GENERAL TERMS AND CONDITIONS OF PURCHASE

SOCIETE GENERALE

WHEREAS

This document (the **"General Terms and Conditions of Purchase" or the "General Terms and Conditions**") governs the transactions between your company (hereinafter the "**Service Provider**") and an entity of the Societe Generale Group (hereinafter the "**Beneficiary**") within an Application Contract explicitly referencing the present General Terms and Conditions and signed between your company and the Beneficiary.

The purpose of the General Terms and Conditions of Purchase is to cover the purchase by the Beneficiary from the Service Provider of Products, Software Licenses ("Product Software" or "SaaS") and/or Services as described in the Application Contract.

The signing of an Application Contract referencing the present General Terms and Conditions implies full acceptance by the Service Provider of the stipulations of the present General Terms and Conditions of Purchase.

The Beneficiary reserves the right to modify the General Terms and Conditions of Purchase. However, it is understood that the General Terms and Conditions applicable between the Parties are those in force on the date of signature of the Application Contract or those in force, as the case may be, on the date of renewal of the Application Contract.

IT IS HEREBY AGREED AS FOLLOWS:

1. DEFINITIONS

Act of Corruption: refers to the deliberate act of (a) giving, offering or promising, directly or indirectly through others such as third party intermediaries, or (b) soliciting or accepting, directly or indirectly through others such as third party intermediaries, any donation, gift, invitation, reward, or anything of value to any person (including any public official), for themselves or for a third party, that would or could be perceived either as an inducement to commit an act of corruption or as a deliberate act of corruption in each case with a view to inducing any person (including a public official) to perform their functions improperly or dishonestly and/or getting any undue benefit.

Act of Influence Peddling: refers to the deliberate act of (i) giving, offering or promising to any person (including any public official), or (ii) yielding to any person (including any public official) who solicits, at any time, directly or indirectly, any donation, gift, invitation, reward, or anything of value, for themselves or for others, in each case to abuse or for having abused their real or supposed influence with a view to obtaining from a public official any favourable decision or undue benefit.

Acceptance: refers to the acceptance procedure implemented in order to verify that the Deliverables and Generic Developments comply with the contractual conditions. The acceptance procedure is described in Article "Delivery and Acceptance" of the General Terms and Conditions.

Application Contract: refers to the document signed between the Service Provider and a Beneficiary, defining the specific conditions of performance of the Products and Services and explicitly referencing the present General Terms and Conditions.

Associated Services: refers to additional services purchased by the Beneficiary. Associated Services are described in an appendix to the Application Contract, where applicable, or may give rise to the signature of an amendment between the Parties.

Beneficiary data : refers to (i) all data forwarded by Users and/or a Beneficiary to the Service Provider within the execution of the Products and Services and/or (ii) all data kept by the Service Provider for a Beneficiary, within the framework of the Contract, including data of a personal or non-personal nature, as well as any data of a sensitive nature. This data is confidential.

Business Hours : refers, unless otherwise stipulated in the Application Contract, the hours from 9.00 a.m to 6.00 p.m on Working Days, in the Beneficiary's time zone.

Calendar: refers to the schedule to supply the Products and Services as specified in the Application Contract.

Conflict of Interest Situation : refers to any situation where the Service Provider, its employees, officers, agents or any other person it controls or whom is linked directly or indirectly to the Service Provider, are subject, as part of their activities, to multiple interests, opposite or different (such as personal interest, employer's interest, interests of one or more clients) from the Beneficiary's interests and whose pursuit may harm the Beneficiary's interests.

Contract: means the combination of the General Terms and Conditions and an Application Contract.

Critical vulnerability: means a Vulnerability which level will be measured using proven calculation methods such as the CVSS standard (version 4.0) that is recommended by the Beneficiary. Any Vulnerability detected by the Service Provider with a CVSS score above 9 will be considered as critical.

Data Subject : refers to any natural person to whom the data directly or indirectly relate.

Deliverables: means the results of all types, supplied, developed or created by the Service Provider while performing the Contract and delivered to the Beneficiary. The Deliverables are defined in the Application Contract.

Documentation : refers to any technical documentation or any instructions, for administration or use, including any updates, improvements, or other changes that may be made and any other element that may be attached to it, supplied by the Service Provider and relating to the Products and Services. .This Documentation must be clear, complete, include a version number, and must be reproducible according to the Beneficiary's requirements.

Element : refers to all patches, updates, new versions, etc. of the Product Software, supplied by the Service Provider within the scope of maintenance services.

Event of Force Majeure: means an event that prevents a Party from fulfilling its contractual obligations provided that such event is beyond its control, could not be reasonably foreseen from the day of conclusion of the Contract and which effects cannot be avoided by appropriate measures.

General Terms and Conditions or General Terms and Conditions of Purchase: refers to this agreement and its appendices, which form an integral part hereof.

Generic Developments: means the IT developments to be integrated into the standard Product Software (version delivered to all the Service Provider's customers).

Good Industry Practices: refers to the information currently gained from the knowledge available to a professional depending on the time, place, and economic environment in which the Contract is implemented.

Group: means the unit formed by a parent company and companies meeting one of the following criteria:

(i) companies complying with the provisions of article L 233-16 of French Commercial Code relating to the criteria governing the scope for consolidating accounts (including sub-consolidated companies),

(ii) companies controlled directly or indirectly pursuant to article L 233-3 of French Commercial Code,

(iii) companies in which the Beneficiary holds a share pursuant to article L. 233-2 of French Commercial Code.

Hosted Services or SaaS: refers to the provision of one or more software applications as a remote service, supplied by the Service Provider, including in particular hosting and maintenance services. The Hosted Service is described in the Application Contract.

ICT service(s): refers to a service related to information and communication technologies within the meaning of Regulation 2022/2554 of the European Parliament and of the Council on digital operational resilience of the financial sector of 14 December 2022 (the "**DORA Regulation**").

License : means the license(s) to use the product granted by the Service Provider to the Beneficiary under the terms of the Contract.

Malware: refers to a harmful computer code, such as a virus, logic bomb, worm, Trojan horse, or any other code or instruction, which infects or affects any program, software, data, file, database, computer, or other equipment or element that damages, impairs, compromises, diverts, permits the diversion or incapacitates the integrity or confidentiality, in whole or in part, of an information system from the use for which it is intended.

Parties: refers collectively to the Service Provider and the Beneficiary.

Processing of Personal Data or Processing: refers to any operation or set of operations applied to Personal Data, carried out using automated processes or not, such as collection, recording, organization, retention, adaptation or modification, extraction, consultation, use, disclosure by transmission, dissemination, or any other form of provision, reconciliation, or interconnection, as well as locking, erasure, or destruction.

Products : refers to the products, materials or equipment covered by the Contract purchased by the Beneficiary from the Service Provider and described in the Appendix to the Application Contract.

Products and Services : refers collectively to the Products, Services, Product Software and/or the Hosted Service acquired by the Beneficiary from the Service Provider as part of an Application Contract. These Products and Services are described in the Application Contract.

Product Software : refers to the software package defined in the Application Contract, the Generic Developments, the Elements and related Documentation.

Personal Data: any information relating to an identified individual or who may be identified, directly or indirectly, by referring to an identification number or to one or more items relating to him/her.

Public Officials refers to all elected officials, dignitaries, candidates for public office, members of royal families, magistrates, officials or employees, regardless of their grade, or any person belonging to or acting on behalf of:

- A government (foreign, national or local) including any department, agency, regulator or one if their bodies or instrumentalities;

- A government department or public authority (including but not limited to customs or tax authorities, embassies and all bodies issuing permits);
- A local or regional public service;
- A State-owned or controlled enterprise (including but not limited to public hospitals, universities, sovereign investment funds or any other state-sponsored entity);
- A political party, or
- An international court or public organisation (e.g. the UN).

Sanctions : means any economic or financial sanctions, trade embargoes or similar measures enacted, administered or enforced by any of the following (or by any agency of any of the following):

a) the United Nations;

b) the United States of America;

c) the United Kingdom;

d) the European Union or any present or future member state thereof or;

e) any other country concerned, subject to the laws and regulations applicable for the purposes of performing the Contract.

Sanctioned Person : means any person, whether or not having legal personality:

a) listed on any list of designated persons in application of Sanctions;

b) located in, or organised under the laws of any country or territory that is subject to comprehensive Sanctions;

c) directly or indirectly owned or controlled, as defined by the relevant Sanction, by a person referred to in (a) or (b) above; or

d) which otherwise is, or will become during the execution of the Contract, subject to Sanctions.

Services: refers to services of any kind performed by the Service Provider on behalf of the Beneficiary, such as consulting, training, support, IT development, maintenance, installation and integration.

Service Levels: refers to the level of quality and operating conditions of the product(s) or service(s) covered by the Contract, as described, where applicable, in the appendix to the Application Contract, and which the Service Provider guarantees to the Beneficiary for the entire duration of the Contract.

Vulnerability: means any weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Working Days: Monday to Friday, excluding public holidays in France or, where applicable, in the country(ies) specified in the Application Contract.

2. PURPOSE

The purpose of these General Terms and Conditions is to define the general conditions under which the Service Provider undertakes to provide the Products and Services described in the Application Contracts.

3. CONTRACTUAL DOCUMENTS

The General Terms and Conditions, which constitute the agreement between the Parties, is composed entirely and exclusively of :

1.The present document, which contains the general stipulations applicable to the Products and Services ;

2. Appendices A “Generic” applicable to all types of Products and Services:

- Appendix A.1: Obligations relating to the fight against unreported employment and fraudulent transnational secondment
- Appendix A.2: Data Destruction Report
- Appendix A.3: User charter for information protection and use of IT resources
- Appendix A.4: Template of work accident notification
- Appendix A.5: Business rules for receiving invoices
- Appendix A6 : Good practices related to the usage of privileged accounts
-

3. Appendix B “Software ”, applicable exclusively to the acquisition of Product Software;

4. Appendix C “SaaS” applicable exclusively to the acquisition of Hosted Service;

5. Appendix D “Products” applicable exclusively to the acquisition of Products.

The agreement between the Service Provider and the Beneficiary consists entirely and exclusively of :

- The present General Terms and Conditions and its appendices online on the day of signature of the Application Contract or on the day of its renewal, as the case may be;
- The Application Contract and its appendices.

In this respect, it is reminded that the signing of the Application Contract by the Parties implies their full and entire acceptance of the conditions stipulated in the General Terms and Conditions.

The General Terms and Conditions supersede all oral or written agreements that may have previously been concluded between the Parties relating to the Products and Services acquired under the Application Contract. It is expressly stipulated that the Service Provider's general terms and conditions of sale/service (or any other similar document published or usually used by the Service Provider) are not applicable to all or part of the Contract.

It is understood that the contractual documents are self-explanatory. However, in the event of any contradiction or discrepancy between the terms of the contractual documents, the documents shall take precedence over each other in the order in which they are listed. It is understood that the General Terms and Conditions shall prevail over any Application Contract in the event of contradiction or discrepancy between the terms of these contractual documents, unless expressly stipulated otherwise in the Application Contract, which explicitly derogate from the stipulations of the General Terms and Conditions.

4. CONTRACT TERM

4.1 Term of the General Terms and Conditions

The General Terms and Conditions apply to Products and Services from the date of entry into force of the Application Contract and for the entire duration of the Application Contract.

4.2 Term of the Application Contracts

The effective date and duration of each Application Contract will be indicated in each Application Contract. Application Contract may only be renewed by amendment. Any tacit renewal is excluded.

5. COORDINATION OF THE CONTRACT AND MONITORING OF THE SERVICES

The Service Provider and the Beneficiary shall each appoint a correspondent to represent them and take all decisions necessary for the proper execution of the Application Contract.

The identity and contact details of the correspondents appointed on signature of the Application Contract are specified in the Application Contract.

In particular, the Beneficiary's correspondent will:

- Check the progress of the Products and Services
- Check that the Products and Services performed comply with the contractual provisions.

The Service Provider's correspondent shall in particular

- Report to the Beneficiary on the progress of the Products and Services.
- Supervise and manage the Service Provider's personnel.

6. SERVICE PROVIDER'S PERSONNEL

6.1 Supervision

The Service Provider's personnel assigned to implementing the Contract remain under the administrative control and the sole managerial and disciplinary authority of the Service Provider for the entire term of the Contract. The Service Provider supervises and monitors its employees, including when the Services are performed on the Beneficiary's premises.

6.2 Skills

The Service Provider undertakes to anticipate a sufficient number of staff with the necessary skills to implement the Contract.

6.3 Health and safety

The Service Provider undertakes to do everything necessary to ensure that when its personnel are working on the Beneficiary's premises they comply with the provisions applicable to external companies working on the aforementioned premises and specifically those governing health and safety.

For its part, the Beneficiary undertakes to inform the Service Provider of these provisions.

The Beneficiary and the Service Provider will comply with the provisions of Law N° 92158 dated 20.02.1992 establishing the specific regulations for health and safety applicable to work carried out by an external company on the Beneficiary's premises.

In the event that, within the scope of the Contract, the Service Provider's personnel should use the Beneficiary's IT system, the Service Provider shall ensure that, at such time, its staff specifically complies with the stipulations contained in the document called "Charte d'utilisation des moyens de

communication électronique" (Charter for use of electronic communication equipment) of the Societe Generale group.

6.4 Unreported employment and obligations relating to transnational secondment

The Service Provider hereby undertakes to comply with the French regulations against unreported employment and any other similar regulation applicable when the contracted services are provided on another territory.

If the Service Provider is sited in a foreign country and that it seconds its employees in France for the purpose of providing the services, it also undertakes to comply with all the legal obligations in the matter (secondment declaration and appointment of a representative in France). The Service Provider undertakes to supply the Beneficiary with all the documents listed in appendix "Obligations relating to the fight against unreported employment and fraudulent transnational secondment".

6.5 Access to premises

For security reasons inherent to the Beneficiary, should an intervention on the Beneficiary's premises be necessary, the Service Provider's personnel will be issued an ID badge showing the name of the Service Provider, the name of the staff member and their photo. This badge must be worn in a visible manner within the Beneficiary's premises, for as long as the member of staff is on these premises.

For the same reasons, the Service Provider will draw up a list of the names of people likely to work on the same site.

The Beneficiary must be able to verify the Service Provider's personnel's authorizations at any time. The Beneficiary must be advised in advance of any new members of staff. In this context, any person arriving at a site without having been previously announced will be refused access to the site. The badges and other access cards supplied by the Beneficiary to the Service Provider must be returned to the Beneficiary at the end of the Contract.

The Service Provider undertakes to report to the Beneficiary any work accident of its employees into the Beneficiary's premises. This report, established according to the template attached in appendix “Workplace accident declaration” shall be sent to the Beneficiary or the third-party it designates, by the 15ft of February, May, August and November of each Year from the effective date of the Agreement. The report shall include all items related to work accidents that happened during the three (3) month preceding the report. If no work accident happened during the relevant period, the report shall indicate "void".

The Service Provider undertakes to comply with the provisions relating to the display of working hours (articles L.3171-1 and D.3171-1 and subsequent of the French Labour Code) for its employees working on the Beneficiary's site who do not have an executive status subject to a working time agreement based on a fixed number of days/hours per year pursuant to article L.3121-38 of the French Labour Code. This display shall take the form of a document with the letterhead of the Service Provider company to be posted in the office where the Service Provider performs its tasks, starting from the first day of work.

7 SERVICE PROVIDER'S OBLIGATIONS

7.1 Obligation of giving advice

Within the scope of its general obligation to advise, the Service Provider shall, in particular:

- Inform, advise and warn the Beneficiary with respect to the Products and Services, as well as in relation to any decisions regarding the performance of the Products and Services which the Beneficiary may make and the Service Provider has been made aware of, provided that the responsibility for the final decision shall rest solely with the Beneficiary;
- Inform, advise and notify the Beneficiary in relation to the coherence of any objectives and choices that the Beneficiary may set or make during the term of the Contract;

- Inform the Beneficiary of technological advances and changes in Good Industry Practice in relation to the Products and Services which may have occurred during the term of the Contract;
- Advise the Beneficiary when the Beneficiary issues additional or new requests.

