt appropriate safeguards before performing any international data transfers, where it is required by Applicable Law, including the execution of additional agreements required by Applicable Law (e.g., the EU Standard Contractual Clauses).

6.11 Compliance with the Applicable Laws. Both GEHC and Supplier shall comply with all provisions of the Applicable Laws applicable to it.

7. OBLIGATIONS BETWEEN INDEPENDENT CONTROLLERS

7.1 This Section concerns situations where GEHC and Supplier are acting as independent Controllers.

7.2 Purposes and Means of the Processing. GEHC and Supplier each determine the purposes and means of their own Processing of Personal Data. They are not receiving instructions from each other and they do not jointly determine the purposes and means of Personal Data Processing. Each of them is responsible for its own Processing of Personal Data under the scope of this PDPA in accordance with the requirements set out in the Applicable Laws.

7.3 Information of Data Subjects. GEHC and Supplier are each responsible for providing the Data Subjects with the information required regarding their own Processing Activities, and in compliance with Applicable Law.

7.4 Data Subjects' rights. Both GEHC and Supplier are responsible for fulfilling the rights of Data Subjects regarding the Processing of their Personal Data. Each of them shall designate a data protection point of contact for Data Subjects.

7.5 Security. It is the responsibility of both GEHC and Supplier to process Personal Data falling under the scope of this PDPA. Both GEHC and Supplier shall implement appropriate technical and organizational measures to ensure an appropriate level of data security to their own Processing of Personal Data.

7.6 Notification of Personal Data Breach. Each Controller is responsible for reporting, when required by Applicable Law, to the competent data protection authority and/or the affected Data Subjects in compliance with Applicable Law the Personal Data Breach it suffered.

7.7 Privacy Impact Assessment. Each Controller is responsible for carrying out any PIAs on the protection of personal data required by the Applicable Law, and with respect to any prior consultation of a competent Supervisory Authority if the Processing is likely to result in a high risk to the rights and freedoms of the Data Subjects concerned.

7.8 **Transfers**. GEHC and Supplier shall each adopt appropriate safeguards before performing any international data transfers, where it is required by Applicable Law, including the execution of additional agreements required by Applicable Law.

7.9 Compliance with the Applicable Laws. Both GEHC and Supplier shall comply with all provisions of the Applicable Laws.

8. REPRESENTATIONS, WARRANTIES, INSPECTIONS AND INDEMNITIES

8.1 **Indemnity**. Supplier indemnifies and shall hold harmless GEHC against any and all costs, charges, damages, expenses and losses (including costs incurred in recovering same) that are incurred by any breach of sections of this PDPA by the Supplier, its Supplier Personnel, or, if applicable, of any action by a Supplier's Sub-Processor that would constitute a breach of this PDPA. The provisions of this section shall survive termination of this PDPA.

8.2 Risk of Loss in Transfer. Each Party shall bear the risk of loss associated with any loss (including any alteration, degradation or corruption) of Personal Data caused by any transfer to or from another Party, except to the extent any such losses arise out of the negligence, wilful misconduct, or breaches of this PDPA by the Party or out of any third party having been provided access to Personal Data, including a Sub-Processor if applicable.

8.3 Insurance. Each Party shall maintain appropriate Cybersecurity and Privacy Liability Insurance throughout the term of the Contract Document.

9. DUTIES OF CONFIDENTIALITY

9.1 The Parties acknowledge that Personal Data in their possession or under their control may constitute or contain information which is of a confidential or otherwise sensitive nature. The Parties will not disclose or transfer Personal Data in contravention of any Applicable Laws or any duties of confidentiality, whether such duties arise under law, by PDPA, by the Contract Document or otherwise. **The termination of this PDPA will not affect any duties of confidentiality** owed by the Parties. The Parties undertake to take all appropriate and reasonable measures to ensure that their employees, including but not limited to those having access to the Personal Data are aware and are bound by the requirements and obligations of confidentiality set out in this Section.

10. SUPERVISORY AUTHORITIES

10.1 The Parties shall cooperate with each other in order to ensure that Supervisory Authorities receive information to which they are entitled under Applicable Laws and shall also assist each other to observe the requirements or directions of any Supervisory Authorities.

11. SEVERABILITY

11.1 If and to the extent that any provision of this PDPA is held to be illegal, void or unenforceable in any jurisdiction, such provision shall be given no effect in that jurisdiction, but without invalidating any of the remaining provisions of this PDPA.

