HITACHI ENERGY GENERAL TERMS AND CONDITIONS FOR PURCHASE OF IT SERVICES CLOUD SPECIFIC SCHEDULE (2023-1 ITALY)

1. ADDITIONAL DEFINITIONS

In addition to the definitions set out in Clause 1 of the GTC, the following definitions shall apply in this Specific Schedule:

Access Term: means the term for which Customer is to be provided the Cloud Services, as specified in the Order;

Cloud Services: means those Services provided by Supplier which are indicated in the Order as being provided on a "Software as a Service", "Platform as a Service", "Infrastructure as a Service" or "Cloud" basis or where there is a reference to this Specific Schedule in the Order;

Cloud Software: means the computer programs listed in the Order and any Modification which is provided by Supplier during the term of the Contract;

Controller: means the entity determining the purposes and means a of the Processing of Personal Data;

Customer Cloud Content: means data (which may be Customer Materials and include Personal Data) which are stored on, or used, and/or processed by Supplier's computer systems;

Data Subject: means the identified or identifiable natural person to whom Personal Data relates;

Disaster Recovery Plan: means a plan that sets out the procedures to be adopted to enable the recovery or continuation of a Cloud Service following a natural or human-induced disaster, including the procedures to be taken by the Supplier in planning and providing for any such event;

Documentation: means the documentation provided to Customer by Supplier in connection with the Cloud Software, including the Specification and any user manuals or other documentation provided under the Contract, and including any documentation described in the Order;

EEA: means the European Economic Area: the European Union Member States along with Iceland, Liechtenstein and Norway;
EU: means the European Union;

Maintenance Release: means a release of the Cloud Software which corrects faults, adds functionality or otherwise amends or upgrades the Cloud Software;

Modification: means any Maintenance Release or Customer specific modification;

Processing: means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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;

Processor: means the entity which Processes Personal Data on behalf of the Controller;

Security Audit: has the meaning given in Clause 7.3;
Specification: means the specification of the Cloud Services supplied under the Contract as set out in the Order;

2. APPLICATION OF THIS SPECIFIC SCHEDULE

This Specific Schedule shall apply to any Cloud Services to be provided by Supplier, as set out in the Order.

3. IMPLEMENTATION

3.1 Supplier must perform all of the activities assigned to it in the Order and perform all other activities (other than those assigned to Customer in the Order) as necessary to implement the Cloud Services (the "Implementation Services").

3.2 Except as otherwise agreed in the Order, Implementation Services are subject to Customer's acceptance. Supplier shall provide the Implementation Services in a timely manner and so as to ensure that any milestone or deadline dates specified in the Order are met.

3.3 Supplier shall provide Customer with regular progress reports that (in reasonable detail) describe the current status of the Implementation Services and identify any actual or anticipated problems or delays (together with details of all actions being taken or to be taken to remedy such problems or delays).

4. CLOUD SERVICES

4.1 Supplier shall provide the Cloud Services in accordance with the Contract. Supplier must provide the Cloud Services from facilities, and using IT architecture and personnel, that are based in the UK, EU, EEA or Switzerland unless otherwise agreed by Customer in writing.

4.2 Supplier grants to each member of the Customer Group, during the Access Term, a worldwide, royalty-free, non-exclusive license to:

4.2.1 use the Cloud Services;

4.2.2 access and use the Cloud Software via the Cloud Services; and

4.2.3 use the Cloud Software (and the Documentation) in relation to any business activity of the Customer Group.

4.3 Customer may grant a sub-license of its rights under Clause 4.2 to any Third Party Provider for the purpose of such Third Party Provider providing any goods, software and/or services to the Customer Group.

4.4 Customer acknowledges that it has no right, title or interest in the Cloud Software or the Documentation except as set out in the Contract.

4.5 Except as permitted under the Contract, Customer must not:

4.5.1 distribute, sub-license or otherwise transfer all or any part of the Cloud Software to any other person;

4.5.2 where a maximum number of users of the Cloud Service is specified in the Order, allow more than the maximum number of authorised users to access and use the Cloud Service;

4.5.3 use the Cloud Software as a service bureau or in any similar activity for the benefit of any person who is not a member of the Customer Group;

4.5.4 reverse engineer, decompile or disassemble the Cloud Software except as permitted by applicable laws;

4.5.5 remove, obliterate or alter any copyright, proprietary or similar notices on the Cloud Software; or

4.5.6 intentionally access, store, distribute or transmit any viruses or other malicious software, or any material during the course of its use of the Cloud Services that:

4.6 is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

a) facilitates illegal activity;
b) depicts sexually explicit images;
c) promotes unlawful violence;
d) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or
e) in a manner that is otherwise illegal or causes damage or injury to any person or property.