7.2 General obligations

The Service Provider undertakes to provide the Products and Services in accordance with the provisions of the Contract. The Service Provider will be under an obligation of performance regarding:

- Compliance with Service Levels as defined, if any, in the Application Contract;
- Compliance with the Calendar;
- Compliance of Generic Developments, Deliverables and, more generally, Products and Services with the provisions of the Contract .

The Service Provider undertakes to provide the Products and Services in accordance with Good Industry Practice for its profession and, without limitation to the foregoing, shall discharge its obligations under the Contract with the required knowledge, experience and skill and to furnish all equipment and/or software required.

The Service Provider is solely responsible for the resources and methods which it applies for purposes of performing the Contract.

The Service Provider shall comply with all laws and regulations (including any changes thereto or any new laws or regulations made after the date of the Contract) applicable to the provision of the Products and Services. In addition, if the performance of the Products and Services requires the Service Provider's personnel to use the Beneficiary's IS, the Service Provider's personnel must follow any awareness program made available by the Beneficiary for the purpose of preventing operational or regulatory risks related to the performance of the services.

The Service Provider shall notify the Beneficiary of any problems that may arise in the provision of the Products and Services on the day on which they occur.

The Service Provider is responsible for ensuring that its staff and subcontractors (if any) comply with these provisions.

Upon request by Beneficiary or otherwise upon expiry or termination (for whatever reason) of the Contract, the Service Provider shall return to the Beneficiary any Beneficiary data as well as all equipment, tools or other elements that the Beneficiary may have supplied to the Service Provider in connection with the provision of the Products and Services.

7.3 Loyalty obligation

The Parties agree, throughout the term of the Contract, to loyally fulfil their respective obligations and to seek, in good faith, all possible solutions enabling a rapid and balanced resolution of potential problems or difficulties that may arise during the performance of the Contract.

8 SERVICE LEVELS

The Parties define the Service Levels, which constitute the list of key performance indicators to be monitored, as well as the performance objectives for the Products and Services. Service Levels are defined if applicable, in the “Service Levels” appendix to the Application Contract.

The Service Provider undertakes to meet or exceed the defined Service Levels.

If the Service Provider fails to provide the Products and Services in accordance with the Service Levels, without prejudice to any other rights and remedies of the Beneficiary, and at no additional cost to the Beneficiary, the Service Provider undertakes to:

- Restore the target Service Levels;
- Pay any associated penalties as defined in the Application Contract, if applicable.

When the Products and Services are classified as “ICT Services” within the Application Contract, the Parties examine, at least once a year as part of the governance of the Contract, the Services Levels to ensure that they comply with market practices, regulatory requirements and the Beneficiary's commercial developments. They decide on any updates, revisions and adaptations to be made to the Service Levels as a result of these developments.

9 FINANCIAL REGULATION

Beneficiary may immediately terminate the Contract without indemnity if the Service Provider or, where appropriate, any of its agent, is in breach of any obligation provided in the present section.

9.1 Fight against corruption and influence peddling

The Service Provider represents and undertakes to the Beneficiary at any time during the term of the Contract, that:

(i) It has knowledge of, and is committed to complying with, the laws and regulations relating to anti-bribery, corruption and influence peddling applicable to the execution of this Contract;

(ii) Neither the Service Provider, nor, to the best of its knowledge, any of the persons whom it controls, including its directors, officers, employees (hereafter the "**Controlled Persons**"), nor any agent or intermediary it has mandated for the purpose of executing the Contract:

(a) has committed any Act of Corruption or Act of Influence Peddling;
(b) is prohibited (or is treated as such), by a governmental or international agency, from responding to requests for proposals or to contract or work with this agency because of any proven or alleged Act of Corruption or of Influence Peddling;

(iii) It has put in place appropriate rules and procedures, in a form and manner mandated by law and/or appropriate for a business of its size and resources, aiming at:

(a) preventing any Act of Corruption and Act of Influence Peddling from being committed by itself, Controlled Persons, and – if any - the agents or other intermediaries it has mandated for the purpose of executing the Contract, and
(b) ensuring that any evidence or suspicion of an Act of Corruption or an Act of Influence Peddling is investigated and handled with the appropriate diligence.

Any Act of Corruption or of Influence Peddling related to this Contract shall be promptly disclosed to the Beneficiary, to the extent permitted by applicable law;

(iv) It maintains reasonably detailed books, records, and accounts, in respect of the execution of the Contract, in a form and manner appropriate for a business of its size and resources.

The Service Provider represents and warrants that it has knowledge of the Beneficiary’s code of conduct governing the fight against corruption and influence peddling.

The Beneficiary may immediately suspend without notice or indemnity any payment, promise to pay, or authorization of any payment (or giving anything of value) to the Service Provider, if the Beneficiary has reasonable grounds to suspect that the Service Provider or any of its agents, intermediaries or Controlled Persons has committed any Act of Corruption or of Influence Peddling in relation to the Contract. Reasonable grounds shall include, but not be limited to, publicly available reports of Act of Corruption or of Influence Peddling. Such suspension shall be maintained only for the time necessary to investigate those grounds in order either to confirm or dispel the suspicions.

The Service Provider and its agents and intermediaries it has mandated for the purpose of executing this Contract, are not linked to, or expected to interact with, Public Official(s), government, or government entities as part of the Services provided to the Beneficiary.

9.2 Fight against conflicts of interests

At any time during the term of the Contract, the Service Provider shall declare and warrant to the Beneficiary that it will not maintain personal or professional relationships which could compromise its professional duties or put itself in a Conflicts of interest Situation vis-a-vis the Beneficiary.

The Service Provider shall report without delay to the Beneficiary any Conflict of Interest Situation in relation with their commercial relationship and to which it might be subject. If the Beneficiary considers that the Conflict of Interest Situation declared by the Service Provider is incompatible with the continuation of the Contract, the Beneficiary may terminate, as of right, without any notice nor compensation, the Contract.

9.3 Sanctions and embargos

(i) The Service Provider represents that neither it, nor any of its affiliate, subsidiary or holding nor, to the best of its knowledge, any of its directors, officers, and employees, or any of its agents and intermediaries, is a Sanctioned Person.

(ii) The Service Provider represents and warrants (which representation and warranty shall be deemed to be repeated at all times until the termination of the Contract) that it shall not provide any Service to, or enter into any arrangement with respect to the Services with, any Sanctioned Person or in violation of Sanctions.

(iii) The Service Provider shall, and shall procure that any agent or intermediaries it has mandated for the purpose of executing the Contract will, promptly upon becoming aware of the same, provide the Beneficiary with details of any claim, action, suit, proceedings or investigation against it with respect to Sanctions.

(iv) The Service Provider shall implement and maintain appropriate rules and procedures designed to comply with Sanctions, representations and undertakings in this Section.

(v) The Service Provider understands that Beneficiary should not process any payment or transaction to the benefit of a Sanctioned Person or in a way that would result in a violation of Sanctions. As such, and regardless whether the Services have already been performed, Beneficiary may immediately suspend any payment, promise to pay, or authorization of any payment (or giving anything of value) to the Service Provider, should the Service Provider be in breach of any Sanctions, representations or undertakings in this Section. Subject to applicable laws, regulations, and authorisations from competent authorities, Beneficiary may process such payment to the benefit of the Service Provider on a frozen account.

10 BENEFICIARY'S OBLIGATIONS

The Beneficiary undertakes to:

- make available to the Service Provider any information and documents in its possession necessary for the Service Provider to perform the Products and Services as specified in the Contract or otherwise agreed between the Parties,
- put the personnel of the Service Provider in contact with the personnel of the Beneficiary, who are concerned by the Products and Services,
- make available, when the Products and Services have to be performed in its premises, to the Service Provider the means held alone by the Beneficiary, and which means are essential for performance of the Products and Services.

11 CORPORATE SOCIAL RESPONSIBILITY

Societe Generale group has implemented measures to detect risks and prevent serious violations with respect to Human Rights and fundamental freedoms, and the health and safety of persons and the environment, which result from its own and its contractors' activities.

Within this context, the Service Provider undertakes to comply with the obligations herein.

The Beneficiary reserves the right to verify compliance with these obligations by the Service Provider, including on by conducting audits on premises, under the conditions of its audit rights, as the case may be, pursuant to the Contract.

11.1 Code of conduct

The Code of conduct of Societe Generale is available on its website https://www.societegenerale.com. As of the effective date of the Contract, the Service Provider represents and warrants that it has read the code and that it has implemented rules that are at least equivalent to those laid out in said code. The Beneficiary requires that individuals of the Service Provider assigned to perform the Products and Services do not contravene its rules, for the whole term of the Contract.

11.2 Sustainable Sourcing charter

To meet its legal and statutory obligations and, in line with the Code of conduct, Societe Generale group wants to associate its suppliers with implementation measures of vigilance. All the commitments made by the Beneficiary and the expectations of the Beneficiary from its suppliers relating to compliance with these rules as regards the Human Rights, working conditions, the environment and the fight against corruption are detailed in the Sustainable Sourcing charter ("The Charter") available on its website https://www.societegenerale.com.

The signing of the Application Contract by the Service Provider implies its compliance with terms at least equivalent to those of the Charter.

12 INTELLECTUAL PROPERTY

12.1 General Provisions linked with intellectual Property

Each of the Parties claims to hold all intellectual property rights necessary for the performance of the Contract or necessary to make available to the other Party the elements or tools necessary for the performance of the Contract.

12.2 Transferring copyright ownership of the Deliverables

The Service Provider automatically transfers on an exclusive basis to the Beneficiary, as and when the Products and Services are performed, all intellectual property rights (and in particular all rights of reproduction, representation, adaptation and more generally exploitation) relating to the Deliverables.

The assignment of intellectual property rights to the Deliverables is made for the entire world and for the duration of the protection currently granted or to be granted in the future to authors, by French laws and regulations and by international conventions.

The rights assigned to the Beneficiary include the rights of reproduction, representation and adaptation, and in particular the rights of dissemination, use, merchandising, translation, decompilation, manufacture, distribution, modification, exploitation free of charge or against payment, commercial, information, promotional and/or advertising rights, by assignment or rental, without limitation of scope or destination, both in France and abroad. All these rights may be exercised by any means, and in particular by any existing or future means of communication, on any existing or future medium and in any language.

The assigned rights may be exercised over all or part of the Deliverables, over any works derived from all or part of the Deliverables, and over any works incorporating them in whole or in part.

The Beneficiary may use and/or arrange for the use of the Deliverables , in whole or part, all works derived from them and all works into which they are incorporated, in part or in whole, as the owner, in the broadest possible manner and for the most diverse of purposes, in all formats, forms and presentations, by all methods, means and processes, and on all media and machines, whether present or future, hitherto known or unknown, hitherto foreseeable or unforeseeable.

The Service Provider also warrants that it has not granted and will not grant to any third party any rights in the Deliverables.

The Service Provider remains the owner of the resources, processes and know-how which were its property prior to the signing of the Application Contract, which it uses to perform the Products and Services and for which it grants a non-exclusive right of use to the Beneficiary.

13 WARRANTIES

13.1 Quality assurance

Unless otherwise stated in the Application Contract, the Products and/or Services provided by the Service Provider are guaranteed, with no additional cost, for one (1) months from the signing of the proper functioning and compliance verification report by the Service Provider and the Beneficiary in the conditions of the Contract.

In any case, the Service Provider shall grant the Beneficiary any applicable legal warranty.

13.2 Intellectual property indemnification

The Service Provider formally guarantees the Beneficiary full and complete enjoyment of the rights granted under the terms of the Contract against any difficulty, claim, indemnity, complaint or opposition whatsoever, related to the products and/or services (including but not limited to software, product software, solution, developments, hardware, service, deliverables) provided expressed by any third party alleging the violation of a right, and in particular against any breach of copyright and/or action of unfair competition and/or action of parasitism, and shall bear all expenses and damages resulting from this.

If, because of such an action, the Beneficiary is prevented from using the whole or any of the products and/or services provided, the Service Provider must, at its own expense:

- Obtain the right for the Beneficiary to use the products and/or services,
- Failing this, replace or modify the products and/or services provided in order to avoid this action and to preserve the same level of functionality, performance and relevance,
- Failing this, refund the Beneficiary any sums paid by the latter under the Contract.

This clause will remain in force after the expiry or termination of the Contract for whatever reason.

14 DELIVERY AND ACCEPTANCE

The Service Provider undertakes to deliver the Deliverables, products and services on the delivery dates defined in the Application Contract.

The Deliverables and Generic Developments will be subject to acceptance testing by the Beneficiary within the timeframe agreed between the Parties, or failing this, within sixty (60) days from the date of delivery to the Beneficiary.

At the end of the acceptance procedure, the Beneficiary may declare :

- a final acceptance of the Deliverables or Generic Developments, subject to their compliance with the stipulations of the Contract, or ;
- a provisional acceptance with reservations.

Any reservations expressed by the Beneficiary in the provisional acceptance report must be corrected by the Service Provider as soon as possible after notification by the Beneficiary, and in any event within a maximum period of fifteen (15) calendar days.

15 FINANCIAL CONDITIONS

15.1 Price

The Beneficiary will pay the Service Provider the fixed global amount appearing in the Application Contract.

The Service Provider undertakes to invoice the Products and Services only in the country where it has its head office or main place of business, or where the Products and Services are performed.

This amount is fixed and final for the entire term of the Application Contract.

This amount is expressed in euros and includes all the costs and expenditure required by the Service Provider to provide the Services, including travel and accommodation costs.

This amount covers if applicable the intellectual property rights acquired for the Beneficiary's Group on the Deliverables as they are defined at article "Intellectual Property".

All taxes incurred in connection with the Contract shall be borne by the Party legally liable for such taxes and no Party will at any time for any reason whatsoever be under any obligation to compensate the other Party for such taxes.

In particular, this amount under the terms of the Contract is exclusive of value-added tax or similar taxes; where applicable, VAT or similar taxes shall be added by the Service Provider, or computed and declared directly by the Beneficiary in accordance with the applicable legislation.

Moreover and also in particular, the Service Provider will bear the cost of any applicable withholding tax.

Therefore, in the event that any payment to be made in respect of any invoice is subject, by law, to any withholding tax, the Beneficiary will withhold taxes based on the rate as specified by law or treaty and subtract the withholding tax from the amount owed to the Service Provider.

If the Beneficiary’s State of residence provides for a specific exemption or reduced tax rate per a tax treaty, the Service Provider will provide, upon request, the Beneficiary with an exemption certificate or reduced rate certificate if required by any law or treaty.

Payment of such net sum to the Service Provider and the payment of the withholding tax to the relevant tax authority shall, for purposes of this Contract, constitute full settlement of the sums owing under the relevant invoice.

The Beneficiary hereby agrees that it will, upon request from the Service Provider, furnish any necessary evidence that may reasonably be required of the payment of the said withholding tax, allowing the Service Provider to pursue any appropriate claim before the tax authorities of is country of residence.

Both Parties will use reasonable efforts and shall co-operate in completing any procedural formalities necessary to minimize withholding taxes or similar, in accordance with the Law.

15.2 Payment of the price

The terms of payment as well as the payment schedule if any are detailed in the appendix “Financial Conditions” of the Application Contract.

Each payment obligation is subject to prior receipt by the Beneficiary of an invoice complying with applicable laws and regulations and meeting the Beneficiary's invoicing requirements set out in appendix "Business rules for receiving invoices". In particular, invoices must include a clearly legible mention of the order reference.

Payment by the Beneficiary will be made within thirty (30) days from the date of issue of the invoice, subject to the Beneficiary receiving said invoice, submitted in electronic format on the invoice-dedicated platform of the Beneficiary within a maximum of seven (7) days following the date of issue. The address

of the invoice dedicated platform are available on Societe Generale website: https://www.societegenerale.com/en

The invoices transmitted electronically by the Service Provider shall be created in a dematerialized manner and must meet the legal requirements so that they can be considered original invoices by the accounting and fiscal standards. Said invoices must be submitted on the invoice-dedicated platform of the Beneficiary. No paper invoice shall be issued and mailed at the same time by the Service Provider.

As an exception to the above, in the event a paper invoice is issued or if the invoice is not compliant with the expected format, payment by the Beneficiary may be made within sixty (60) days from the date of issue of the invoice, in accordance with the payment term authorized by the law.