APPENDIX 1A: DATA PROCESSING – IT

This Appendix describes the data processing and applies whenever the Contract Document is related to services which include, among others, cloud, hardware, IT, software and telecom services. Nevertheless, the nature of the processing, the categories of personal and sensitive data and the categories of data subjects shall always be limited only to the extent necessary to perform the contract document.

DESCRIPTION OF PROCESSING

Categories of data subjects

	Categories of data subjects		
1.	**Current Employees (including managers, directors, executives, interns and trainees, implants and secondees, and expats) and/or ex-employees**	☒ **YES**	☐ **NO**
2.	**Relatives / Beneficiaries**	☒ **YES**	☐ **NO**
3.	**Job Applicants / Candidates**	☒ **YES**	☐ **NO**
4.	**Commercial Contacts (B2B), Suppliers / Vendors / Contractors, (including their representatives and signatories)**	☒ **YES**	☐ **NO**
5.	**Visitors / Attendees / Students**	☒ **YES**	☐ **NO**
6.	**Users and subscribers**	☒ **YES**	☐ **NO**
7.	**Patients**	☒ **YES**	☐ **NO**
8.	**Passengers**	☒ **YES**	☐ **NO**
9.	**Existing / Prospective Customers**	☒ **YES**	☐ **NO**
10.	**Minors / Children**	☒ **YES**	☐ **NO**
11.	**Other vulnerable categories (*e.g.* elderly people, victims of domestic violence, refugees or asylum seekers)**	☒ **YES**	☐ **NO**
12.	**Other (please specify):**_____		

Categories of personal data

	Categories of personal data transferred		
1.	**National ID number / Passport number**	☒ **YES**	☐ **NO**
2.	**Social Security Identification number**	☒ **YES**	☐ **NO**
3.	**Identification data (e.g. name, address, date of birth, phone number, vehicle number plate, driver license, client number, employee number, signature…)**	☒ **YES**	☐ **NO**
4.	**Electronic identification data (e.g. email addresses, IP addresses, MAC addresses, logs, e-signature and/or certificates, advertising identifiers, social network identifiers such as handles, information collected and stored via cookies or other similar technologies…)**	☒ **YES**	☐ **NO**

	Categories of personal data transferred		
5.	Profiles (assessment of the data subject with integration in a class or a prediction of a certain characteristic or a certain behaviour)	☒ YES	☐ NO
6.	Personal characteristics (e.g. age, sex, marital status, size, weight, appearance, physical marks)	☒ YES	☐ NO
7.	CRM data (e.g. information about customers, their needs, contacts, communication, level of satisfaction…)	☒ YES	☐ NO
8.	Lifestyle, click patterns, search and/or navigation history, payment history	☒ YES	☐ NO
9.	Physiological data (*e.g.* personality, character…)	☒ YES	☐ NO
10.	Household composition	☒ YES	☐ NO
11.	Hobbies and interests	☒ YES	☐ NO
12.	Social Media profiles (personal and/or professional)	☒ YES	☐ NO
13.	Affiliations / Memberships	☒ YES	☐ NO
14.	Consumption habits	☒ YES	☐ NO
15.	Products and services (*e.g.* credit card number, account number, insurance policy number, statement of products, salary and income, expenses, consumption, maintenance, VAT number…)	☒ YES	☐ NO
16.	Housing and/or vehicle characteristics	☒ YES	☐ NO
17.	Geolocation data	☒ YES	☐ NO
18.	Studies and/or training / Certifications / Awards / Publications / Referrals	☒ YES	☐ NO
19.	Profession/occupation and employment history, status, and referrals	☒ YES	☐ NO
20.	Photos or image recordings (e.g. CCTV, surveillance camera, registered training, VoIP services…)	☒ YES	☐ NO
21.	Sound recordings (e.g. voice, telephone / VoIP conversations, training…)	☒ YES	☐ NO
22.	HR data: salary and staff presence, evaluations, KPI's, career plan, appraisals, references , and personnel control data (e.g. logging, whistleblower regulations, warrants, insider trading prevention, complaints management and quality control…)	☒ YES	☐ NO
23.	Security related information: physical security data regarding customers, staff and visitors (e.g. authorizations and access rights/privileges, clearance levels); ICT security data related to clients, staff and visitors (e.g. example permissions and rights, use of a badge, Internet access, user credentials such as user names and passwords, security tokens, multi-factor authentication, etc.)	☒ YES	☐ NO
24.	Customer control data (e.g. fraud prevention, AML and terrorist financing, KYC, sanctions list…)	☒ YES	☐ NO