5. CUSTOMER CLOUD CONTENT

5.1 Notwithstanding Clause 10.5 of the GTC:

5.1.1 Customer Cloud Content will be and remain the property of Customer;

5.1.2 Supplier and Supplier's Team shall not be entitled to use or access any Customer Cloud Content; and

5.1.3 Supplier must not use, store, copy, or disclose any Customer Cloud Content except as necessary for the performance of its obligations under the Contract or as otherwise expressly authorised in writing by Customer.

5.2 Supplier must ensure that Supplier's Team (or any other employees, agents or subcontractors of Supplier) do not attempt to access, or allow access to, any Customer Cloud Content to which they are not entitled.

5.3 Immediately on request from Customer and at the end of the term of the Contract Supplier shall overwrite or permanently erase from its computer systems all copies of the Customer Cloud Content (except copies of Customer Cloud Content stored on backups of Supplier's systems that cannot be deleted with reasonable efforts).

5.4 Customer shall indemnify and hold Supplier harmless from and against all costs, claims, demands, liabilities, expenses, damages or losses (including any direct or indirect consequential losses, loss of profit, and all interest, penalties and legal and other professional costs and expenses) arising out of a claim that the provision of Customer Cloud Content to Supplier infringes the Intellectual Property Rights of any third party.

6. CLOUD WARRANTIES

6.1 In addition to any warranties given by Supplier in the GTC, Supplier represents, warrants and undertakes that the Cloud Software as a whole and any individual Modification will:

6.1.1 during the term of the Contract, be free from any material defects; and

6.1.2 comply and perform in accordance with the Documentation.

6.2 Without limiting Clause 6.1, Supplier represents, warrants and undertakes that each Modification will not degrade the functionality or performance of the Cloud Software.

6.3 Supplier represents, warrants and undertakes that, when delivered to Customer or otherwise implemented by Supplier under the Contract:

6.3.1 it will not insert or include, or permit or cause any person or software to insert or include, any Malicious Software into the Cloud Software as a whole or any individual Modification;

6.3.2 it will use up-to-date, industry accepted anti-virus software to check for and prevent any malicious software or viruses being introduced into the Cloud Software as a whole or any individual Modification; and

6.3.3 it will co-operate with Customer to mitigate the effect of any malicious software or viruses found in the Cloud Software as a whole or any individual Modification.

6.4 Supplier represents and warrants that it has obtained, and undertakes that it will maintain during the Access Term, all consents, licenses and permissions required by it to perform its obligations under the Contract.

6.5 Supplier represents, warrants and undertakes that except as otherwise agreed in the Order, the Cloud Services will comply with security standards, controls and requirements as set out in ISO 27001:2013, SOC 1 type II and/or SOC 2 type II including its avail-ability trust principles.

6.6 The remedies set out in Clause 6.2 of the GTC shall apply.

7. CLOUD SECURITY AND AUDIT OBLIGATIONS

7.1 Supplier at its sole cost will cause a licensed provider of attestation and compliance services to provide Customer and its auditors once a year an ISO 27001:2013, a SOC 1 type II and a SOC 2 type II audit report on controls placed in operation and tests of operating effectiveness at Supplier's and Supplier's service providers' facilities with respect to the Cloud Services.

7.2 Any such certifications and audit reports as per Clause 7.1, and any such other information as required by Customer that

Supplier prepares as a standard matter for its other customers, will be pro-vided at no additional cost to Customer.

7.3 Except as otherwise provided in the Order, upon Customer's request (not more than once per calendar year and in addition in case of a security incident, Supplier's non-compliance with its security obligations and/or regulatory requirements) Customer may conduct a security audit to verify Supplier's compliance with its security obligations under the Contract ("Security Audit"). Such Security Audit may be conducted by Customer or a third-party auditor subject to Customer and/or third party auditors agreeing to reasonably acceptable confidentiality terms. Except in case of regulatory requirements or other circumstances that require prompt action, Customer shall provide at least thirty (30) days prior written notice of its intention to conduct a Security Audit. Customer shall conduct the audit in an expeditious manner, within a reasonable time and in a way to not unreasonably disrupt Supplier's day-to-day business operations. Supplier shall reasonably cooperate and provide such documentation and access as reasonably required by Customer to conduct a Security Audit. For the avoidance of doubt, Supplier shall in no event be obliged to provide any information related to other customers.

7.4 Supplier shall comply with the additional security, audit and reporting requirements, if any, specified in the Order.