If the Service Provider is not able to issue an invoice in electronic format, the Service Provider will ask the Beneficiary's correspondent for the exceptional conditions to be complied with for issuing an invoice in paper format.

In the case of a non-payment by its due date, any amount due to the Service Provider and not contested by the Beneficiary shall bear interest at a rate equal to three times the legal interest rate, starting from the first Working Day on which payment is late. These penalties shall be increased with a fixed compensation for recovery costs of forty (40) euros per unpaid credit.

In case of late payment, the Service Provider will immediately notify the Beneficiary in writing of the application of this clause.

15.3 Exclusion of "Hardship" provision

Both Parties agree to expressly exclude the provisions set forth in article 1195 of the French Civil Code.

15.4 Associated Services

Any request from the Beneficiary for Associated Services or modifications, of whatever kind, will form the subject, on the part of the Service Provider, of an additional or modifying proposal, which, if it is accepted by the Beneficiary, will result in the establishment of an amendment to the Application Contract signed by both Parties. The charges for Associated Services appear if applicable in appendix "Financial Conditions" of the Application Contract.

16 PENALTIES

16.1 Penalty application principles

It is expressly agreed between the Parties that the penalties do not constitute full discharge.

The penalties shall be subject to notification.

The Parties agree that penalties notified to the Service Provider that are not contested may be recovered by offsetting them against the amounts due by the Beneficiary under the terms of the Application Contract.

In the event that no payment is due by the Beneficiary, the penalties must be paid by the Service Provider within a maximum of thirty (30) calendar days following receipt of the Beneficiary's notification by the Service Provider.

Unless otherwise specified in the Application Contract, it is understood that the penalties may not exceed 15 % of the total value of the Application Contract.

If the upper limit of the penalties is reached, the Beneficiary may, without prior notice period, terminate the concerned Application Contract by registered letter with an acknowledgement of receipt without prejudice to damages which it may be awarded.

In addition, the Beneficiary may claim from the Service Provider the cost of any backup solution made necessary in order to meet at the objectives defined in the Application Contract.

16.2 Delay penalties

In the event of failure to meet the deadlines agreed between the Parties, the Beneficiary reserves the right to charge the Service Provider a penalty calculated in accordance with the formula defined when applicable in the Application Contract.

16.3 Penalties for non-respect of Service Levels

In the event of non-compliance with Service Levels, penalties may be applied under the conditions defined in the Application Contract.

17 CONFIDENTIALITY

17.1 Confidentiality obligation

Both Parties undertake, as regards the content of the provisions of the Contract, as well as information from the other Party which they may come to know within the framework of negotiating and implementing the Contract, where this information is of a sensitive nature, specifically on a financial, ethical, economic, technical or commercial level, or where it is declared as such by the other Party or where it is of a personal nature, to:

- Keep it strictly confidential and refrain from passing it on to anyone, except (i) to any entities of Societe Generale Group or (ii) for the strictly necessary purpose of implementing the Contract,
- Refrain from using it, directly or indirectly, or allowing it to be used by a third party under their control, for purposes other than the implementation of the Contract.

Each of the Parties undertakes in particular to keep all information obtained due to its presence on the other party's premises strictly confidential and to show great discretion with regard to the other party's techniques, resources and procedures that it has been required to share knowledge of due to performance of the Contract.

The following shall not be considered Confidential Information under the Contract

- Information that are in the public domain at their disclosure date or which becomes public knowledge after that date with neither Party responsible for the disclosure,
- Information acquired in good faith by one or other Party from a third-party not bound by a confidentiality commitment,
- Information known by the Parties before the Contract is signed,
- Information required by law or by an administrative or legal authority; it being understood that, in this case, the party concerned by these proceedings will notify the other party beforehand of the legal request for disclosure.

The responsibility of proving the above-mentioned information falls on the Party receiving the Confidential Information.

17.2 Banking Secrecy

The Beneficiary is subject to professional secrecy under the conditions defined in articles L 511-33 of French Monetary and Financial Code (and, where applicable, L 531-12 of French Monetary and Financial Code where the Beneficiary is an investment firm). As a result, the Service Provider acknowledges that the information transmitted by the Beneficiary within the framework of the Contract must be deemed to be covered by professional secrecy and therefore undertakes to keep it strictly confidential and undertakes not to pass it on to third parties without the express authorisation of the Beneficiary.

17.3 Protection of Privileged information

Privileged information is precise information, which has not been made public and which relates, directly or indirectly, to one or more issuers of financial instruments, or one or more financial instruments, and

which, if it were made public, would be likely to have a serious effect on the price of the financial instruments in question or the price of financial instruments linked to them.

The possession, even accidental, of inside information requires the person possessing it to refrain from:

- Using it on his/her own behalf or on behalf of others,
- Passing it on for purposes or activities other than those for the purpose of which it is held.

17.4 Duration of the confidentiality obligation

The obligations forming the subject of this article apply to information received from the date of signature of the Application Contract or the date on which the Beneficiary issues its statement of requirements.

The Parties will be bound by this obligation for as long as the information in question have not been made public, unless the Party in question specifically agrees previously and in writing to waive the duty of confidentiality.

This article will remain in force after the expiry or termination of the Contract for whatever reason.

17.5 Personnel and sub-contractors

Both Parties guarantee that the obligations relating to confidentiality detailed in this article will be imposed on their personnel and their possible sub-contractors and will be entirely responsible in the event that their personnel and possible sub-contractors should breach these obligations.

17.6 Restitution/Destruction

Subject to the provisions of article "Personal Data" and "Transferability", the Parties undertake to return or destroy, as instructed by the other Party, every data/information, on the request of the Party in question within a maximum time of fifteen (15) days from receiving the request.

18 PERSONAL DATA

The purpose of this article is to describe the Service Provider's commitments relating to the Processing of Personal Data when the Service Provider acts as a Data Processors (Article 18. 1 below) or as a Data Controller (Article 18.2 below) , it being understood that the terms “Data Processor” and “Data Controller” have the meaning given in the Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016 applicable as from 25 May 2018 (hereinafter, the "**GDPR**").

The qualification of the Service Provider as retained by the Parties in the context of the Processing is set out within the Application Contract.

18.1 Processing of Personal Data in the context of a “Data Controller to Data Processor” relationship

The Parties undertake to comply with all regulations in force from time to time applicable to the Processing of Personal Data, in particular the GDPR.

18.1.1. Description of the Processing

The Service Provider is authorised to process the Personal Data on behalf of the Beneficiary only to the extent necessary for the provision of the Products and Services. The authorised Processing operations are described in the appendix "Description of Personal data Processing" to the Application Contract.

18.1.2 Instructions from the Beneficiary

The Service Provider undertakes in particular to:

- Process Personal Data solely for the purpose(s) that is/are the subject of the Products and Services ;

- Process Personal Data in accordance with the instructions of the Beneficiary set out in the Contract. If the Service Provider considers that an instruction infringes the GDPR or other Union or Member State data protection provisions, it shall immediately inform the Beneficiary. In addition, if the Service Provider is required to transfer personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the Service Provider is subject, it will notify the Beneficiary of that legal obligation prior processing, unless that law prohibits such information on important grounds of public interest.
- Take into account, with respect to its tools, products, applications or services, the principles of data protection by design and by default.

18.1.3 Onward sub-processing

The Service Provider is authorized to engage the onward sub-processors listed in the Appendix of the Application Contract "List of sub-contractors -Processing locations" to carry out the Processing described in the Appendix "Description of Personal Data Processing" of the Application Contract.

In the event of the recruitment of other Sub-processors, the Service Provider shall obtain the written, prior and specific authorization of the Beneficiary.

Where the Service Provider engages an onward sub-processor for carrying out processing activities on behalf of the Beneficiary, the same data protection obligations as set out in the Contract must be imposed on onward sub-processors, by way of a contract or with another legal act, in particular to ensure that the onward sub-processors provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing of personal data meet the requirement of the GDPR. Where an onward sub-processor fails to fulfil its data protection obligations, the Service Provider remain fully liable to the Beneficiary for the performance of any onward sub-processor's obligations.

The operations entrusted to any onward sub-processor are set out in the Appendix "List of Sub-processor(s)- Processing locations". This list shall be updated in the event of any change of onward sub-processor.

18.1.4 Application of European regulations on transfers of data outside the European Economic Area

1. General provision

The Service Provider may use processing activities located in a country outside the European Economic Area (hereinafter "EEA") that has not been recognized by the European Commission as providing personal data with an adequate level of protection to that in force in the EU (hereinafter "Non-Adequate Country"), provided that the transfer of personal data outside the EU is necessary for the performance of the Services, and subject to (i) having obtained the prior consent of the Beneficiary and (ii) having secured the transfer with one of the appropriate safeguards listed by Article 46 of the GDPR (hereinafter "Appropriate safeguards") including all the necessary security measures.

The security measures provided for in the appropriate safeguard are regularly reassessed and, if necessary, adapted when they no longer guarantee an adequate level of protection.

The Service Provider provides in the appendix "Description of Personal data processing" to the Application Contract the location of the processing activities of any kind.

When the Service Provider transfers personal data toward the United States by claiming a certification to the transatlantic legal framework validated on July 10, 2023, by the European Commission (hereinafter "US-EU Data Privacy Framework"), it undertakes, in the event of loss or non-renewal of its certification to the DPF, to notify the Beneficiary and to implement as soon as possible any framework required by the GDPR.

2. Specific obligations for onward sub-processing

After prior consent from the Beneficiary, collected under the conditions set out in the "Onward sub-processing" clause of this article, the Service Provider may engage an onward sub-processor located in a non-adequate country, provided that the transfer of personal data outside the EU is necessary for the performance of the Services, and subject to:

- Carrying out and communicating to the Beneficiary a Data transfer impact assessment (hereinafter "TIA") realized in accordance with GDPR and European Data Protection Board (EDPB) requirements or, failing that, the communication to the Beneficiary of any relevant information or document allowing to carry out such a TIA;
- Deploying the necessary technical, organizational, and contractual security measures taking into account the conclusions of the TIA (hereinafter "Supplementary measures"), if necessary, in cooperation with its onward sub-processors;
- Implementing with its onward sub-processor an appropriate safeguard including, in particular, the necessary Supplementary measures;
- Providing the Beneficiary, upon first request, with a copy of the Appropriate safeguard kept up-to-date.

In addition, when the Service Provider intends to subcontract all or part of the Service to an onward sub-processor located in the United States claiming a "US-EU Data Privacy Framework" certification, the Service Provider undertakes to (i) notify the Beneficiary if this certification is not renewed or is canceled, and (ii) to ensure that:

- The onward sub-processor is effectively part of the company certified to the "US-EU Data Privacy Framework", based on the information available from the U.S. Department of Commerce's website;
- The transfer is compliant with the scope of the certification granted in terms of data processing purpose and category of data transferred, based on the information available from the U.S. Department of Commerce's website."

18.1.5 Data subjects informations

The information to be provided pursuant to the GDPR to natural persons concerned by a Processing activity (hereinafter "Data subjects") are provided by the Beneficiary at the time of the initial collection of the personal data.

18.1.6 Data Subjects rights and response to Beneficiary request

The Service Provider undertakes to respond in writing to the Beneficiary's requests, within five (5) working days of the request, to allow the Beneficiary to:

- Respond to data subjects exercising a right provided for by the GDPR within the regulation deadline;
- Carry out a TIA;
- Respond to Data protection authority's requests;
- Ensure the compliance of its Data processing activities.

When a Data Subject exercises a right provided for by the GDPR directly with the Service Provider, the Service Provider must immediately transfer the request upon receipt by e-mail to Sg-Protection.Donnees@socgen.com

18.1.7 Notification of Personal data breaches

The Service Provider shall notify the Beneficiary as soon as it becomes aware of a data breach impacting its organization and relating to personal data subject to this Contract.

The notification shall be made by e-mail to the address "breach-groupdpo.eur@socgen.com" and shall include, in particular, the elements listed below, accompanied, if relevant, by any information or document enabling the Beneficiary to investigate the incident:

- Description of the data breach including where possible, the categories and approximate number of data subjects impacted and the categories and approximate number of personal data records affected;
- Name and contact details of the data protection officer or other contact point where more information can be obtained;
- Likely consequences of the data breach;
- Measures taken or proposed to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

When the Service Provider is unable to provide the aforementioned information immediately, it undertakes to communicate them to the Beneficiary as soon as possible and, in any event, without undue delay.

18.1.8 Security measures

The Service Provider undertakes to implement the security measures described in the “Security” article as well as:

- The means to ensure the confidentiality, integrity, availability and ongoing resilience of its systems and processing activities of personal data;
- The means to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident;
- A procedure for regularly testing, analyzing and evaluating the effectiveness of technical and organizational measures to ensure the security of the Processing, and providing evidence at first request of the Beneficiary;
- Make the Beneficiary's personal data accessible only to employees (i) trained to protect personal data, (ii) authorized by virtue of their duties and (iii) subject to an obligation of confidentiality, and this, strictly within the limits of what is necessary for the performance of their duties.

18.1.9 Retention period

At the end of the Processing of the Personal Data, the Service Provider undertakes to (i) return to the Beneficiary and/or the third-party Provider designated by the Beneficiary and (ii) to destroy all Personal Data.

The Service Provider undertakes to provide to the Beneficiary a personal data destruction record.

18.1.10 Data Protection Officer

The Service Provider will inform the Beneficiary of the name and contact details of its data protection officer, if any.

18.1.11 Records of Processing activities

The Service Provider shall keep written records of all the categories of Processing activities which it has carries out for the Beneficiary in accordance with the provisions of the GDPR.

18.1.12 Documentation and audit

The Service Provider will provide the Beneficiary with the records necessary to demonstrate compliance by the Service Provider with all its obligations and to enable audits, including inspections, that may be carried out by the Beneficiary in accordance with the terms and conditions of the article "Audit and Inspection by the Beneficiary".

18.2 Processing of Personal Data in the context of a “Data Controller to Data Controller” relationship

As part of the organization and execution of the purpose of the Products and Services, the Service Provider is considered to be a Data Processor and as such undertakes to comply with all obligations incumbent upon it resulting from the regulations applicable to the Processing of Personal Data, in particular, the GDPR.

19 SECURITY

19.1 General security obligations

In general, it is the Service Provider's duty to implement the necessary technical and organisational measures to ensure the security of the Beneficiary's data, in order to:

- ensure the availability, authenticity, integrity, confidentiality of the Beneficiary's IT system insofar as the Products and Services may have an impact on it;
- protect the Beneficiary's data from disclosure, modification, destruction, loss, alteration, access, processing, whether accidental, illegal or unauthorised.
- the implementation of the measures to make the Beneficiaries' Personal Data accessible and viewable only to those personnel of the Service Provider duly authorized and authorized by reason of their functions and quality, within the strict limits of what is necessary for them to the performance of their duties;
- ensure the traceability of operations and processing performed for the Beneficiary and likely to impact the security of the Beneficiary's data;
- maintain the appropriate level of information systems security skills for the Products and Services to be provided in accordance with the contract terms (qualifications, authorizations, certifications) and be able to prove it upon request. It must also certify that it has sufficient understanding of the technologies required and the necessary know-how;
- maintain up-to-date all IT solutions (software, firmware, IT components, workstation, devices) used by the Service Provider during the contract. The Service Provider must inform the Beneficiary as soon as its inability to maintain such solutions comes to its knowledge or in case of obsolescence or IT solutions end of support.
- The systematic maintenance of all IT solutions (software, firmware, components, workstations, devices) used by the Provider for the benefit of the Beneficiary. The Provider is obliged to inform the Recipient as soon as he knows that he will be unable to carry.

The entire set of rules is reflected in the information system security policy of the Service Provider, which defines the measures aimed at protecting the availability, integrity, and confidentiality of data, information assets, and ICT assets of the beneficiary and those of their clients.

The Service Provider undertakes to prove, it has implemented these measures during the entire term of the Contract, immediately on the Beneficiary's request.

Subject to the provisions of Articles "Personal Data" and "Transferability", the Parties undertake to return or destroy, as instructed by the other Party, every data/information, on the request of the Party in question as soon as the request is received by the other Party. On the request of the Beneficiary, the Service Provider will transmit the data destruction report duly completed and signed, according to the template enclosed in Appendix "Data destruction report".