	Categories of personal data transferred
25.	Other (please specify):_____

Sensitive data

	Sensitive data		
1.	Racial or ethnic origin	☐ YES	☒ NO
2.	Political opinions	☐ YES	☒ NO
3.	Religious or philosophical beliefs	☐ YES	☒ NO
4.	Trade union membership	☐ YES	☒ NO
5.	Genetic data (e.g. DNA, blood type…)	☐ YES	☒ NO
6.	Biometric data (e.g. fingerprints, iris / hand recognition, bone scintigraphy…)	☐ YES	☒ NO
7.	Health-related data	☐ YES	☒ NO
8.	Sex life or sexual orientation	☐ YES	☒ NO
9.	Criminal / administrative convictions and / offences re. data (including security measures)	☐ YES	☒ NO
10.	Other (please specify):_____		

Nature of the processing

	Nature of processing		
1.	Collection	☒ YES	☐ NO
2.	Organization	☒ YES	☐ NO
3.	Recording and / or storage	☒ YES	☐ NO
4.	Alteration, adaptation or redaction	☒ YES	☐ NO
5.	Retrieval	☒ YES	☐ NO
6.	Pseudonymization and / or anonymization	☒ YES	☐ NO
7.	Consultation, and/or alignment	☒ YES	☐ NO
8.	Combination	☒ YES	☐ NO
9.	Blocking	☒ YES	☐ NO
10.	Erasure and / or destruction	☒ YES	☐ NO
11.	Disclosure (either by transmission, dissemination or otherwise making available)	☒ YES	☐ NO

	Nature of processing
12.	**Other (please specify):**_____

APPENDIX 1B – HR

This Appendix describes data processing and applies whenever the Contract Document is related to human resources services, such as, but not limited to payroll and trainings. Nevertheless, the nature of the processing, the categories of personal and sensitive data and the categories of data subjects shall always be limited only to the extent necessary to perform the contract document.

DESCRIPTION OF PROCESSING

Categories of data subjects

	Categories of data subjects		
1.	**Current Employees (including managers, directors, executives, interns and trainees, implants and secondees, and expats) and/or ex-employees**	☒ **YES**	☐ **NO**
2.	**Relatives / Beneficiaries**	☒ **YES**	☐ **NO**
3.	**Job Applicants / Candidates**	☒ **YES**	☐ **NO**
4.	**Other (please specify):**_____		

Categories of personal data

	Categories of personal data transferred		
1.	**National ID number / Passport number**	☒ **YES**	☐ **NO**
2.	**Social Security Identification number**	☒ **YES**	☐ **NO**
3.	**Identification data (e.g. name, address, date of birth, phone number, vehicle number plate, driver license, client number, employee number, signature…)**	☒ **YES**	☐ **NO**
4.	**Electronic identification data (e.g. email addresses, IP addresses, MAC addresses, logs, e-signature and/or certificates, advertising identifiers, social network identifiers such as handles, information collected and stored via cookies or other similar technologies…)**	☒ **YES**	☐ **NO**
5.	**Profiles (assessment of the data subject with integration in a class or a prediction of a certain characteristic or a certain behaviour)**	☒ **YES**	☐ **NO**
6.	**Personal characteristics (e.g. age, sex, marital status, size, weight, appearance, physical marks…)**	☒ **YES**	☐ **NO**
7.	**Lifestyle, click patterns, search and/or navigation history, payment history**	☒ **YES**	☐ **NO**
8.	**Physiological data (*e.g.* personality, character…)**	☒ **YES**	☐ **NO**
9.	**Household composition**	☒ **YES**	☐ **NO**
10.	**Hobbies and interests**	☒ **YES**	☐ **NO**
11.	**Social Media profiles (personal and/or professional)**	☒ **YES**	☐ **NO**