7.5 Supplier shall apply the Disaster Recovery Plan as set out in Annex 1 to this Specific Schedule.

8. DATA PROTECTION

8.1 In providing the Cloud Services, Supplier is processing Personal Data in a capacity as Processor under the instructions of Customer acting as Controller, in compliance with the Data Processing Annex as set out in Annex 2 to this Specific Schedule.

ANNEX 1
DISASTER RECOVERY PLAN

ANNEX 2

DATA PROCESSING ANNEX ("DPA")

1. CUSTOMER'S INSTRUCTIONS TO SUPPLIER

1.1 Supplier will follow the instructions received from Customer with respect to the Processing of Personal Data.

1.2 Customer instructs Supplier to collect, process and use Personal Data to provide the services as agreed in the Order. Additional instructions may be issued by Customer.

1.3 Supplier shall inform Customer immediately if he considers any instructions to violate applicable data protection laws.

2. OBLIGATIONS OF SUPPLIER

2.1 Supplier shall not use the Personal Data for any purpose other than described in the Order.

2.2 Obligations with respect to Supplier's Personnel

2.2.1 Confidentiality. Supplier shall ensure that its personnel engaged in the Processing of Personal Data under this DPA have been bound to confidentiality and are prohibited, from accessing, processing and/or using any Personal Data without authorization and for purposes other than fulfilling Supplier's contractual obligations vis-à-vis Customer.

2.2.2 Upon Customer's request, Supplier will provide Customer with its standard form personnel data secrecy and confidentiality agreements or template language and if required under an audit or applicable law, evidence that the relevant personnel is indeed obliged by such data secrecy and confidentiality agreements, which survive the termination of personnel engagement.

2.2.3 Reliability. Supplier shall ensure the reliability of any personnel engaged in the Processing of Personal Data.

2.2.4 Supplier will familiarize all individuals having access to the Customer's Personal Data with the data protection provisions relevant to their work.

2.2.5 Limitation of Access: Supplier shall ensure that Supplier's personnel's access to Personal Data is limited to those personnel performing services in accordance with the Order.

2.3 Supplier's assistance to the Customer

Supplier shall reasonably assist Customer in fulfilling their obligations under the GDPR and handling Data Subject requests and claims. This especially applies with regards to:

2.3.1 Customer's obligation to comply with their obligations (with respect to Data Protection Impact assessments and Prior Consultation with a supervisory authority) according to Articles 35 to 36 GDPR;

2.3.2 any request made by a supervisory authority against Custom-er with regard to the Processing of Personal Data under the Order; and

2.3.3 any claim or any inspection or procedure that Customer becomes subject to and that relates to the processing of Personal Data by Supplier.

2.4 Supplier shall inform Customer immediately of any inspections, investigation and/or measures conducted and/or any criminal, administrative or summary offence procedure by a competent authority and relating to Personal Data or regarding the processing of Personal Data in connection with the Order.

2.5 Supplier shall notify Customer immediately of any request for disclosure of Personal Data from a law enforcement authority, intelligence agency or other type of government access request, unless such notification is prohibited under applicable law. With regard to possible access by public authorities to Personal Data transferred to a 'third country' in accordance with section 6.3, governed by the EU Standard Contractual Clauses in Attachment 4, the "Supplementary Measures Appendix" in Attachment 4.A will apply.

2.6 Supplier shall notify the Customer of Supplier's point of contact for all issues related to data privacy and data protection within the scope of the Order.

2.7 Supplier shall monitor the internal processes and upgrade the technical and organizational measures to ensure that processing within his area of responsibility is in accordance with the applicable data protection laws.

3. SUB-PROCESSORS

3.1 Customer consents that Supplier may engage the sub-processors identified in Attachment 3.

3.2 Any sub-processor to whom Supplier transfers Personal Data, even those used for storage purposes, will have entered into written agreements with Supplier that are no less protective than this DPA.

3.3 Except as set forth in the DPA, or as Customer may otherwise authorize in writing, Supplier will not transfer to any third party (not even for storage or remote support purposes) Personal Data Customer provides to Supplier for the purpose described in the Contract.

3.4 Supplier is liable for the acts and omissions of its sub-processors to the same extent Supplier would be liable if performing the services of each sub-processor directly under the terms of this DPA, except as otherwise set forth in the Order.

4. RIGHTS OF DATA SUBJECTS

4.1 Supplier may not on its own authority correct, rectify, remove, restrict, block or export any Personal Data.

4.2 Supplier can either enable Customer to correct, rectify, remove, restrict, block or export their Personal Data, or correct, rectify, remove, restrict, block or export any Personal Data without undue delay, however in no event longer than within ten

(10) days on instructions from Customer.

4.3 If a Data Subject contacts Supplier directly with any inquiry or request, Supplier will inform Customer of the inquiry or request without undue delay. Supplier will reasonably support Customers in dealing with such inquiries or requests.