The security policies, procedures and measures implemented by the Service Provider, on the Beneficiary's instructions as it may be, must in any event be documented, accessible to the Beneficiary, adapted to the sensitivity of the Products and Services and remain compliant with Good Industry Practice and international standards or recommendations (eg. National Institute of Standards and Technology (NIST) cybersecurity framework, ISO 27001/27002/27005, 2020 FSB CIRR toolkit, G7 Fundamental Elements of Cyber security in the finance sector, CPMI-IOSCO guidance on cyber resilience, 2020 FSB CIRR toolkit, the G7 Fundamental Elements of Cyber security in the financial sector and the BCBS principles for operational resilience.) applicable in this field.

The Service Provider assures the Beneficiary that all regulatory requirements related to information systems security are identified and fulfilled all along the duration of the Contract.

The Service Provider ensures that its personnel and subcontractors in charge of the assignment comply with the security obligations and ensure they are kept regularly informed.

The security monitoring of the Provider by the Beneficiary may be strengthened, on the initiative of the Beneficiary, by sending an annual questionnaire to the Service Provider, aimed at measuring the

Service Provider's level of maturity with the security commitments made under the Contract. The Service Provider undertakes to respond to that questionnaire exhaustively and faithfully, at no additional cost, so that the Beneficiary can take the appropriate measures to dynamically adapt the risk management measures.

At the end of the Contract, the Service Provider undertakes to return any equipment or device provided by Societe Generale.

19.2 Obligation relating to the protection of the Service Provider's IT System

Due to the sensitivity of the Beneficiary's data that may be processed in the Service Provider's IT system, the latter shall take particular care to ensure the physical and logical security of the IT system used to process the Beneficiary's data. The Service Provider commits to maintaining up-to-date inventories of the assets involved in delivering services to the Beneficiary.

When the Service Provider's IT system should process data belonging to the Beneficiary, the Service Provider undertakes to ensure:

- The recording by the service provider of the Beneficiary's assets concerned by the service in up-to-date registers;
- The maintaining of an inventory of network interconnexions with stakeholders involved in the Products and Services delivered to the Beneficiary and the supervision of these interconnexions;
- back-up of the data necessary for the service and of the Beneficiary's data, when applicable and on the request of the Beneficiary, so that service and data can be restored.
- Back-up procedures are formalized and shall include in particular the responsibilities, periodicity, storage conditions, process for access and restoration as well as the control processes.
- The storage and processing of the Beneficiary's data separately from its own data or from any other Service Provider's client data.
- data confidentiality and integrity of data at rest, in transit, and when possible, as well as, if encryption is used, the protection of the keys through which the Beneficiary's data is encrypted .
- Implementation of a system for detecting sensitive data leaks (email, web browsing, copying to removable media)
- Segregation between production environments and non-production environments
- Protection of data outside of the production environment through mechanisms of minimization, desensitization, and encryption for the most sensitive data
- The access management relying on the least privilege principle, the definition of user and technical profiles, the implementation of the segregation of duties, the regular review of access rights (at least annually), the systematic use of nominative user account.
- Implementation of authentication systems for all the persons accessing the Beneficiary's data via logical access control. These controls will be reinforced by using Strong Authentication (i.e. Authentication using two or more factors to achieve authentication. Factors include: something you know (password/PIN), something you have (cryptographic identification device) or something you are (biometric)) methods such as multi-factor authentication to limit access to sensitive data and/or functions.
- The implementation of a bastion service to access technical administration tasks; its access is secured through strong authentication, the flows between the bastion and the administration workstations and managed assets are encrypted according to best practices, and the logs are collected.
- The implementation of network segmentation that prevents access to administration functions of managed assets without going through the bastion service.
- Transmission to the Beneficiary, on the latter's request and immediately, of traces/records (such as log files and security events) and all security analyses performed for it by the Service Provider

during the term of the Contract. The Beneficiary is hereby authorised to transmit these elements to competent authorities, on their request.

The Service Provider also undertakes to implement a trace policy designed to keep usable records for one year of the actions and/or attempted actions performed in its IT system (e.g. outgoing/incoming data streams, new application versions, tests, errors, deduplication and wipes etc.) for audit and evidentiary purposes. The records must include as a minimum nature, reference, user ID and time stamp and must be stored in a centralized tool.

- Implementation, as soon as the Service Provider is aware of an incident or a threat which may affect its IT system, of suitable strengthened security measures or any solution which makes it possible to efficiently respond to the incident or the threat.
- The centralized retention of source code and the Software Bill Of Materials, necessary for the execution of Products and Services provided to the Beneficiary.
- The implementation of a firewall, with filtering rules being recertified at least every six months, to protect the assets required for the execution of the Products and Services for the Beneficiary.

The security measures implemented by the Service Provider must be documented, compliant with Good Industry Practice applicable in this field and appropriate, such as logical access controls and the encryption means applied to the Beneficiary's data compliant with market standards in order to prevent access to its IT system by unauthorised persons.

The Service Provider implements a procedure to test, analyse and evaluate, at least once a month, the effectiveness of technical and organizational measures to ensure the security of the processing of personal data.

The Service Provider set up a policy dedicated to the security of its IS infrastructure and implements technical and organisational measures, methods and protocols compliant to market standards to minimise the risks related to the infrastructure it uses.

In this respect, it implements automated mechanisms to isolate the affected informational assets in case of events of cyber attacks.

The Service Provider undertakes to inform the Beneficiary of the locations where the latter's data is hosted, stored and processed. The Beneficiary may define a restricted geographical area where its data can be hosted, stored and processed. Said geographical area is defined in the Appendix "List of subcontractors - Processing locations" of the Application Contract.

With regard to the activities provided, the Service Provider must implement all technical and organisational resources with a view to complying with the constraints of the PCI-DSS Standard for applications which store, process or transfer sensitive bank card data.

PCI-DSS assessments must be carried out by authorised organisations and repeated annually.

The Service Provider must be able to justify, upon Beneficiary request, the implementation of every above-mentioned measures for the entire duration of the Contract.

19.3 Security incident detection and management

19.3.1 Incident detection and management

19.3.1.1 Security Incident Detection

The Service Provider is committed to proposing the implementation of a security incident management framework outlining the incident detection, incident response and crisis management processes.

These processes will include:

- The Service Provider's monitoring of its information system in order to detect security events and trigger an alert in the event of a security incident.

- Maintaining a security incident management procedure that analyses, classifies, contains and responds to these events in a timely manner.

19.3.1.2 Security Incident notifications to the Beneficiary

The Service Provider is under the obligation to:

- inform the Beneficiary, as soon as acknowledged, of any security incident, that is susceptible to affect the information system, the Beneficiary's data or information. in a way that business continuity, confidentiality or integrity would be affected, by sending an email to the address cert.sg@socgen.com, followed by a phone call to CERT Societe Generale (+33(0)1-5898-7200). When notifying the incident to the Beneficiary, the Service Provider will transmit all the documentation and the useful technical information that will allow the Beneficiary to assess the impact of the incident as major if relevant, and if necessary to notify the incident to the competent authority.
- Keep the Beneficiary updated of the evolution of the incident
- Provide the Beneficiary with a single point of contact to communicate on any incident;
- Provide the Beneficiary with an appropriate support in case of incident affecting the service it provides, with no additional fee.

In the event of a security incident on the Service Provider systems susceptible to affect the Beneficiary's security, the latter will have to decide to cut, until the incident is fully controlled and the remediation completed, partially or totally every technical links with the Service Provider.

The Service Provider undertakes to assist the Beneficiary for no additional fee in taking any action to remedy or deal with a security incident, including by notifying the competent authorities and the persons affected by the breach.

19.3.2 Vulnerability management

The Service Provider undertakes to:

- Keep up-to-date a vulnerability management policy and procedure ranging from identification to the deployment of patches and updates.
- Inform the Beneficiary about the risks related to the security and protection of the systems, and offer to implement concrete solutions for detecting attempted intrusions and security breaches, specifying the associated cost which must be agreed by the Beneficiary.
- Inform the Beneficiary with no delays, of any critical vulnerability related to the service provided.
- If any new critical vulnerability affecting the security of Products and Services is identified, to respect the period time described below for each following steps:

make available to the Beneficiary within two working days from the time it has been identified, any palliative or workaround solution which does not, in any manner, modify the price and the functionalities of the Products and Services supplied under the Contract.

make available to the Beneficiary within five working days from the time it has been identified, a definitive solution to fix the problem and keep the Beneficiary regularly informed of the progress of its actions.

In the event no solution should be provided within the agreed deadlines, a remediation plan shall be agreed between the Parties within thirty (30) days.

supply to the Beneficiary or implement the necessary software patch as soon as the Service Provider knows about it or as soon as it is provided by the developer and/or the manufacturer.

19.3.3 Security Testing

The service provider must define and deploy up-to-date procedures on security testing of the Products and Services, products and data of the Beneficiary.

These procedures must allow the detection of Vulnerabilities. To ensure the detection of vulnerabilities, these procedures shall include relevant security testing techniques such as:

- Source Code review that ensures that Products and Services delivered to the Beneficiary are not affected by any libraries.
- Scan for unprotected secrets
- Weekly Vulnerability Scans
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Penetration Tests

The Service Provider is required to provide, at least annually, the Beneficiary with indicators on the execution of these tests.

The Service Provider is required to remediate the vulnerabilities detected by these tests in accordance with the requirements defined in the Vulnerability management section hereafter.

19.4 Commitments in case of use of the Beneficiary's IT system by the Service Provider

19.4.1 Security measures

When the Service Provider's personnel may have access to the Beneficiary's IT system, with the latter's express prior authorisation, whether while working on the Beneficiary's premises or through remote access, the Service Provider must implement the following security measures:

- The Service Provider undertakes to only use the resources and connection means to the Beneficiary's IT system, made available to it by the latter, for the sole purpose of providing the Products and Services agreed in the Contract.
- In this respect, any use, communication, dissemination or transmission in any manner by the Service Provider of the Beneficiary's confidential information, such as defined in the "Confidentiality" clause of the Contract, outside the Beneficiary's IT system is not permitted without the latter's authorisation, regardless of the cause, the reason, or the purpose.
- In the event that the use of the Beneficiary's IT system requires high-strength authentication means, the Service Provider shall comply with the Beneficiary's delivery and protection processes relating to these means.
- The Service Provider commits itself to keep up-to-date and communicate to the Beneficiary, the inventory of access rights to the Beneficiary's IT system, until the end of the Contract.
- When the Contract comes to an end, both Parties revoke all access rights to the Beneficiary's IT system for the Service Provider.

19.4.2 Awareness, training and good practices

The Service Provider staff will attend the IT systems raising awareness module. The Service Provider shall ensure that its employees complete the training materials intended for them, available through the Service Provider dedicated platform for training *MyElearning*, within the first few days of it made available by the Beneficiary.

The Service Provider is required to respect the Beneficiary's "User charter for information protection and use of IT resources" when processing the Beneficiary's assets.

The Service Provider shall ensure that its employees that have, under the Products and Services provided, an account qualified by the Beneficiary of "Account with Privileges" (i.e. account with extended rights, enabling to perform administration or management actions not authorized to regular users) realize before the beginning of the mission the module of awareness "Accounts with privileges" approved by Society General as available under the following link: an e-learning on https://cybersecurity.youaredigital.fr/.

The Service Provider and its staff must respect the good practices as regard as accounts with privileges available in Appendix “Good practices related to the usage of privileged accounts “, during the entire Contract period.

20 AUDIT AND INSPECTION BY THE BENEFICIARY

The Service Provider undertakes to ensure that its level of risk control is constantly monitored and that the security policies and rules applicable to the Products and Services are complied with, including by its own sub-contractors.

20.1 Conditions and scope of the audit

The Service Provider expressly authorizes the Auditor (**i.e.**, means the Beneficiary or any individuals or legal entities (whether or not belonging to the Societe Generale Group) commissioned by the Beneficiary to conduct an audit) to carry out an audit of the Products and Services, including of its own sub-contractors, to verify that the Service Provider's obligations under this Contract are met.

The Beneficiary may not exercise its right to conduct an audit more than twice (2) over the course of a twelve (12) month's period and shall perform the audit during opening hours in order not to significantly disrupt the Service Provider’s and its sub-contractors’ activities. In case of major security incident, the Beneficiary may conduct, as an exception, an additional audit.

Notwithstanding anything to the contrary in the Contract, the audit may be conducted without any prior notice if the application of a notice is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.

In particular, the audit will allow to ensure:

- that the Service Levels are met;
- that the Calendar is applied;
- that the integrity and confidentiality of the Beneficiary's Data are protected in compliance with the stipulations set out in the Contract, and specifically the "Security", "Personal Data" and "Confidentiality" clauses;
- that the physical site of the Service Provider or its subcontractors where Beneficiary Data is hosted is secured;
- that the general security obligations laid out in the "Security" clause are met.

The Service Provider accepts that the auditor will have access, including on the premises, to the facilities and infrastructures dedicated to implementing the Contract as well as the information it needs to perform its duties, specifically to the results of previous audits performed under the terms of the Contract with the Service Provider or its sub-contractors.

The purpose of the audits carried out on the premises shall be to assess the security level of the resources (equipment, infrastructures, applications, etc.) used by the Service Provider and/or by third parties it has appointed for this purpose, to provide the Services, including:

- Regarding the security organisation, to identify Vulnerabilities related to the system's operating processes and to security management;
- Regarding the configuration of IT system components, to review the technical configurations of the components used by the system where the Beneficiary's data is processed.
- Regarding the security of hosting sites, to verify that the necessary measures have been taken to secure the hosting site in accordance with the Beneficiary's requirements.

The Service Provider expressly accepts the inspections intended to verify that the Service Provider's obligations under the Contract are met and to verify the security level of the Beneficiary's IT system managed by the Service Provider to be carried out by a regulatory authority or, as the case may be, by a third party appointed by the State, under the conditions defined by law.

The Service Provider also agrees to answer every question asked by the auditor and/or the regulatory authority and to allow access, under the Service Provider's supervision, to all the tools and means necessary to conduct the audit process.

The Beneficiary undertakes to pay for the internal costs related to the audit process.

20.2 Failure management

Should the audit report or the technical audits reveal a failing by the Service Provider to meet its contractual obligations, a meeting of a steering committee which includes representatives of the Beneficiary and the Service Provider will be called by the Beneficiary. The purpose of this meeting will be to consider, together, the means that will be used to deal with the failures and the conditions (including deadlines) under which the Service Provider will implement the corrective measures deemed necessary by the aforementioned committee to remedy the failures.

In the event that the Service Provider should fail to remedy the failures identified by the audit within the required time, the Beneficiary will automatically be entitled to terminate the Contract without prior notice, without prejudice to any damages it may claim.

21 FORCE MAJEURE

Neither Party is liable for any failure to perform its contractual obligations under this Contract due to an Event of Force Majeure.

Where there is an Event of Force Majeure, the Party prevented from performing its contractual obligations under the Contract must immediately notify the other Party giving full particulars of said Event of Force Majeure and the reasons for the Event of Force Majeure preventing that Party from performing its obligations under this Contract and that Party must use its best efforts to mitigate the effect of the Event of Force Majeure upon performance of the Contract and to fulfil its obligations under this Contract.

Upon completion of the Event of Force Majeure, the Party affected must as soon as possible recommence the performance of its obligations under this Contract.

To the extent that an Event of Force Majeure continues for a period exceeding fifteen (15) days, the Parties agree to enter into discussions in order to take this into account.

If they fail to agree on the consequences to be given to this situation within a maximum period of fifteen (15) days, the Contract may then be terminated without compensation by either party subject to a written notice to the other Party and without prejudice to the application of the provisions of the article "Reversibility".

22 LIABILITY

Each Party will be liable to the other Party in accordance with the rules of common law and will compensate the other Party for direct damage/losses of any kind.

The Service Provider is responsible for its personnel and sub-contractors and for damage/losses caused by its personnel and sub-contractors.

Neither Party is liable for:

- damage/losses which may result from an action by the other Party, an action by a third party or a case of force majeure,
- consequential damage/losses such as those accepted by French case law.