	Categories of personal data transferred		
12.	Affiliations / Memberships	☒ YES	☐ NO
13.	Consumption habits	☒ YES	☐ NO
14.	Products and services (*e.g.* credit card number, account number, insurance policy number, statement of products, salary and income, expenses, consumption, maintenance, VAT number…)	☒ YES	☐ NO
15.	Housing and/or vehicle characteristics	☒ YES	☐ NO
16.	Geolocation data	☒ YES	☐ NO
17.	Studies and/or training / Certifications / Awards / Publications / Referrals	☒ YES	☐ NO
18.	Profession/occupation and employment history, status, and referrals	☒ YES	☐ NO
19.	Photos or image recordings (e.g. CCTV, surveillance camera, registered training, VoIP services…)	☒ YES	☐ NO
20.	Sound recordings (e.g. voice, telephone / VoIP conversations, training…)	☒ YES	☐ NO
21.	HR data: salary and staff presence, evaluations, KPI's, career plan, appraisals, references , and personnel control data (e.g. logging, whistleblower regulations, warrants, insider trading prevention, complaints management and quality control…)	☒ YES	☐ NO
22.	Security related information: physical security data regarding customers, staff and visitors (e.g. authorizations and access rights/privileges, clearance levels); ICT security data related to clients, staff and visitors (e.g. example permissions and rights, use of a badge, Internet access, user credentials such as user names and passwords, security tokens, multi-factor authentication, etc.)	☒ YES	☐ NO
23.	Other (please specify):_____		

Sensitive data

	Sensitive data		
1.	Racial or ethnic origin	☒ YES	☐ NO
2.	Political opinions	☒ YES	☐ NO
3.	Religious or philosophical beliefs	☒ YES	☐ NO
4.	Trade union membership	☒ YES	☐ NO
5.	Genetic data (e.g. DNA, blood type…)	☒ YES	☐ NO
6.	Biometric data (e.g. fingerprints, iris / hand recognition, bone scintigraphy…)	☒ YES	☐ NO
7.	Health-related data	☒ YES	☐ NO

8.	**Sex life or sexual orientation**	☒ **YES**	☐ **NO**
9.	**Criminal / administrative convictions and / offences re. data (including security measures)**	☒ **YES**	☒ **NO**
10.	**Other (please specify):_____**		

Nature of the processing

	Nature of processing		
1.	**Collection**	☒ **YES**	☐ **NO**
2.	**Organization**	☒ **YES**	☐ **NO**
3.	**Recording and / or storage**	☒ **YES**	☐ **NO**
4.	**Alteration, adaptation or redaction**	☒ **YES**	☐ **NO**
5.	**Retrieval**	☒ **YES**	☐ **NO**
6.	**Pseudonymization and / or anonymization**	☒ **YES**	☐ **NO**
7.	**Consultation, and/or alignment**	☒ **YES**	☐ **NO**
8.	**Combination**	☒ **YES**	☐ **NO**
9.	**Blocking**	☒ **YES**	☐ **NO**
10.	**Erasure and / or destruction**	☒ **YES**	☐ **NO**
11.	**Disclosure (either by transmission, dissemination or otherwise making available)**	☒ **YES**	☐ **NO**
12.	**Other (please specify):_____**		

APPENDIX 1C – OTHER

This Appendix describes the data processing and applies whenever the Contract Document is related to where the service is not clearly defined within either of the above categories or is a combination of both. Nevertheless, the nature of the processing, the categories of personal and sensitive data and the categories of data subjects shall always be limited only to the extent necessary to perform the contract document.

DESCRIPTION OF PROCESSING

Categories of data subjects

	Categories of data subjects		
1.	**Current Employees (including managers, directors, executives, interns and trainees, implants and secondees, and expats) and/or ex-employees**	☒ **YES**	☐ **NO**
2.	**Relatives / Beneficiaries**	☒ **YES**	☐ **NO**
3.	**Job Applicants / Candidates**	☒ **YES**	☐ **NO**
4.	**Commercial Contacts (B2B), Suppliers / Vendors / Contractors, (including their representatives and signatories)**	☒ **YES**	☐ **NO**
5.	**Visitors / Attendees / Students**	☒ **YES**	☐ **NO**
6.	**Users, and subscribers**	☒ **YES**	☐ **NO**
7.	**Patients**	☒ **YES**	☐ **NO**
8.	**Passengers**	☒ **YES**	☐ **NO**
9.	**Existing / Prospective Customers**	☒ **YES**	☐ **NO**
10.	**Minors / Children**	☒ **YES**	☐ **NO**
11.	**Other vulnerable categories (*e.g.* elderly people, victims of domestic violence, refugees or asylum seekers…)**	☒ **YES**	☐ **NO**
12.	**Other (please specify):**_____		