5. SECURITY BREACH AND NOTIFICATION

5.1 Supplier shall, notify Customer without undue delay after becoming aware of any security breach at Supplier leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise processed by Supplier or its sub-processors.

5.2 The notification shall contain at least:

- a description of the nature of the security breach including, where possible, the categories and approximate number of Data Subjects affected by the breach and the categories and the ap-proximate number of Personal Data records concerned;
- the name and contact details of the data protection officer or other point of contact from whom additional information can be obtained;
- a description of the likely consequences of the security breach;
- a description of the measures taken or proposed by Supplier to remedy the security breach, including, where appropriate, measures to mitigate any negative consequences.

If, and to the extent that it is not possible to provide all this information at the same time, the information may be communicated in a staggered manner without undue delay.

5.3 Customer instructs Supplier to take all measures Supplier deems necessary or helpful to secure the Personal Data processed on behalf of Customer and to minimize any possible adverse con-sequences to the Data Subjects.

6. LOCATION OF PROCESSING AND INTERNATIO-NAL TRANSFERS

6.1 Supplier will process Personal Data exclusively within a Member State of the EU, the EEA or Switzerland. Every processing (including the mere possibility of access) outside these territories requires Customer's prior written consent.

6.2 In addition to the requirement of Customer's approval under 6.1, each and every transfer of data to a state which is not a Member State of either the EU, the EEA or Switzerland shall only occur if the specific conditions of articles 44 et seq. GDPR have been fulfilled. Personal Data may only be transferred to third countries, for which no adequacy decision in accordance with article 45 GDPR has been made, if such transfer can be legitimized by agreeing on the EU Standard Contractual Clauses. Upon Customer's request Supplier will provide said documentation to Customer.

6.3 If and to the extent Personal Data is transferred to a third country, the Parties agree that the EU Standard Contractual Clauses as attached hereto as Attachment 4 shall apply to any such transfer between Customer and Supplier, as well as the "Supplementary Measures Appendix" in Attachment 4.A. For the avoidance of doubt, this also applies to transfers of Personal Data to the United Kingdom if the European Commission has not provided adequacy status to the United Kingdom at the end of the Brexit transitional period.

6.4 Upon Customer's request Supplier shall enter into any additional Data Processing Agreement or additional data protection agreement as required by mandatory data protection law or a competent data protection or other competent authority, or into any updated version of the EU Standard Contractual Clauses with Customer. Supplier shall ensure that its relevant Affiliates or sub-processors shall, upon Customer's request, promptly enter into any such agreement with Customer.

7. TECHNICAL AND ORGANIZATIONAL MEASURES

7.1 Supplier will implement and maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of the Personal Data, as set out in Attachment 2 to this DPA.

7.2 If Supplier, or any sub-processor, falls under Section 702 of the U.S. FISA, Supplier shall implement technical measures to make access to the Personal Data impossible or ineffective. The same applies if Supplier, or any sub-processor, is processing data in a 'third country' where public authorities may request access to the Personal Data, where such access goes beyond what is necessary and proportionate in a democratic society.

7.3 Upon Customer's request, Supplier will provide evidence of the technical and organizational measures' effectiveness through

(i) current auditor's certificates, reports or excerpts from reports pro-vided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor), or (ii) a suitable certification of IT security or data protection auditing (e.g. ISO/IEC 27001).

7.4 The technical and organisational measures are subject to technical progress and further development. Supplier may amend the technical and organizational measures, provided that the new measures do not fall short of the level of security provided by the specified measures and do not cause any disruption or failure of Customer`s IT infrastructure.

7.5 Supplier will not materially decrease the overall security of the Cloud Service during the term of the Order. If Supplier makes a substantial change to the technical and organizational measures, it will notify Customer in due time in advance. Customer has the right to object if it believes that the change does in fact fall short of the level of data protection, is not in line with applicable data protection law or causes an adverse effect on Customer. If Custom-er objects, Supplier will continue to maintain the measures as specified in Attachment 2.

8. RETURN AND DELETION OF PERSONAL DATA

8.1 Upon termination of the Order, Supplier shall in accordance with Customers instruction immediately return or securely delete or overwrite and destroy in a data-protection compliant manner all documents, processing and utilization results, and data sets related to the Order. This shall apply accordingly to any and all test, waste, redundant and discarded data and/or material. The log of the destruction or deletion shall be provided on request.

8.2 Documentation necessary to demonstrate orderly processing of Personal Data in accordance with this DPA shall be stored by Sup-plier beyond termination of the Order for the duration of the respective retention period. Upon Customer's request Supplier will provide said documentation to Customer.