Notwithstanding any stipulation to the contrary in the Contract, no limitation of liability or compensation shall apply in respect of :

- Compensation pursuant to Article “”Intellectual property indemnification »;
- Failure to comply with the confidentiality obligations set out in the “Confidentiality” Article;
- Failure to comply with the obligations relating to the Processing of Personal Data set out in the “Personal Data” Article;

- Bodily injury, as well as any damage caused by willful misconduct or gross negligence;
- Other cases provided for by applicable law and jurisprudence.

The present article shall survive the termination and expiration of the Contract for any reason whatsoever.

23 TERMINATION OF THE CONTRACT

23.1 Termination for breach

In the event of a failure by a Party to comply with its obligations under the Contract, the other Party may formally notify the breaching Party to remedy such breach within a maximum period of thirty (30) calendar days, by means of a registered letter with acknowledgement of receipt.

If, by the end of the thirty (30) calendar days period, the breach has not been (or is not capable of being) remedied, the other Party may as of right terminate all or part of the Contract, by means of a registered letter with acknowledgement of receipt, without prejudice to any damages or interest that it may be entitled to claim.

In the event of termination of the Contract, for whatever reason, the Service Provider shall deliver to the Beneficiary the Services and Deliverables as they were on the effective date of termination and the Beneficiary shall pay to the Service Provider the consideration for the Services actually performed by the Service Provider up to the effective date of termination.

23.2 Termination for regulatory and/or legislative cause

It is agreed between the Service Provider and the Beneficiary that the Beneficiary may terminate the Contract as of right, without indemnity and without prejudice to the provisions of article "Transferability", if:

- the termination of the Contract is requested by the European Central Bank or any other relevant authority to whose supervision the Beneficiary or the Societe Generale Group is subject, in which case the termination shall take effect at such time as requested by such authority;
- the termination of the Contract is required because the terms of the Contract fail to comply with any regulation (or change thereto) applicable to the Beneficiary or the Societe Generale Group coming into effect after the date of the Contract, in which case the termination of the Contract shall take effect without prior notice.

23.3 Termination for convenience

It is hereby agreed between the Service Provider and the Beneficiary that the Beneficiary shall be entitled to terminate the Contract for convenience at any time.

In this case, the Beneficiary will have to comply with the two following cumulative conditions:

- The Beneficiary must send its request for early termination by registered letter with acknowledgement of receipt, giving at least as many months prior notice of such termination as the number of years that has elapsed since the beginning of the contractual relationship, but in no event more than eighteen (18) months;
- The Beneficiary shall pay the Service Provider compensation equivalent to 25% of the amount still owed by the Beneficiary to the Service Provider under the Application Contract concerned.

23.4 Termination relating to the use of an ICT service

This Article applies when the Products and Services are classified as “ICT Services” within the Application Contract.

It is agreed between the Service Provider and the Beneficiary that the Beneficiary may, ipso jure, without compensation and subject to the provisions described in the “Reversibility” clause, terminate the Contract in the event of:

- A serious breach by the Service Provider of the applicable legislative or regulatory provisions;
- Circumstances likely to affect the performance of the Products and Services, in particular in the event of significant changes affecting the Products and Services or the Service Provider's situation.
- Proven weakness(es) on the part of the Service Provider with regard to its overall management of ICT-related risks within the meaning of DORA and, in particular, the manner in which the Service Provider ensures the availability, authenticity, integrity and confidentiality of the Beneficiary's Data;
- Where a supervisory authority can no longer effectively supervise the Beneficiary due to conditions or circumstances relating to the Contract.

24 TRANSFERABILITY

The Service Provider guarantees the Beneficiary access to, retrieval and return of the Beneficiary's Data in an easily accessible format, particularly in the event of insolvency, resolution, discontinuation of the Service Provider's activities or termination of the Contract for any reason whatsoever.

25 INSURANCE

The Service Provider declares that he has contracted insurance from a reputedly solvent insurance company covering the consequences of his Professional Civil Liability, his General Civil Liability/Operation, and cyber insurance, up to an amount corresponding to the risks and responsibilities incumbent upon him under both the ordinary law and his contractual commitments, and in accordance with the customs of the profession. The Service Provider undertakes to maintain this insurance for the entire term of the Contract and to inform the Beneficiary of any changes.

The Service Provider must prove to the Beneficiary that it has taken out this insurance in response to request from the Beneficiary.

26 CHANGE OF OWNERSHIP OF THE SERVICE PROVIDER

As the Contract has been entered into *intuitu personae*, the Service Provider must inform the Beneficiary of any change of control (within the meaning of Article L. 233-3 of the French Commercial Code) by registered letter with acknowledgement of receipt sent within one month of such change of control.

The Beneficiary may, within one (1) months from the receipt of such notification, send the Service Provider a termination notice by registered letter with an acknowledgement of receipt, such termination to take effect one (1) month after receipt by the Service Provider of such termination notice.

If the Service Provider fails to notify the Beneficiary in accordance with this article of any change of control which occurs with respect to the Service Provider, the Beneficiary may terminate the Contract as of right, without indemnity and without prior notice, by sending a registered letter with an acknowledgement of receipt to the Service Provider.

27 ASSIGNMENT OF THE CONTRACT

Except in the case of an enforced assignment of the Contract occurring within the framework of insolvency proceedings of which it is the subject, the Service Provider may not assign, transfer or transmit to a third party, for whatever reason and by whatever means, including within the framework of an operation resulting in the universal transfer of all or some of its assets, the obligations incumbent on it by virtue of the Contract, without the prior written agreement of the Beneficiary

In case of failure regarding this provision, the Beneficiary may inform the Service Provider, by registered letter with acknowledgement of receipt, within a three (3) months delay starting from its knowledge of

the assignment, of its intention to terminate the Contract. Termination of the Contract will be effective one (1) month after receipt of such letter by the Service Provider.

It is stipulated that the Service Provider's obligations under the terms of the Contract will remain in force, without it being necessary to obtain the agreement of the Service Provider, in the case of:

- the transfer by the Beneficiary of all or some its rights and obligations under the terms of the Contract to any company within its group,
- changes in the assets or the corporate body of the Beneficiary, as follows, without this list being exhaustive, the transfer of business, lease management, a merger, partial contribution of assets or de-merger. Furthermore, any change in the Beneficiary share ownership, including in the case of a change of ownership, may not provide a reason for continuation of the Contract to be called into question.

In the event of the occurrence of one of the aforementioned operations, the Beneficiary will inform the Service Provider as quickly as possible and the Service Provider will confirm that from this point in time it accepts these operations and recognises the Beneficiary possible successor, which, as a result, will become its co-contracting party.

28 SUB-CONTRACTING

The Service Provider may not outsource all or any of its obligations under the Contract without the prior written agreement of the Beneficiary. In the event of authorized sub-contracting, the Service Provider will ensure that any subcontractors comply with all provisions in this Contract. In this regard, the Service Provider undertakes to entrust its subcontractor(s) with all obligations, at least equivalent to those stipulated in this Contract.

When the Products and Services are classified as “ICT Services” within the Application Contract, authorized subcontractors shall be listed in an Appendix to the Application Contract entitled “List of subcontractors under the article “Sub-contracting” of the General Terms and Conditions”

29 COMMUNICATION

The Beneficiary authorizes the Service Provider to include its name, during the term of the Contract only, with the exclusion of any other information, on a list of references that it may circulate to prospective clients. Any other communication in any form whatsoever and for whatever reason will be subject to the prior written agreement of the Beneficiary.

30 ICT SERVICE WITHIN THE MEANING OF REGULATION (EU) 2022/2554

When the Products and Services are classified as “ICT Services” in the Application Contract, the Service Provider undertakes, in addition to the obligations already provided for elsewhere in the Contract, to:

- Cooperate fully with the Beneficiary's competent authorities and resolution authorities, including the persons appointed by them;
- To provide, at no additional cost, assistance in the event of ICT-related incidents in connection with the Products and Services.

31 GENERAL CLAUSES

31.1 Titles

The titles of paragraphs and articles of the Contract are used to make the Contract easier to read but may not, in any case, be used as a guide for interpretation.

31.2 Elected domicile

For the implementation of the Contract and its effects, the Parties elect domicile at their respective registered offices as they appear at the beginning of this Contract.

31.3 Partial invalidity

Should one or more stipulations of the Contract be ruled, pronounced or declared invalid on the basis of a particular law, regulation or ruling by a competent court, the Parties will meet to agree on one or more stipulations to replace the invalid stipulation or stipulations and to enable the aim of the original clause or clauses to be achieved as far as possible. All other stipulations of the Contract will retain their force and scope.

31.4 Non-waiver

The fact that one of the Parties fails to invoke a failure by the other Party to fulfil any one of its obligations may not be interpreted as a waiver of the obligation in question or as an addendum to the Contract, which may prevent the non-defaulting Party from invoking it in the future.

31.5 Notification

Notifications are issued by means of a registered letter with an acknowledgement of receipt. Unless stipulated otherwise in the Contract, any notification will become effective from the date on which it is first presented.

32 APPLICABLE LAW, DISPUTES AND ALLOCATION OF JURISDICTION

The Contract is governed by French law.

In the event of a dispute that may arise between the Parties regarding the validity, implementation or interpretation of the Contract, the Parties undertake to work together diligently and in good faith with a view to finding an amicable solution. In this regard, internal mediation may be used by either Party notifying its claim at: mediation.par@socgen.com.

If however, no agreement can be reached within a period of three (3) months from the receipt of a letter notifying the other party of the existence of a disagreement, sole jurisdiction is allocated to the Paris Commercial Court (or if the Paris Commercial Court is declared incompetent, a court under the jurisdiction of the Paris Court of Appeal) without regards to a plurality of defendants or the introduction of third parties.

The obligation to comply with the aforementioned deadline does not apply to emergency, interim, summary or ex parte proceedings. The Paris Commercial Court (or, in the event of the Commercial Court's lack of jurisdiction, a court within the jurisdiction of the Paris Court of Appeal) is also expressly empowered to hear such emergency or protective proceedings.

APPENDICES A – GENERICS

Appendix A.1 - Obligations relating to the fight against unreported employment and fraudulent transnational secondment

FRENCH DOMICILED COMPANY

(Articles D. 8222-5 and D. 8254-2 of French Labour Code)

Documents, certificates, and lists to supply at the signature of the Contract, and then, every 6 months.

Documents to be supplied:

1. A certificate of provision of social declarations and payment of social taxes and contributions issued by the organization of Social Protection in charge of the collection of the social taxes and contributions falling to the Party and of less then 6 months (URSAFF certificate). Remarks: the authenticity verification of the certificate falls to the Client
2. An extract of the registration in the Trade and Companies Register (K or K bis);

[Or an identification card proving the inscription in the register of occupation;

Or an estimate, an advertising document, or a professional correspondence provided it mentions the name, or the corporate name, the full address, and the registration number delivered by the occupation register, or a list or a chart of a professional order, or the reference of the approval issued by the competent authority;

Or a receipt of a declaration deposit in progress of registration with a centre of professional formalities for natural or juridical person]

Foreign employees

A nominative list of the foreign employees submitted to a work authorization required by the Article L 5221-2 of the French Labour Work.

This list, based upon the personnel register, must precise for each employee:

- his hiring date,
- his nationality,
- the nature and the order number of the document used as a work authorization.

COMPANY SITED ABROAD

Fight against unreported employment:

(Articles L. 8222-4 / D. 8222-7; L. 8254-1 and L. 8222-4 / D. 8254-3 of the French Labour Code)

Transnational secondment:

(Articles L. 1262-2-1 / R. 1263-2-1 and R.1263-3; L. 1262-4-1 / R. 1263-12; L. 1221-15-1 / D. 1221-24 and D. 1221-24-1; L. 4231-1 and L. 8281-1 of the French Labour Code)

Documents to provide at the signing of the Contract, and every six months:

The listed documents shall be written in French or supplied with a French version.

I - Documents required by the regulations relating to the fight against unreported employment

In any cases, the Provider/Consultant agrees to supply:

1. A document mentioning its individual identification number allocated accordingly to article 286 ter of the French general tax code;

[if the Service Provider is not required to have such a number, a document including its address and identity or, when necessary, the details of its temporary tax representative in France;]

2. A document certifying the regularity of the company's social situation with regard to EU regulation n°883/2004 of April 29th, 2004 or any international law on social security
3. **and**, when the legal texts of the country of address demands it, a document issued by the organization in charge with the mandatory social regime declaring the Party up to date with its social declaration and the payment of the related contributions, or an equivalent document, or, failing that, a certificate of provision of social declaration and payment of the related contributions required by article L. 243-15 of the French Code of Social Security. In the latter hypothesis, the Client must make sure of the authenticity of said certificate with the organization in charge of collecting social contributions.

NB: regarding the document certifying the regularity of the company's social situation, French jurisprudence specified that it was certificate E 101 which has become certificate A 1.

When the Party's registration in a professional register is mandatory in the country of address, one of the following documents:

1. A document issued by the authority holding the professional register, or an equivalent document certifying the registration;
   [or an estimate, an advertising document or a business correspondence, on which appears the Service provider's name or corporate name, full address and the nature of registration with the professional register; Or for companies to become, a document of under six months issued by the competent authority attesting to the application for registration with the professional register].
2. When the provider has foreign employees from non-member states of the European Union.

It must, when signing the contract (only), supply to the Client (SG) a nominative list of the foreign employees for whom a work permit is required. This list must specify for each employee:

- their hiring date,
- their nationality,
- the type and order number of the work permit.

II - Documents required by the specific regulations on transnational secondment (foreign company sending employees on secondment in France)

Any foreign provider which second employees in France must, prior to commencement of the service contract, supply to the client (SG) the following documents:

- For each employee, a copy of the secondment declaration transmitted to the labour inspectors of the location where services must be provided. This declaration must be appended to the personnel register of the SG entity that invites the employees on secondment and is made accessible to the staff representatives and the administration controllers. A secondment declaration CERFA template is available at https://mdel.mon.service-public.fr/pro_mademarchev5/sfjsp?interviewID=SIPSI
- A copy of the letter of appointment of a representative in France of the foreign company in charge of liaising with the administration controllers listed in article L. 8271-1-2 of the French Labour Code. This letter of appointment must include the name, surname date and location of birth, email and postal address in France, when applicable the corporate name, and the telephone number of the representative. It specifies the acceptance of the appointment by the person concerned and the effective date and duration of the appointment, which cannot exceed the period of secondment. It must indicate, for the documents listed in article R. 1263-1 (documents that the provider is supposed to keep on the premises where the services are provided), either the location where they are kept on the national territory, or the conditions to access them and review them from the national territory.
- A sworn statement from the Provider indicating that employees are accommodated in suitable conditions compatible with human dignity but also that it complies with Labour Law as regards:
  - Individual and collective freedoms at the workplace;
  - Discriminations and professional equality between women and men;
  - The protection of maternity, maternity, paternity and child care leaves, leaves for family events;

- The conditions of placement and guarantees to workers by companies providing temporary employment;
- The right to strike;
- Working hours, compensatory rest, public holidays, annual paid leaves, working hours and night work for young workers;
- Conditions of eligibility to adverse weather leaves;
- Minimum wage and payment of the wage, including overtime pay;
- Rules relating to health and safety at work, legal working age, employment of children

Appendix A.2 - Data Destruction Report

TEMPLATE REPORT TO BE SIGNED BY THE SERVICE PROVIDER WHEN BENEFICIARY DATA SHOULD BE PROCESSED BY THE SERVICE PROVIDER OR ANY OF ITS SUBCONTRACTORS REPORT DESTRUCTION OF BENEFICIARY DATA BY THE SERVICE PROVIDER

The company _____ (hereinafter the "Service Provider") and Societe Generale [or Group entity] (hereinafter the "Beneficiary") concluded on _____ a contract for_____ regarding_____.

The Service Provider certifies that it has destroyed all of the data and/or information of the Beneficiary that it has processed directly or using a subcontractor, under the terms of the Contract. The Service Provider certifies that its subcontractor has also fulfilled this obligation of destruction, on the date hereof.

Drawn up in_____, on _____

Surname and name of the representative of the Service Provider: _____

Signature: _____

To be signed in two original copies, one for the Service Provider, one for the Beneficiary.