Categories of personal data

	Categories of personal data transferred		
1.	**National ID number / Passport number**	☒ **YES**	☐ **NO**
2.	**Social Security Identification number**	☒ **YES**	☐ **NO**
3.	**Identification data (e.g. name, address, date of birth, phone number, vehicle number plate, driver license, client number, employee number, signature…)**	☒ **YES**	☐ **NO**
4.	**Electronic identification data (e.g. email addresses, IP addresses, MAC addresses, logs, e-signature and/or certificates, advertising identifiers, social network identifiers such as handles, information collected and stored via cookies or other similar technologies…)**	☒ **YES**	☐ **NO**

	Categories of personal data transferred		
5.	Profiles (assessment of the data subject with integration in a class or a prediction of a certain characteristic or a certain behaviour)	☒ YES	☐ NO
6.	Personal characteristics (e.g. age, sex, marital status, size, weight, appearance, physical marks...)	☒ YES	☐ NO
7.	CRM data (e.g. information about customers, their needs, contacts, communication, level of satisfaction...)	☒ YES	☐ NO
8.	Lifestyle, click patterns, search and/or navigation history, payment history	☒ YES	☐ NO
9.	Physiological data (*e.g.* personality, character...)	☒ YES	☐ NO
10.	Household composition	☒ YES	☐ NO
11.	Hobbies and interests	☒ YES	☐ NO
12.	Social Media profiles (personal and/or professional)	☒ YES	☐ NO
13.	Affiliations / Memberships	☒ YES	☐ NO
14.	Consumption habits	☒ YES	☐ NO
15.	Products and services (*e.g.* credit card number, account number, insurance policy number, statement of products, salary and income, expenses, consumption, maintenance, VAT number...)	☒ YES	☐ NO
16.	Housing and/or vehicle characteristics	☒ YES	☐ NO
17.	Geolocation data	☒ YES	☐ NO
18.	Studies and/or training / Certifications / Awards / Publications / Referrals	☒ YES	☐ NO
19.	Profession/occupation and employment history, status, and referrals	☒ YES	☐ NO
20.	Photos or image recordings (e.g. CCTV, surveillance camera, registered training, VoIP services...)	☒ YES	☐ NO
21.	Sound recordings (e.g. voice, telephone / VoIP conversations, training...)	☒ YES	☐ NO
22.	HR data: salary and staff presence, evaluations, KPI's, career plan, appraisals, references , and personnel control data (e.g. logging, whistleblower regulations, warrants, insider trading prevention, complaints management and quality control...)	☒ YES	☐ NO
23.	Security related information: physical security data regarding customers, staff and visitors (e.g. authorizations and access rights/privileges, clearance levels); ICT security data related to clients, staff and visitors (e.g. example permissions and rights, use of a badge, Internet access, user credentials such as user names and passwords, security tokens, multi-factor authentication, etc.)	☒ YES	☐ NO
24.	Customer control data (e.g. fraud prevention, AML and terrorist financing, KYC, sanctions list...)	☒ YES	☐ NO

	Categories of personal data transferred
25.	Other (please specify):_____

Sensitive data

	Sensitive data		
1	Racial or ethnic origin	☐ YES	☒ NO
2.	Political opinions	☐ YES	☒ NO
3.	Religious or philosophical beliefs	☐ YES	☒ NO
4.	Trade union membership	☐ YES	☒ NO
5.	Genetic data (e.g. DNA, blood type…)	☐ YES	☒ NO
6.	Biometric data (e.g. fingerprints, iris / hand recognition, bone scintigraphy…)	☐ YES	☒ NO
7.	Health-related data	☐ YES	☒ NO
8.	Sex life or sexual orientation	☐ YES	☒ NO
9.	Criminal / administrative convictions and / offences re. data (including security measures)	☐ YES	☒ NO
10.	Other (please specify):_____		

Nature of the processing

	Nature of processing		
1.	Collection	☒ YES	☐ NO
2.	Organization	☒ YES	☐ NO
3.	Recording and / or storage	☒ YES	☐ NO
4.	Alteration, adaptation or redaction	☒ YES	☐ NO
5.	Retrieval	☒ YES	☐ NO
6.	Pseudonymization and / or anonymization	☒ YES	☐ NO
7.	Consultation, and/or alignment	☒ YES	☐ NO
8.	Combination	☒ YES	☐ NO
9.	Blocking	☒ YES	☐ NO
10.	Erasure and / or destruction	☒ YES	☐ NO
11.	Disclosure (either by transmission, dissemination or otherwise making available)	☒ YES	☐ NO

	Nature of processing
12.	**Other (please specify):**_____