9. MISCELLANEOUS

In the event of any contradictions, the provisions of this DPA shall take precedence over the provisions of the Order.

ATTACHMENT 1

CATEGORIES OF PERSONAL DATA, CATEGORIES OF DATA SUBJECTS AND PURPOSE OF COLLECTION, PROCESSING AND USE OF PERSONAL DATA

This Attachment forms part of the DPA and must be completed by the parties.

Controller

The controller is [PLEASE SPECIFY BRIEFLY THE ACTIVITIES OF PG RELEVANT TO THE TRANSFER]

Processor

The processor is [PLEASE SPECIFY BRIEFLY THE PROCESSOR'S ACTIVITIES RELEVANT TO THE TRANSFER]

Data subjects

The personal data concern the following categories of data subjects

[PLEASE SPECIFY]

Examples are:

Employees including volunteers, temporary, casual and agency contract workers

Candidates for employment at PG, Former employees, Family members of employees

Agents, advisors, freelancers of Customer

Prospects, Customers, Business Partners, Vendors, Partners, Suppliers

Customer's Users authorized by Customer to use the Services

Categories of data

The personal data concern the following categories of data [PLEASE SPECIFY]

Examples are:

Name, first / last
private / business address
private / business Email address
Date of birth
Age
Gender
List of customer's employees and addresses
Records of work or achievements
Newsletter mailing list with email addresses
individual Bank statements
Itemised telephone bills
Online identifiers (e.g. IP addresses, cookies)
Device identifier (e.g. mobile device IDs)
Passport number
Travel Visa info
Driving license number
Credit Card number
Training records
Family data: name of wife, children
Resume /CV
Job Position / Title
Timesheets
Payroll information

Special categories of data (if appropriate)

The personal data concern the following special categories of data

[PLEASE SPECIFY]

Examples are:

Political Opinion
Religious or philosophical belief
Race or ethnic origin
Trade Union membership
Health data
Sex life and sexual orientation
Genetic or biometric data
Facial images and fingerprints
Criminal records

Processing operations

The personal data will be subject to the following basic processing activities

[PLEASE SPECIFY]

[DELETE EXAMPLES THAT ARE NOT APPLICABLE]

ATTACHMENT 2

TECHNICAL AND ORGANIZATIONAL MEASURES

As part of the Services, Supplier agrees that it shall take all necessary steps and security precautions in accordance with world-recognized industry standards and in accordance to Art. 5/1 f and Art. 32 GDPR to minimize the risk of confidentiality, integrity and availability losses of the Customer Information and Personal Data that is processed by Supplier (data processor) to perform the Services.

Supplier shall design, implement and maintain (including a process for regularly testing, assessing and evaluating the effectiveness) Technical and Operational Measures protecting the security of Customer Information and Personal Data while under Supplier's possession, custody or control, that cover at least the areas below:

1. INFORMATION SECURITY POLICIES

1. Supplier shall develop and maintain appropriate Information Security Policies, aligned to best industry standards and the GDPR, that protect Supplier's information systems from loss, damage, unauthorized disclosure and all other data breaches or disruption of business, including any Customer Information and Personal Data, obtained by Supplier to provide the Services.

2. ORGANIZATION OF INFORMATION SECURITY

1. Supplier shall retain suitably qualified personnel, with clearly defined roles and responsibilities, within their information security organization, to coordinate the implementation of security for the Supplier organization.
2. Supplier shall ensure that security management is embedded in project management.
3. Supplier shall effectively segregate duties, roles and responsibilities, to prevent misuse or unauthorized/unintentional changes of Customer's Information and Personal Data.

3. HUMAN RESOURCES SECURITY

1. Supplier shall assure all employees and sub-contractors undergo background screening.
2. Supplier shall maintain policies and procedures that ensure the suitability of Supplier personnel and sub-contractors in relation to their roles and responsibilities.
3. Supplier shall provide appropriate information security aware-ness and training program, so that Supplier employees and sub-contractors understand their security responsibilities, in relation to Customer Information and Personal Data.
4. Supplier shall develop and communicate disciplinary actions aiming at employees who have violated security policies and standards.
5. Supplier shall ensure that all necessary procedures are defined and performed for Supplier's employees upon change of role, end of engagement, termination of employment, contract or agreement. In particular, all privileges shall be revoked in a timely manner.

4. ASSET MANAGEMENT

1. Supplier shall develop and implement information classification, labelling, and handling rules.
2. Supplier shall maintain procedures to identify, control and maintain the ownership and security classification of key Supplier assets and Customer Information and Personal Data processed by Supplier.
3. Supplier shall maintain policies defining the acceptable useof information and assets, and communicate these to all appropriate users of Supplier assets and information.