Appendix A.3: User charter for information protection and use of IT resources

The protection of Societe Generale's Information Assets and Information System is a key stake. This protection is everyone's responsibility.

The following charter confirms Societe Generale's desire to:

- Protect its Information Asset and its brand image.
- Ensure a fair and responsible use of its Information System.

The application of this Charter forms part of the general principles of social and professional life, and reflects Societe Generale's commitments in the area of information protection and use of IT resources. It aims to achieve a balance between the company's security needs and respect for individual and collective freedoms. The exercise of these freedoms has consequences and limits, which is what this text intends to recall.

This charter reminds Users of their responsibility, the rules of use and the controls carried out to enable Societe Generale to protect itself against all types of risks such as fraud, information leakage, unavailability of its Information System, cybercrime and regulator non-compliance.

Societe Generale is committed to regularly informing the User of the rules contained in the charter because the User is the most important actor in Information Protection.

1. Objectives and scope

1.1 Objectives

Societe Generale provides to all Users of its Information System a set of IT Resources as well as information and data needed to accomplish their missions. The use of these resources requires each User to comply with the rules laid down by Societe Generale.

This charter sets the rules to ensure the security and performance of the Information System, to preserve the data confidentiality in compliance with the laws in force and the rights and freedoms recognized to Users. The examples mentioned in this charter are not exhaustive.

The Charter shall be annexed to the Internal policies and shall have the same effect as such.

Due to the continuous evolution of technologies, this charter may be subject to changes.

1.2 Scope of Application

This charter applies to the entire SGPM (Societe Generale Personne Morale) perimeter and is likely to constitute a reference framework for the Group's subsidiaries in the implementation of their own use rules. Each User of the Information System or who may hold Societe Generale's Information Assets must comply with it.

1.3 Charter communication mode

Information Assets and Information System protection requires consistent, clear and regular information allowing Users to understand all the conditions of use. This charter is brought to the attention of any User of the Information System or Information Assets of the concerned perimeter.

For third parties (such as service providers, contractors, trainees, …), the charter is communicated to them, if necessary, at the time of the contract signature. The third-party service provider or partner shall communicate the charter to all those of its employees who, exceptionally, are given access by Societe Generale to the Information System or any Information Assets of Societe Generale.

2. Rules for information protection and use of IT Resources

2.1 Respect of Information confidentiality

2.1.1 Information Classification

When using Societe Generale's Information System, the User must apply the general principles:

Confidentiality of the information held, in accordance with Societe Generale's privacy policy.

Respect of bank secrecy.

Personal Data Protection.

Inside Information Protection.

To do this, the User commits to defining and updating the Confidentiality level of the information contained in the documents / messages that they are required to create or modify according to the four-level scale: C0-Public; C1-Restricted; C2-Confidential; C3-Secret and to respect the associated rules of use.

2.1.2 Data protection

The User commits to protecting the Group's Information Assets, in particular by respecting the following rules:

- On Societe Generale's premises, clean your desk and secure your documents and equipment before leaving them unattended (computer lock, session log off, anti-theft cable, locker, etc.).
- Ensure that confidential information is not left in meeting rooms.
- Limit printing and use devices according to the Confidentiality level (garbage can, secure container, shredder, etc.) for their destruction.
- Outside Societe Generale's premises, make sure to use all means of theft prevention (anti-theft cable, hotel safes) and protection of disposed information (computer lock, session log off, privacy filters, etc.), in order to reduce the likelihood of theft of equipment or information.
- Remain vigilant regarding the risk of information disclosure in crowded places (public transportation, elevators, restaurants, etc.) by adopting the strictest discretion regarding one's professional activities.

- Do not participate in telephone meetings in public places.
- Strictly limit confidential paper documents and their circulation outside Societe Generale's premises.
- At home (home working or on-call duty) or in another remote location (example of working from one's premises for a service provider), ensure that confidential or non-public information is not seen, heard or shared with unauthorized third parties who may be present, remain vigilant about the presence of any connected objects (security camera, voice assistants permanently connected etc.), in case of absence, close the work session and protect paper documents from prying eyes.
- Remain vigilant about any unusual request from an unsafe source (phishing, fake president fraud, etc.) and contact your security correspondents in case of doubt.
- Respect the visitor accompanying process in effect in Societe Generale's premises.

2.1.3 Personal Data Protection

The regulations regarding Personal Data protection define the conditions under which the processing of Personal Data may be carried out and the rights of the persons concerned by the processing.

Thus, the User, in the context of their professional activity and the execution of their missions, must act in accordance with these regulations and respect the fundamental rights and freedoms as well as the privacy of individuals. More specifically, the User must ensure that the processing of Personal Data that they may be required to carry out in the context of their professional activity, comply with the data protection policies applicable to their perimeter and the internal policy for the protection of Personal Data.

The User is reminded that Personal Data processed by Societe Generale shall not be communicated or used in any form whatsoever for purposes that are foreign to or contrary to the mission entrusted to them by Societe Generale, for personal purposes or in the context of activities outside the company.

In case of questions regarding the regulations related to Personal Data Protection, the User is invited to contact the data protection experts of their activity perimeter.

Assuming that the User is at the root cause of a Personal Data breach (loss of availability, integrity or confidentiality of Personal Data), they must inform as soon as possible the persons referred to in the procedures in effect within the company so that they can, if necessary, inform the supervisory authorities concerned within the required time, and, if applicable, inform the persons concerned by the data breach.

2.2 General rules for using the Societe Generale's Information System

2.2.1 User Responsibility

Access to Societe Generale's IT Resources is provided to Users for professional purposes and according to business needs. This means that a message sent or received from an IT resource provided to the User is of a professional nature unless used in the context of paragraph 2.2.3 "Private use".

Each User is regularly informed of the applicable rules of the use of the Information System and the protection of Societe Generale's information.

Each User is thus responsible for the use they make of the IT Resources provided to them.

In the event of the deterioration of the equipment and in the absence of any negligence or fault on the part of the User, Societe Generale will bear the cost of the equipment.

The Responsibility of the User will be engaged if they are personally accountable of a non-compliant use. In this regard, authentication and Traces are means to reveal the User's identity.

Failure to respect the defined rules in this Charter may result in the application of disciplinary measures for its author, in an appropriate and proportionate manner, in accordance with the scale of the sanctions provided in the internal code of conduct.

The User must contact their Security Correspondent or their hierarchical superior as soon as they suspect a security breach or a potential attack on the Societe Generale Information System. They are not responsible of alerting the other Users.

2.2.2 Access to Societe Generale's resources

Each User receives individual access rights to the Group's Information Systems through confidential authentication means (confidential codes, smart cards, etc.). This access right cannot, in any way, be transmitted, even temporarily, to a third party without engaging the responsibility of the User. The means of authentication are strictly personal and must only be used for the User's own use. The User is responsible for their confidentiality.

Therefore, the User must in particular:

- Choose confidential codes that comply with Societe Generale's password policy, keep them secret and update them according to the frequency set by Societe Generale.
- commit not to give to unauthorized Users access to information systems, through materials they use,
- Lock its software / system session before leaving Equipment unattended,
- Not use or attempt to use any User account other than one's own or hide one's true identity,
- Not bypass the means of security and monitoring.
- Not use their access right to the Information System for purposes other than those for which the access right has been granted.
- Use the resources of the Information System within the strict framework of its professional activity, defined by its function and within the limits of their attributions or the delegations granted to them.

The User's access right automatically ceases when they leave the company (exit from the workforce or end of contract). It can also be modified during a change of assignment and/or according to business requirements.

The User may be granted Privileged Access Rights to the Information System that they can only exercise for the purpose for which these rights were granted to them. The User must refer to the specific rules issued by Societe Generale concerning the management of Privileged Access Rights.

2.2.3 Private Use

Reasonable private use of the Information System (accessing websites, sending e-mails, file storage, telephony, printing, photocopying, scanning, etc.) is tolerated within the daily needs and family life framework. This tolerance is subject to the respect by the User of the principles set out in this charter.

The private use must be limited, both in duration and frequency and must not have an impact on the User's professional activity.

In the context of a private use of the information systems, the User is required to:

- If they use a file directory, to identify the name of this directory by the keyword "[prv]" or any other clear and unambiguous identifier of the private nature of the information.
- If printing a private document, identify the name of the document by the keyword "[prv]".
- If they issue e-mails or any other form of message (e.g. sms), mention in the subject field the keyword "[prv]" (or at the beginning of the message when the subject field does not exist).
- If they wish to receive e-mails or any other form of messages (e.g. sms), to have the sender mention in the subject line the keyword "[prv]",1 (or at the beginning of the message when the subject field does not exist). Each User must inform their correspondents when communicating their e-mail address on a private basis. These messages will be subject to the same technical inspection procedures as those defined in §3 "Control measures and supervision".

---

[1] Regardless of accents or lowercase/uppercase; will therefore be accepted for example "

[Prv], [pRV], ... »

No information of a professional nature can benefit from the keyword [prv]. As such, it can neither be stored in the file directory "[prv]", nor be printed, photocopied, scanned with the keyword "[prv]", nor be issued or received by the User in e-mails or in any other form of message with the subject "[prv]". Societe Generale reserves the right to block the output of a message or document marked "[prv]" if professional information is detected (see §3 "Control measures and supervision"). Users will then receive an email informing them of the automatic blocking of this sending and may refer to their hierarchy for any request to unblock the sending of said message.

The private use of the Information Systems is the sole and entire responsibility of the User. Societe Generale will not put specific security measures for the protection of private content.

If it turns out that precise and consistent indications prove that the User is engaged in a malicious or abusive use of the keyword "[prv]" or the possibility left to their to use the company's resources for private purposes, Societe Generale will be entitled to draw all the disciplinary and possibly judicial consequences.

The misuse of the "[prv]" tag may be deducted also from the content automated detection, the frequency of messages received or sent, the volume of data exchanged, stored or printed, the attachments and connection duration.

Societe Generale will be able to read the content of messages and private files based on the respect of the regulations in force and in particular the secrecy of correspondence.

2.3 Rules for using professional digital equipment and tools

The tools and User accounts used in the professional context must be those authorized by Societe Generale.

Non-exhaustive list of examples:

File exchanges must be carried out through tools validated by Societe Generale in compliance with confidentiality rules.

Any exchange of messages on sensitive, strategic or commercial subjects must be carried out through tools validated by Societe Generale.

All professional identifiers must be used in a strictly professional context and must not be communicated on websites not authorized by Societe Generale.

A personal (i.e. non-professional) e-mail address must be used to register on external sites (excluding authorized professional activities).

Automatic transfer of business email to personal (i.e. non-business) email is not allowed. The transfer to the professional email of another employee, or to a professional shared email can only be done at the initiative of the employee itself. When the professional context requires it, and if the transfer of the email is not implemented, the employee will have to set their e-mail to send a message designating the person(s) to contact during their absence.

2.3.1 Rules for using Equipment

Whether for Equipment provided by Societe Generale or for Personal Equipment used for professional purposes, the User commits to taking the necessary measures to guarantee the security of professional information and must in particular comply with the following rules:

- Remain vigilant about Equipment Access by third parties.
- Respect the configuration and the basic configuration of the Equipment or the secure solution deployed on the Equipment.
- Perform the required maintenance and updates.
- Notify user support and/or its Security Correspondent in case of a failure, malfunction, alteration, theft, loss or security breach of the terminal.

In addition, with regard to Personal Equipment used for professional purposes, the User also undertakes to comply with the rules concerning the access right described in paragraph 2.1.1 "Information Classification " as well as the confidentiality rules referred to in paragraph 2.1.2 "Data protection".

Certain public, non-mastered or non-approved applications by Societe Generale, may nevertheless be accessible to the User. These applications present risks and may in particular collect information without the User's knowledge such as technical data (device type, OS version, etc.), usage data (date and time of installation, use, etc.), but also certain personal data elements (geolocation, age, preferences, etc.). The use or download of these applications for professional purposes from the Equipment can only be done after having been previously validated by the security teams.

2.3.2 Rules for using the Internet

2.3.2.1 Internet browsing

Societe Generale provides Internet access to all Users of its Information System according to its business needs. Only websites with a direct and necessary link to the professional activity carried out are intended to be consulted. Societe Generale reserves the right to filter site categories by default and block downloads on certain sites. The associated rules and processes are governed by the Internet Browsing Filtering Policy.

The User must be particularly vigilant with regard to the content consulted, downloaded and exchanged on the sites with the Internet access provided by Societe Generale. In particular, it is forbidden to:

- Transmit or publish confidential or non-public Information about Societe Generale, its subsidiaries or more generally about Societe Generale entities, its customers or partners, or its workforce (unless authorized by the hierarchy and protected by adequate validated means).
- View, download, transmit or store content of a pornographic, pedophile, racist, xenophobic or violent or defamatory nature, containing any incitement to hatred, undermining respect for the human person and dignity, inciting the commission of any offence or crime, glorifying terrorism, or any content that is contrary to public order or offensive, or that infringes on Societe Generale's internal or external brand image.
- Commit reprehensible acts with regard to applicable law, in particular with regard to respect for intellectual property rights .
- Participate in gambling.
- Carry out a commercial activity in a private capacity.
- Create or administer Internet or electronic communication services unrelated to the needs of their professional activity.

The downloading of programs is only allowed to persons explicitly authorized. The User must take care not to overload the Societe Generale Information System in an abusive manner, in particular by limiting transfers of large files or access to certain multimedia resources.

2.3.2.2 Social networks and external instant messaging

As part of personal use of social networks and external instant messaging, the User shall refrain from disclosing confidential information about Societe Generale, their professional activity, the roles and responsibilities of their colleagues or their clients and undertakes to follow the communication rules issued by Societe Generale, particularly with regard to respect for banking secrecy. The User must not engage in controversies that pose a risk to the image of Societe Generale.

Furthermore, messages that are offensive, denigrating or likely to infringe on the privacy, image or reputation of employees and the company are prohibited. Societe Generale will be entitled to draw all disciplinary and possibly judicial consequences.

2.3.3 Rules for using messaging and internal communication tools

Societe Generale provides Users of its Information System with a set of means of communication (e-mail, instant messaging, internal communities, etc.).

It is forbidden to transmit, retransmit or publish messages of a defamatory, abusive, denigrating or likely to infringe the privacy of persons, the image, reputation or consideration of persons and messages that would be contrary to the laws in force. Such messages could engage the responsibility of the User and Societe Generale.

The User must not transmit messages such as false alarms or rumors (unverified information likely to mislead someone).

The User must strive to limit the number and size of attachments to avoid overloading the network. they must also use mailing lists with wisely and avoid sending copies to an unjustified number of recipients.

3. Control measures and supervision

Societe Generale reserves the right to monitor the use made of IT Resources and Information Assets, in compliance with the legal framework and the privacy of Users to:

- Ensure the security of the Information System and the Information Asset.
- Ensure compliance with the rules defined in this charter.
- Fulfil the obligations arising from the laws and regulations governing the activities of credit institutions and investment firms.

3.1 Control Measures and Traces

Control measures can thus be put in place in order, for example :

Check the installed software on the workstations provided by Societe Generale, in order to ensure that no malicious software compromises the User's computer.

Verify that the protection mechanisms put in place by Societe Generale on professional and personal Equipment used in the professional context are not deactivated.

Control the content of e-mails or any other form of messages / files / directories / documents that are stored / sent / transferred / printed in the software and equipment provided by Societe Generale in order to ensure the security of the Information System and Information Assets.

Block e-mails that contain documents identified as not being allowed to leave the Group Societe Generale. Users will then receive an email informing them of the automatic blocking of this sending and may refer to their hierarchy for any request to unblock the sending of this email.

Filter the flows exchanged on the Internet.

Block access to unauthorized sites.

More generally, any control measure necessary to preserve the security of Societe Generale's Information System and Information Assets may be implemented.

The functioning of the control measures is the responsibility of the system administrators whose duty of confidentiality is set out in paragraph 3.3 "Duty of confidentiality of system administrators" of this charter.

In compliance with the principles of transparency and proportionality, Users' attention is drawn to the fact that the computer security devices (firewalls, access control systems, etc.) set up by Societe Generale generate Traces of systems that make it possible to identify events (authentication to a session, deletion of files, use of applications, etc.). These Traces can then be correlated amongst one another to investigate the causes of an event that has or could potentially impact the security of Information Assets and Information Systems.