5. ACCESS CONTROL

1. Supplier shall implement procedures designed to control access to information systems processing Customer Information and Personal Data, including providing unique user identification and access controls.
2. Supplier shall limit access to Customer's Information and Personal Data to authorized users with business justification and following least privileges rule.
3. Supplier shall implement multifactor authentication to control remote access to information systems processing Customer Information and Personal Data.
4. Supplier shall review the list of privileges in their systems (used to provide services) against the list of entitlements on a periodic basis.
5. Supplier shall ensure no standing access to production environment for employees, who processes the data in case of trouble shooting. Access should be allowed only in case of trouble shooting after management approval and authentication.

6. CRYPTOGRAPHIC CONTROLS

1. Supplier shall develop and implement a policy on the use of cryptographic controls for the enduring protection, confidentiality and preservation of integrity of sensitive information and assets. As minimum, Supplier shall ensure that Customer's Information and Personal Data is protected by encryption at transfer, digital signing and encryption at rest.
2. Supplier shall develop and implement a policy on the use, protection and lifetime of cryptographic keys to ensure their protection against unauthorized access or modification, and loss.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

1. Physical security perimeters shall be defined to ensure only authorized access to organization's information facilities and effective physical and environmental controls and safeguards shall be implemented to protect areas where information is stored or processed.
2. Supplier shall provide the physical protection of any equipment used for processing Customer Information and Personal Data as well as all infrastructure supporting information systems.
3. Supplier shall develop, communicate, and enforce the procedures for working in areas where Customer Information and Personal Data are processed.
4. Supplier shall implement clear desk policy for storage media and clear screen policy for areas where Customer Information and Personal Data are processed.

8. OPERATIONS SECURITY

1. Supplier shall maintain a suitable set of processes and procedures for the effective management of information systems processing Customer Information and Personal Data, including:

- Change management
- Capacity management of business-critical systems and components
- System planning and acceptance
- Protection against malware
- Regular backup of information and software, as well as testing recovery capabilities against recovery time objectives and recovery point objectives

- Logging and reviewing of events, which could potentially have impact on the security of information systems
- Decommissioning of information systems
- Secure Development and protection of pre-production environments
- Procedures for management, handling, disposal and storage of media

2. Supplier shall provide and use separate environments for development, testing and operational purposes.
3. Supplier shall ensure the production data (real data) shall not be used outside production environment. If production data needs to be copied to test environments secure data anonymization/ pseudonymization techniques shall be applied, to ensure potential leakage of such data will not pose any risk for PG and its contractual and regulatory obligations.
4. Supplier shall define and implement rules on the installation of software by employees and contractors on End User devices owned by the organization (workstations, mobiles etc.).
5. Supplier shall follow the principle of data minimalization, in particular pseudonymization /anonymization should be applied when gathering data for statistical purposes.

9. COMMUNICATIONS SECURITY

1. Supplier shall manage network security to protect information systems.
2. Supplier shall apply security safeguard protecting used networks and the borders with other networks, with means including network segregation, secure remote access, intrusion detection and perimeter protection.
3. Supplier shall define requirements and implement policy for signing non-disclosure agreement with external parties, where non-public information is exchanged.
4. Supplier shall enforce exchange of information with external parties only via mutually agreed methods. For electronic exchange, the best practices in terms of selection of cryptographic protocols and algorithms shall be applied.

10. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

1. Specification, acquisition, development and maintenance of Information Systems, including both those procured from external vendors and those internally produced, Supplier shall determine the necessary confidentiality, integrity and availability requirements, and continue to review these against an enduring risk profile through the usage lifecycle.
2. Supplier shall define and maintain principles for the appropriate security aspects of any software development lifecycle.
3. Supplier shall identify and evaluate technical vulnerabilities and threats, and shall deploy an effective patch and vulnerability management policy designed to remediate Supplier's Information Systems.
4. Supplier shall assure that Systems processing Customer Information and Personal Data are logically or physically separated on from other customers data.

11. SUPPLIER RELATIONSHIPS

1. Supplier shall establish and maintain formal agreements with third parties involved in the service delivery management of Sup-plier's information systems processing Customer Information and Personal Data, incorporating where appropriate the necessary security controls, policies and service level agreements.
2. No Customer Information and Personal Data can be shared with third party (including sub-contractors) without clear and unambiguous consent of Customer.

12. INFORMATION SECURITY INCIDENT MANAGEMENT

1. Supplier shall prepare and maintain an incident response plan and program containing procedures and directions to follow in the event of an incident related to the security of Supplier's computer infrastructure, documenting the necessary steps and channels of communication to be followed.
2. Supplier shall ensure that the directions incorporate appropriate procedures for notifying PG, and other necessary stakeholders, promptly if any security Incident is determined to have caused a security breach involving Customer's Information or Personal Data.
3. Supplier shall notify Customer about identified weakness in system and services having influence on the security of Customer's Information and Personal Data.

13. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

1. Supplier shall develop and maintain Business Continuity impact analyses and Disaster Recovery plans, designed to prevent Customer Information and Personal Data loss as well as maintain Supplier's delivery of the Services with minimal interruption. Each plan shall detail measures to support the effective restoration of services, to resume operations as soon as possible after an emergency.
2. Supplier shall conduct periodic testing of most critical business functions, to provide assurance that these are readily available in the event of a declared disaster.
3. Supplier shall implement redundant logical and physical assets where needed to meet availability requirements. Periodical tests shall ensure smooth failover.
4. Supplier shall ensure that backups are taken offsite, to support the recoverability of Supplier systems in the event of a disaster.

14. COMPLIANCE

1. Supplier shall provide assurance that Supplier information systems comply with security requirements and policies, applicable laws and regulatory requirements.
2. Supplier shall implement appropriate audit controls, limiting access to tools and systems thus preventing misuse or compromise, and ensuring that audits comply with the Supplier Security Policy.

ATTACHMENT 3

LIST OF SUBPROCESSORS

(Internal Note: In the event that Supplier has already engaged subcontractors at the time the contract is signed this attachment should be filled in:
providing the name of the subcontractor, their address and a description of the services subcontractor provides with regard to the processing of Personal Data)
Customer consents to Supplier engaging the following sub-processors:

Sub-processor (full legal name)	Address/country	Description of services provided by the sub-processors

ATTACHMENT 4

STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA FROM THE EU TO THIRD COUNTRIES (CONTROLLER TO PROCESSOR TRANSFERS)

Data Transfer Agreement with GDPR provisions

For the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

[LEGAL ENTITY NAME OF PG ENTITY EXPORTING PERSONAL DATA]
[ADDRESS] [TELEPHONE][FAX]
[E-MAIL]
(the data **exporter**)
and
[LEGAL ENTITY NAME OF PROCESSOR THE PERSONAL DATA IS TRANSFERRED TO]
[ADDRESS] [TELEPHONE][FAX]
[E-MAIL]
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedomsof individuals for the transfer by the data exporter to the data importer of the personal data specified in Attachment 1.

CLAUSE 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and'supervisory authority' shall have the same meaning as in the applicable data protection law;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protectionwithin the meaning of the applicable data protection law;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importerwho agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the Directive 95/46/EC and any legislation and/or regulation implementing ormade pursuant to it, or which amends, replaces, re-enacts or consolidates any of it (including the Regulation (EU) 2016/679

(f) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)), and all other applicable laws relating toprocessing of personal data that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by the supervisory authorities, the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(g) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration,unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

CLAUSE 2

Details of the transfer

The details of the transfer and in particular the special categoriesof personal data where applicable are specified in Attachment 1which forms an integral part of the Clauses.

CLAUSE 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 15 in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 15 in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which ittakes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Suchthird-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

CLAUSE 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporteris established) and does not violate the relevant provisions of thatState;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importerto process the personal data transferred only on

the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Attachment 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access,in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or assoon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of the applicable data protection law;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to thedata protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Attachment 2, and a summary description of the security measures, as well as a copyof any contract for subprocessing services which has to be madein accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under theClauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

CLAUSE 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses;if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend thetransfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicableto it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) `that it has implemented the technical and organisational security measures specified in Attachment 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentialityof a law enforcement investigation,

ii. any accidental or unauthorised access, and

iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject tothe transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities coveredby the Clauses which shall be carried out by the data exporter oran inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy ofthe Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in whichcase it may remove such commercial information, with the exception of Attachment 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

CLAUSE 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to inClause 3 or in Clause 11 by any party or subprocessor is entitledto receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agreesthat the data subject may issue a claim against the data importeras if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because boththe data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent,the subprocessor agrees that the data subject may issue a claimagainst the data subprocessor with regard to its own processingoperations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed theentire legal obligations of the data

exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties agree that if one party is held liable for a violationof the Clauses committed by the other party, the latter will, to theextent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate withthe data exporter in the defence and settlement of the claim.

CLAUSE 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importerwill accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in whichthe data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

CLAUSE 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the rightto conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

CLAUSE 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

CLAUSE 10

Variation of the contract

1. The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.
2. The following commercial clauses have been added as new provisions/clauses:

(a) Clause 13 (Additional obligations of the data importer);

(b) Clause 14 (Correction, deletion and blocking of data); and

(c) Clause 15 (Data subjects' rights).