The Traces collected by Societe Generale include the following information (non-exhaustive list):

Sent or received messages:

- All the resources accessed by the User through Internet with details such as the technical connection parameters (including the User account ID, date and time, volume of data transmitted...).
- User authentications access to IT Resources with details such as the date and time of access.
- List of technical parameters necessary for the management of e-mail services (User account identification, recipient's contact details, date and time, volume, format and nature of attachments, etc.).

Traces may be retained in accordance with the relevant internal policies and applicable regulations.

3.2 Exploitation of the Traces

For operational purposes, a statistical exploitation of the Traces is carried out, in anonymous way. It consists, in particular, of establishing statistics on the connections and contacts made.

Nevertheless, Societe Generale may carry out nominative audits on the Enterprise Traces, following a malfunction, a security alert or the presumption of non-compliant use of IT Resources, while respecting the secrecy of private correspondence referred to in paragraph 3.3 "Duty of confidentiality of system administrators".

In this case, the material findings are intended to identify the various circumstances that will enlighten Societe Generale on the possible realization of a non-compliant use and on the identity of its author.

3.3 System Administrators' Duty of Confidentiality

System administrators ensure the normal operation and networks and systems security.

Consequently, by their very functions, they can have access to all the information related to Users.

They are bound by a duty of confidentiality and must respect the processes and rules related to their activity.

In this context, the Administrators must not disclose these information when it is covered by the secrecy of private correspondence or falls within the privacy of Users and does not question the proper application technical operation, nor the security, nor the interest of the company.

3.4 Technical and administrative measures

For technical or administrative purpose, access to IT resources may be suspended, restricted or deleted, individually or collectively when necessary, in particular in order to maintain the availability or integrity of Societe Generale 's Information System and the protection of Societe Generale ;s Information Assets.

Glossary

Confidential Information: all information which may only be communicated to Users on a need-to-know basis, and the disclosure of which would have a high-level impact for the Group, its entities or the person or people concerned. Inside information is included at least in this level of classification.

Equipment: All equipment made available to the User by Societe Generale or personal equipment used for professional purposes (workstations, phones, tablets, etc.).

Group: Refers to the group formed by Societe Generale Legal Person and its subsidiaries.

Information Assets: Represents all the information and/or knowledge held by the Group (including customer information, personal data, etc.).

Information System: All the elements of Societe Generale that contribute to the creation, processing, circulation and preservation of information in the company (database, application software, procedures, documentation, etc.), including the computer system itself (central processing unit, peripherals, operating system, etc.).

Inside Information: Information of a precise nature which has not been made public relating, directly or indirectly, to issuers or Financial Instruments listed on Organised Markets within the European Economic Area (EEA), and, if made public, would be likely to have a significant effect on the prices of those Financial Instruments or on the price of related derivative Financial Instruments.

Instant messaging: Application allowing the instant exchange of messages and files between several people.

Internal community: Group of employees forming a virtual community on the communication tools set up by Societe Generale.

IT resources: Refers to all of Societe Generale's hardware (workstations, smartphones, tablets, printers, video surveillance cameras, etc.) and software (collaborative tools, applications, etc.) that allow the User to process information in a digital, analog or paper format.

Malware: software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system such as virus, worms, Trojan horses or any other code or instruction. This software can be used to:

Infect or affect any program, software, data, file, database, computer or other hardware or component.

Damage, compromise integrity or confidentiality, disrupting in whole or in part the operation.

Hijack or allow to hijack whole or part of the Information System from the use for which it is intended to.

Personal data: Any data or information relating, directly or indirectly, to identified or id

Appendix A.4: Template of work accident notification

DEPARTMENT	DATE OF ACCIDENT	PLACE OF ACCIDENT	JOURNEY / WORK	CIRCUMSTANCES OF THE ACCIDENT	LOCATION OF INJURY	NATURE OF INJURY	WA SEEN / INF	SICK LEAVE YES / NO

Appendix A.5: Business rules for receiving invoices

The following information must be specified:

ENTITY OF THE SOCIETE GENERALE GROUP	Entity that must be charged, as indicated to you (on the purchase order or by your customer contact).
NUMBER OF THE INVOICE or CREDIT NOTE	Must not include special characters or spaces and must be in upper case letters with a maximum of 30 characters.
DATE OF THE INVOICE or CREDIT NOTE	Must not be later than the current date.
NUMBER OF THE ORDER	It is mandatory. It is the reference number of the purchase order sent through SAP ARIBA. It includes 8 alphanumeric characters.
INVOICE INFORMATION	Quantity, price, VAT, etc.
VAT SCHEME	Charged or paid.

The following information is mandatory in some cases:

IT CONSULTANTS' SERVICES (PII)	MEN OF LAW
PERIOD CODE	REFERENCE OF THE COLLECTION CASE (P@TRIC CODE)
Is mandatory, in addition to the number of the order, only for contracts starting by 'ATU', 'ATG' or 'FOR'. The period code includes 2 letters ('AS', 'ST', 'DE') followed by 2	Is mandatory only for Men of Law providers. The P@tric code must be entered in the "case number" field in the drop-down list of non-required

digits corresponding to the month and 2 digits corresponding to the year of the assignment.	fields in the header of the invoice /credit note.

Appendix A.6: Good practices related to the usage of privileged accounts

For each employee having a privileged account on this workstation (physical or virtual)

A privileged account on your workstation has been provided to you as a part of your activities. Having access to a privileged account is a security exception.

Good practices

- Only install applications from a trusted origin (editor website must be preferred), with no malicious or illegal purposes;
- Ensure that the application you want to install is not already available in the application inventory tool. Additionally, ensure to comply with license issues;
- Keep the application up-to-date, and perform the update as soon as the editor make the update available;
- Only ask for a privileged account when this usage is strictly needed, and not systematically;
- When you are defining a password, ensure that the password comply with Societe Generale password policy.
- Do not give to anyone your admin credentials to anyone;
- Do not stock your password in plain text on a physical (e.g. post-It) or logical (e.g. text file) support.
- Following a mobility/departure/long term absence, if the password of a generic/service account is known to the user, it must be changed.

Those actions are prohibited:

- Create or move a user to the Administrator group;
- Edit the other groups;
- Edit System privileges or Groups used by services;
- Edit or remove security parameters of the workstation;
- Edit or alter the features of security tools;
- Edit the configuration of your workstation for any purpose without the express written permission of the support and your CISO (Chief Information Security Officer, go/secu for more details);
- Install a program (tool, software, freeware, …) without the express written permission of your manager.

Each employee having a privileged account to work on this workstation (physical or virtual), shall respect the rules listed above.

Moreover, each person concerned by this document must act under the legislation, the national law, rules, procedures within Societe Generale and good practices related to his activity.

APPENDIX B « SOFTWARE »

1 - DEFINITIONS

Anomalies are classified into three (3) categories. In the event of a disagreement between the Parties regarding the qualification of the degree of severity of the Anomaly, the Beneficiary's qualification shall prevail.

- **Blocking Anomaly**: means an Anomaly rendering the use of the product or service impossible, in whole or in part, impossible or the use or test of an essential function of the product or service ; or giving rise to limitations or restrictions in the use of the product or service rendering an essential function of the product or service unusable in production; or giving rise to limitations or restrictions in the testing of the product or service, rendering an essential function of the product or service untestable. The Anomaly must be corrected by the Service Provider within (twenty-four) 24 hours or within the period specified in the Application Contract, as the case may be.
- **Serious Anomaly**: means an Anomaly giving rise to limitations or restrictions in the use of the product or service or in the testing of the product or service without these limitations or restrictions being sufficient for the Anomaly to be qualified as a Blocking Anomaly. The Anomaly shall be corrected by the Service Provider within a period of seventy-two (72) hours or within the timeframe specified in the Application Contract as the case may be.
- **Minor Anomaly**: means any Anomaly which is not considered as a Blocking Anomaly or a Serious Anomaly. The Anomaly shall be corrected by the Service Provider within a period of five (5) Working Days or within the timeframe specified in the Application Contract as the case may be

Evolution: designates a major, independent version of the Product Software. . Evolutions will be indicated by the evolution of the first decimal of the Software Version (v X.1).

Maintenance : Refers to all support, assistance and maintenance services provided by the Service Provider aiming at correcting and improving the Product Software and enabling the Beneficiary to use the Product Software in compliance with the Contract. The Maintenance terms and conditions are described in the Application Contract.

Updates: means successive formulations of the same Version, following corrections, adaptations or minor enhancements.

System : refers to the combination of equipment, operating system and operating or network infrastructure, implemented by the Beneficiary or their subcontractors in order to use the Product Software.

Users: Refers to any physical person belonging or not to the Group, authorized by the Beneficiary to use the Product Software within the limits of the number of Licenses purchased in the Application Contract. Employees whose employment contract has terminated/expired or any contractors/consultants whose contractual relationship with the Beneficiary is no longer in force will no longer be considered as Users.

The Service Provider expressly authorizes access to and use of the Product Software by all third-parties acting on behalf of the Beneficiary and under his responsibility, regardless of the capacity in which this third party intervenes.

Version(s): refers to the set of all the functional and technical characteristics of the Product Software. . Versions include updates and upgrades.

2 - PURPOSE

The purpose of this Appendix is to define the specific terms and conditions applicable to the Parties when the purpose of the Application Contract is to license a Product Software and purchase associated Maintenance services.

The License will be granted and the Maintenance services will be performed in accordance with the provisions of the Contract.

3 - DELIVERY AND ACCEPTANCE OF THE PRODUCT SOFTWARE

When the Product Software is delivered, the Service Provider supplies Documentation in paper and electronic form, at no extra charge. This Documentation describes the specifications, the installation process and the help for using the Product Software. The Service Provider authorizes the Beneficiary to reproduce the Documentation without modification and in any number.

The Service Provider undertakes to deliver the Product Software and Documentation in accordance with the deadlines otherwise agreed between the Parties and, failing this, within ten (10) Working Days from the date of signature of the Application Contract. The delivery medium for the Product Software is included in the price of the Product Software.

The Service Provider will contact the Beneficiary prior to delivery to discuss the precise terms of delivery.

The Product Software and Documentation are subject to a delivery check by the Beneficiary to ensure that all the elements ordered are present.

If, at the end of a period of twenty (20) Working Days following delivery of these elements, the Beneficiary :

- Has not expressed any reservations, the Beneficiary signs two (2) copies of the delivery report, which triggers the phase of verification of correct operation and conformity.
- Upon notification of documented reservations specifying the missing elements, the Service Provider is obliged to dispatch the missing elements within five (5) Working Days. On receipt of all missing elements, the Beneficiary signs the delivery report in two (2) copies, which triggers the verification of correct operation and conformity phase.

4 - INSTALLATION AND VERIFICATION OF PROPER FUNCTIONNING

4.1 Installation of the Product Software

After delivery, the Service Provider installs the Product Software if this has been agreed between the Parties.

4.2 Verification of the Product Software's proper functioning and compliance

As part of the verification of the correct functioning and conformity of the Product Software, the Beneficiary carries out the test sets it wishes.

If, at the end of this verification period, the Beneficiary :

- Has not expressed any reservations, it is deemed to have a Product Software that complies with the functionalities contained in the Documentation and in the description of the Product Software provided in appendix of the Application Contract. The Beneficiary signs the report on the verification of correct functioning and conformity or notifies the Service Provider in writing of the absence of reservations.
- Having notified the Service Provider in writing of any reasoned reservations, the Service Provider is obliged to bring the Product Software into compliance within a maximum of ten (10) Working Days, or if this is not possible, to implement a temporary alternative solution before definitive compliance within a maximum of five (5) Working Days.

Once any reservations have been remedied, the Beneficiary signs the report on the verification of correct functioning and conformity, or notifies the Service Provider by any written means, marking the start of the warranty period.

5 - DELIVERY AND ACCEPTANCE OF THE ELEMENTS SUPPLIED UNDER MAINTENANCE SERVICES

5.1 Delivery of Elements supplied under Maintenance services

Upon delivery of each Element, the Service Provider supplies Documentation, in paper and electronic form, at no extra charge.

Each delivery is subject to verification by the Beneficiary of the presence of all Elements. This verification takes a maximum of ten (10) working days.

In the event of incomplete delivery, the Service Provider undertakes to deliver the missing Elements within a maximum of five (5) Working Days. The Beneficiary shall notify his acceptance of delivery in writing by any written means or by signing a delivery report.

5.2 Installation of the Elements supplied under Maintenance services

When agreed between the Parties, after delivery, the Service Provider installs the Elements and verifies the correct operation and conformity of these Elements in relation to the functionalities contained in the Documentation and in the specifications, within a maximum period of ten (10) Working Days from the date of written notification of acceptance of delivery by the Beneficiary.

5.3 Verification of correct functioning and conformity of Elements supplied under Maintenance services

As part of the verification of correct functioning and conformity of the Elements supplied by the Service Provider, the Beneficiary runs the test sets he wishes. If, at the end of this period of verification of correct functioning and conformity, the Beneficiary :

- has not expressed any reservations, he is deemed to have Elements that comply with the functionalities contained in the Documentation and in the specifications. The Beneficiary signs the verification report or notifies the Service Provider in writing.
- If the Beneficiary has notified the Service Provider in writing of any justified reservations, the Service Provider is obliged to remedy the situation within a maximum of five (5) Working Days.

Once the reservations have been resolved, the Service Provider and the Beneficiary sign the report on the verification of correct functioning and compliance, or notify the Service Provider by any written means.

6 - SERVICE PROVIDER'S MAINTENANCE OBLIGATIONS

The Service Provider is bound by an obligation of performance with regard to :

- Carrying out Maintenance services in accordance with the provisions of the Contract, and in particular resolving Anomalies as quickly as possible, or within the timescales agreed between the Parties.
- Carrying out upgrades to the Product Software resulting from legal or regulatory changes, within a timeframe compatible with the entry into force of such changes,
- The implementation of Product Software upgrades related to System upgrades.

The Service Provider will ensure the maintenance of the Product Software on the System and will take into account any changes to the System imposed in a global manner by the constructors or editors having supplied the component parts in such a way that the Product Software remains compatible with the System.

It is understood that the Beneficiary reserves the right to accept, refuse or delay the installation of the Elements.

In the event of activation of a Maintenance service (e.g. 24x7) involving transfers of Personal Data outside the EU, the Service Provider undertakes to sign the standard contractual clauses, under the conditions defined in the “Personal Data” article of the General Terms and Conditions.

7 - RIGHTS OF USE

The Service Provider declares and warrants that it is the author or entitled party of the author of the Product Software in accordance with the provisions of the French Intellectual Property Code.

The Service Provider grants the Beneficiary a non-exclusive right to use the Product Software, exclusively for the needs of the Users, within the scope of their activity and under the conditions set out in the Contract.

The right to use the Product Software is granted :

- for the entire world or for the territory specified in the Application Contract, as the case may be, and ;
- for the duration of protection currently granted or to be granted in the future to authors, by French laws and regulations and by international conventions, or for a limited period specified in the Application Contract, as the case may be.

The Beneficiary is entitled to make a back-up copy of the Product Software to ensure operational security. It is expressly agreed that the Beneficiary may transfer the Product Software to a system or site other than the Beneficiary's system or site, at no additional cost, subject to prior notification to the Service Provider.

The Service Provider expressly authorizes access to and use of the Product Software by any third-party acting on behalf of and under the responsibility of the Beneficiary, irrespective of the capacity in which such third-party acts.

8 - DECLARATION OF USE

Should the Beneficiary be required to make and send to the Service Provider a declaration of use of the Product Software, the Parties will agree in advance on the relevant terms and conditions, and in particular :

- the tool to be used by the Beneficiary to produce this declaration ;
- the format ;
- the content;
- the frequency of sending to the Service Provider.

In the event of a discrepancy between actual usage and the usage defined in the Contract, the Beneficiary undertakes to rectify the situation, under the conditions defined in the “Financial Conditions” appendix to the Application Contract, within a period agreed between the Parties.

9 - SOURCES CODE DEPOSIT

In the event that the Service Provider grants the Beneficiary a license for the duration of copyright protection (known as a “perpetual” license), the Service Provider certifies that the Product Software's source codes are deposited under its name with a trusted third party, and undertakes to maintain them there and to deposit any modifications, in particular updates and new Versions, free of charge, for the duration of the Contract.

The cases in which the Beneficiary may request free access to the Product Software source codes from the depository company are as follows:

- judicial liquidation or cessation of activity of the Service Provider and not taken over by a third party,
- back-up in the event of partial cessation of the Service Provider's business, including the Product Software ,
- cessation of Maintenance services not taken over by a third party.

The Beneficiary may only use the source codes for the exclusive purpose of maintaining the Product Software. This measure, if it occurs, does not confer on the Beneficiary any new intellectual property rights on the Product Software.

This article shall survive the termination or expiration of the Contract for any reason whatsoever.

10 - SERVICE PROVIDER AUDIT RIGHTS

The Service Provider may, at its own expense and no more than once a year during the term of the Contract, have an audit carried out to enable it to verify the Beneficiary's compliance with the Licenses.

This audit may be carried out either by an employee of the Service Provider, or by any third party chosen by the Service Provider in agreement with the Beneficiary and subject to a confidentiality agreement.

A method agreement will define the audit conditions agreed by the Parties. It is specified that the audit may only cover Licenses used during the two years preceding notification of the audit.

The Beneficiary undertakes to assist the auditors appointed by the Service Provider for this purpose, and to provide the Service Provider with the information required to carry out the audit, it being understood that the audit assignment may not disrupt the Beneficiary's business.

Within thirty (30) days of notification by the Service Provider, the Beneficiary must provide the auditor with access to its premises during normal business hours.

The conclusions of the audit will be communicated to the Beneficiary, who will then have a period of thirty (30) days in which to express his observations and reservations.

In the event that the conclusions of the audit show that the Beneficiary is not complying with the conditions of use of the Licenses set out in the Contract, unless the Beneficiary has legitimate reservations about the conclusions of the audit, the Beneficiary must pay the Service Provider, by way of license adjustment, a sum equal to the amount that should have been paid to the Service Provider for compliant use, by applying the contractual rate in force as defined in the “Financial Conditions” appendix to the Application Contract. Payment will be made within forty-five (45) days from the end of the month in which the invoice is sent by the Service Provider.

APPENDIX C « SAAS »

1 - DEFINITIONS

Users : Refers to any natural person, whether or not belonging to the Societe Generale Group, authorized by the Beneficiary to use the product or service covered by the Contract within the limit of the number of Licenses acquired, where applicable, under the Application Contract. Employees whose employment contract is terminated/expired or contractors/consultants whose contractual relationship with a Societe Generale Group entity is no longer in force will no longer be counted as Users.

2 - PURPOSE

The purpose of this Appendix is to define the specific conditions applicable to the Parties when the purpose of the Application Contract is to purchase a Hosted Service.

3 - APPROVAL OF THE HOSTED SERVICE AND RELATED SERVICES

Once the Hosted Service has been made available to the Beneficiary and/or any Associated Services have been delivered to the Beneficiary, an acceptance report will be drawn up and signed. In the event that the Hosted Service and/or Associated Services are not delivered in conformity, the Beneficiary may terminate the Contract ipso jure, without delay or compensation, following notification to the Service Provider of the non-conformity of the services.

4 - RIGHTS OF USE OF THE HOSTED SERVICE

The Beneficiary and Users are authorized to use the Hosted Service in accordance with its intended purpose, for the duration of the Contract, for the needs of the Beneficiary's and/or Users' business, wherever in the world they may be connected to this service, in accordance with applicable law.

The Beneficiary undertakes not to (i) resell, sub-license, rent, share, or make the Hosted Service available to any unauthorized third party in any way, with the exception of entities of the Beneficiary's Group and subject to any stipulation to the contrary in the Contract; (ii) illegally access, disrupt the integrity or performance of the Hosted Service or the data it contains; (iii) reverse engineer the Hosted Service.

The Service Provider expressly authorizes any third party acting on behalf of and under the sole responsibility of the Beneficiary to access and use the Hosted Service for the purposes of the Beneficiary's business, provided that such third party is not a direct competitor of the Service Provider in the same type of services.

The Beneficiary is responsible for the use of the Hosted Service by its Users or any authorized third party acting on the Beneficiary's behalf, using the identifiers provided by the Service Provider, and undertakes to ensure that Users comply with the provisions of the Contract.

5 - SECURITY - DETECTION, INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

This Article supplements the stipulations of the “Security” Article of the General Terms and Conditions.

The Service Provider undertakes to propose the implementation of a security incident management protocol describing the incident detection and response process, as well as the alert and crisis

management processes. The implementation of this protocol, and any changes to it, will require the prior agreement of the Beneficiary.

These processes will include in particular :

- monitoring by the Service Provider of its Information System in order to detect security events and trigger an alert in the event of a security incident;
- maintaining a security incident management procedure to analyze, classify, contain and react to such events.

The Service Provider also undertakes to implement a Business Continuity Plan that is sufficiently dimensioned to meet its obligations under the Contract, guaranteeing the effective continuity of the Products and Services to be provided, taking into account all risk scenarios and in particular any climatic or environmental risks depending on the location where the Products and Services are provided. The Service Provider shall communicate the Business Continuity Plan to the Beneficiary upon first request.

6 - HOSTED SERVICE AVAILABILITY

Unless otherwise specified in the Application Contract, it is understood that the Hosted Service availability rate will be a minimum of 98% per contract year.

7 - TRANSFERABILITY

As the Service Provider has control over operating the services provided to the Beneficiary, it undertakes, in the event of termination of the Contract, for any reason whatsoever, including in the event of the Service Provider's insolvency, winding-up or cessation of business, to ensure transferability of the service in order to allow the Beneficiary or service provider chosen by the Beneficiary, to take over the execution of the services, and all elements that may have been supplied to the Services Provider within the framework of the services, without interruption and in optimal conditions. As such, the Service Provider notably undertakes to ensure the data portability in a structured and commonly used format.

Additionally, the Service Provider will implement the Services described in the appendix "Transferability Plan" appended to the Application Contract, where applicable, and undertakes to restore to the Beneficiary, within a maximum time-frame of ten (10) days, before the date of the end of the Contract if this is known, in the event of early termination, all Beneficiary data in a format that conforms to market standards and in order to guarantee its integrity, and any programs, hardware or other software made available by the Service Provider to the Beneficiary within the framework of the Contract. At the Beneficiary's request, the Parties may review the Transferability Plan in order to ensure that it is still suitable for the Products and Services and discuss its content again if necessary.

The Service provider finally undertakes to ensure the irreversible destruction of the Beneficiary's information which would have passed to the Service Provider, in the conditions defined in the appendix "Transferability Plan".

At the Beneficiary's request, assistance services may be supplied by the Service Provider to reload Beneficiary data extracted from the Products and Services onto the system chosen by the Beneficiary, subject to a cost estimate accepted and signed by the Beneficiary.

8 - TECHNICAL SECURITY AUDITS

This Article supplements the provisions of Article "Audit and control by the Beneficiary" of the General Terms and Conditions.

The Service Provider authorises to conduct security audits (including scanning, vulnerability automated testing, penetration tests, infrastructure and configuration audits) on its systems and with any subcontractors that may be involved or affected, including specifically companies hosting the whole or part of the Service Provider's system, once a year or following any incident having impacted the service provided to the Beneficiary.

Evidence of audits carried out on its systems or on subcontractors systems by the Service Provider must be communicated under the format of a summary report to the Beneficiary.

The Auditor will be allowed to conduct security audits. These audits will consist in conducting a set of technical and/or organisational tests, automated or manual, on the Service Provider's IT system or the IT system of any subcontractor involved in the provision of the Services. These audits may include:

- Vulnerability Scanning (infrastructure & applicative),
- Source code reviews,
- Configuration audits,
- Penetration tests,
- Organisational audits,
- Thread led penetration testings (as defined by EU 2022/2554 Digital Operational Resilience Act). The Service Provider commits to participate and fully cooperate in the TLPT carried out by the financial entity.

In order to review and examinate a system's records and activities, to determine the adequacy of system controls, to ensure compliance with established security policy and procedures, to detect breaches in security services, and to recommend any changes that would be indicated for countermeasures, the Service Provider warrants that it holds the necessary and sufficient rights and authorisations to conduct the aforementioned security audits on the IT system and with all subcontractors that may be involved or affected.

These security audits shall be the subject of prior notification to the Service Provider.

It is understood that the purpose of these security audits is not for the Beneficiary to access data belonging to other clients of the Service Provider but to verify the security of the system and the infrastructure used to provide the Services.

Security audits shall be subject to the signing of a prior agreement between the Parties under the terms laid out in Appendix "Agreement for conducting a technical security audit".

APPENDIX "TEMPLATE AGREEMENT FOR CONDUCTING A TECHNICAL SECURITY AUDIT"

This agreement is concluded on [date], between Societe Generale ("the Beneficiary") and the company <_SUPPLIER_COMPANY_NAME/>.

The Beneficiary wants to perform a technical security audit of the IT architecture of the company <_SUPPLIER_COMPANY_NAME/>.

The Parties agree:

1.Vulnerability and penetration tests

Under this agreement, <_SUPPLIER_COMPANY_NAME/> expressly authorises the Beneficiary to carry out vulnerability testing and scanning on the IT system used by <_SUPPLIER_COMPANY_NAME/>.

Vulnerability testing shall be nondestructive.

Vulnerability testing will be carried out on the IP addresses communicated by <_SUPPLIER_COMPANY_NAME/>.

The company <_SUPPLIER_COMPANY_NAME/> warrants that it holds all the necessary rights and authorizations to conduct those tests on the computers corresponding to these IP addresses.

Vulnerability testing and scanning will be carried out by the Beneficiary or its subcontractors on [SPECIFY DATE].

The company <_SUPPLIER_COMPANY_NAME/> must make the tested IT systems available on the dates indicated so that vulnerability testing can be carried out.

The Beneficiary will remain available during vulnerability testing and agrees to immediately put an end to the tests when receiving notification from the company <_SUPPLIER_COMPANY_NAME/>.

2.Confidentiality

The Parties agree to:

- keep the other party's sensitive data and information which might be accessed during vulnerability testing strictly confidential, refrain from transmitting the aforementioned information or make it available to third parties and use it for the sole purpose of implementing the agreement.
- Refrain from using the information, directly or indirectly, or allowing it to be used by a third party, for purposes other than the proper performance of the agreement.
- Use all necessary endeavours to ensure that confidential information is stored separately from the other documents and protected against unauthorized access.

Beneficiary

Name:

Function:

Signature: _____ Date: _____

<_SUPPLIER_COMPANY_NAME/>

Name:

Function:

Signature: _____ Date: _____

APPENDIX D « PRODUCTS »

1 - DEFINITIONS

Delivery receipt : Refers to the receipt, at the time of delivery of the Product, which confirms that the packages delivered are (or are not) in apparent perfect condition, that the delivery is (or is not) complete, and that the deadlines have (or have not) been met.

Defect: Refers to any non-conformity of the Product in relation to its description.

Software : means, for the purposes of this Appendix, all computer programs and procedures enabling the execution of a function or task, as well as its associated documentation, necessary for the use and proper operation of the Product. The term Software also includes updates and new versions.

Final Acceptance Report: means the report used to establish the conformity and proper functioning of the Product with regard to the specifications and performances defined in the "Description of Products and Services" appendix to the Application Contract.

Site: means the site to which the Products and/or Associated Services are to be delivered.

2 - PURPOSE

The purpose of this Appendix is to define the specific conditions applicable to the Parties when the purpose of the Application Contract is to purchase Products and, where applicable, Associated Services.

3 - DESCRIPTION OF PRODUCT SUPPLY TERMS

As part of the supply of Products, the Service Provider will set up a sales organization and services to meet the Beneficiary's expectations. The main elements are described in the following paragraphs.

The supply of the Product is divided into three parts:

- transport,
- delivery
- reception.

The final stage in the supply of the Product is the final acceptance phase.

3.1 Transport of the Product

Transport is the sole responsibility of the Service Provider, who undertakes to deliver the Product to the Site designated in the Application Contract. The Beneficiary undertakes to accept the Product in accordance with the provisions of the Contract.

The Service Provider waives its right to invoke, in respect of the Beneficiary, any exceptions or limits of liability which may be raised against it by the carrier, the Service Provider remaining in all cases solely liable in respect of the Beneficiary.

3.2 Product delivery terms

The Product will be delivered with its existing Documentation (instructions for use, routine maintenance and installation) including, where applicable, that relating to Software and integrated components.

The Product will be delivered in packaging on which the identity of the recipient of the Products will be clearly indicated.

The applicable delivery times are those defined in the Application Contract.

3.3 Receipt of the Product

The Service Provider will present the Beneficiary with the Delivery receipt. The Beneficiary must then check that the packages delivered are (or are not) in perfect apparent condition, that the delivery is (or is not) complete, and that the deadlines have (or have not) been met.

To this end, the Beneficiary will sign the Delivery receipt. Any reservations concerning the delivery must be notified immediately in writing on the Delivery receipt.

In the event of incomplete delivery, the Beneficiary reserves the right to accept (or not) partial delivery.

It is understood between the Parties that any incomplete delivery will be considered as a delay in delivery, insofar as an undelivered part remains beyond the agreed deadline.

Failure to meet the deadlines specified in the present article shall automatically give rise to the application of the penalties provided for in the Contract, where applicable.

3.4 Product verification and acceptance

- Verification

Once the Delivery receipt has been signed, the Beneficiary shall check the Product. The Service Provider may, if the Beneficiary so requests, assist him in this process. The purpose of these verification operations is to enable the Beneficiary to ensure :

- that the Product complies with the specifications and performances defined in the appendix to the Application Contract, and that the Product is free of any Defects;
- that the Product functions in accordance with its associated Documentation.

If the Beneficiary detects a non-conformity or a Defect in relation to the above criteria, the Beneficiary shall draw up, within a maximum period of fifteen (15) days from the signing of the Delivery receipt, a reservation document which he shall send to the Service Provider, summarizing the corresponding reservations.

On receipt, the Service Provider undertakes to bring the Product into conformity with the aforementioned criteria:

- either by correcting the Defects within a maximum of ten (10) Working Days, from receipt of the reservations made by the Beneficiary;
- or by exchanging the Product within a maximum of ten (10) Working Days from receipt of the reservations expressed by the Beneficiary.

Failure by the Service Provider to meet these deadlines may result in the application of the late delivery penalties described in the Contract, where applicable.

- Final Acceptance (Final Acceptance Report)

On completion of the verification operations, the Beneficiary will issue a Final Acceptance Report, which will be signed by the Parties if the Product passes the said operations.

This Final Acceptance Report certifies :

- that the Product conforms to the specifications and performance defined in the Contract;
- the correct operation of the Product;
- compliance with delivery deadlines.

3.5 Service quality commitment

The Service Provider undertakes to provide a quality of service associated with the supply of the Product.

Service quality indicators, defined where applicable in an appendix to the Application Contract, relate in particular to :

- on-time delivery ;
- compliance with lead times for Associated Services (e.g. product installation, user training, etc.);
- meeting deadlines for resolving Defects during the warranty period.

In the event of non-compliance with these commitments, penalties as provided for in the Contract may apply, where applicable.

4 - RIGHT TO USE THE SOFTWARE INTEGRATED INTO THE PRODUCT

Where the Product is sold equipped with operating systems or any other Software required for its operation, the Service Provider must ensure that the relevant editor's user license is supplied to the Beneficiary with the Product.

In this respect, the Service Provider declares that it is duly authorized to grant the non-exclusive user licenses granted by the editors concerned.

This license will be effective both in France and abroad, and for the entire legal duration of copyright protection in force.

It is understood that this clause will remain in force on termination of the Contract, whatever the cause.

5 - TRANSFER OF OWNERSHIP AND RISK

The Service Provider remains the owner of the Product until full payment has been received.

Consequently, before payment has been made, the Beneficiary may not assign, sublet, lend or give as security the Product which is the subject of the Contract.

However, the transfer of risks will take place as soon as the Beneficiary signs the Delivery receipt.