CLAUSE 11

Subprocessing

1. The data importer shall not subcontract any of its processingoperations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so onlyby way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liableto the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and thesubprocessor shall also provide for a third-party beneficiaryclause as laid down in Clause 3 for cases where the data subjectis not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law.Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated atleast once a year. The list shall be available to the data exporter'sdata protection supervisory authority.

CLAUSE 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless European or Member State legislation imposed upon the data importer prevents it fromreturning or destroying all or part of the personal data transferred.In that case, the data importer warrants that it will guarantee theconfidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

ATTACHMENT 4.A

STANDARD CONTRACTUAL CLAUSES "SUPPLEMENTARY MEASURES APPENDIX"

BACKGROUND

1. In judgment C-311/18 (Schrems II) the Court of Justice of the European Union (CJEU) has indicated that controllers or processors, acting as data exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the data importer in the third country, if the lawor practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Standard Contractual Clauses (SCCs). In those cases, the CJEU still leaves open the possibility for data exporters and importers to implement supplementary measures that fill any (possible) gapsin the protection and bring it up to the level required by EU law.
2. This Appendix provides additional supplementary measures,drawing on the recommendations contained in the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted by the European Data Protection Board on 10 November 2020.

AGREED TERMS

1. This Appendix forms part of the Controller-to-Processor Standard Contractual Clauses under EU Commission Decision 2010/87/EU in Attachment 4.
2. In the event of a conflict between:
   (a) The Clauses in this Appendix 4.A; and
   (b) The Clauses adopted by the European Commission under Commission Decision 2010/87/EU,

the Clauses described under Clause 2(b) of this Appendix shall take precedence.

3. As regards possible access to the transferred personal data by public authorities, the data importer warrants and undertakesthat:
   (a) it shall review, under the laws of the country of destination, the legality of any request for disclosure of the transferred personal data to a public authority, notably whether it remains within the powers granted to the requesting public authority, andto exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds underthe laws of the country of destination to do so. When challenging a request, the data importer shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. It shall not disclose the transferred personal data requested unless and until required to do so underthe applicable law or procedural rules;
   (b) it shall document the legal assessment carried out under a), as well as any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make it available to the data exporter. It shall also make it available to the competent supervisory authority upon request;
   (c) it shall provide the minimum amount of information permissible when responding to a request for disclosure of the transferred personal data, based on a reasonable interpretation of the request;
   (d) it shall inform the requesting public authority of any incompatibility of the request with the safeguards contained in the Clauses and the resulting conflict of obligations for the data importer. The data importer shall also immediately notify the dataexporter, insofar as possible under the laws of the country of destination;
   (e) it shall document and record the requests for access to the transferred data received from public authorities and the response provided as well as the actors involved. These records should be made available to the data exporter, insofar as possible under the laws of the country of destination;
   (f) the data exporter may exercise its power to require that the data importer submit its processing facilities and other documentation and files to audit or inspection pursuant to Clause5(f) of the Clauses by giving 12 hours' notice to the data importer. The data importer shall ensure that data exporter is in a positionto verify whether the transferred personal data was disclosed to public authorities and under which conditions they were disclosed. In particular, access logs and other similar trails mustbe tamper-proof so that auditors are in a position to find evidence of disclosure. Access logs and other similar trails must also distinguish between accesses due to regular business operations and accesses due to orders or requests for access. When carrying out its obligations under this Clause, the data importer will in all circumstances cooperate with the data exporter and the competent supervisory authority in a timely fashion;
   (g) it shall make reasonable efforts to monitor any legal or policy developments which might lead to its inability to comply with its obligations under the Clauses. In particular, the data importer shall make reasonable efforts to inform the data exporter of legal or policy developments ahead of their implementation and, where possible, before access is granted to the transferred personal data;
   (h) it has not purposefully created back doors or similar programming that could be used by public authorities to access either or both of the following:
   (i) the system(s) that the data importer uses for processing of the transferred personal data;
   (ii) the transferred personal data themselves;
   (i) it has not purposefully created or changed its business processes in a manner that facilitates access to such personal data or systems by public authorities; and
   (j) to the best of its knowledge, national law or government policy applicable to the data importer does not require the data importer to do either or both of the following:
   (i) create or maintain back doors or to facilitate access to the transferred personal data or systems by public authorities;
   (ii) be in possession or to hand over the encryption key.

On behalf of the data exporter: **On behalf of the data importer:**

Name (written out in full):	Name (written out in full):
Position:	Position:
Date:	Date:
Signature:	Signature:

Name (written out in full):	Name (written out in full):
Position:	Position:
Date:	Date:
Signature:	Signature: