This document sets out the general terms and conditions for the contracting of suppliers by Banco de Sabadell, S.A. (hereinafter, the Bank) of future products and services negotiated and awarded through the Bank's Purchasing Portal. The acceptance of this document by the supplier interested in providing products and services (hereinafter, the Supplier) entails:

a. That they have read and understood the terms included herein.
b. That they are a company with sufficient capacity to provide such products and services.
c. That they have the capacity to undertake, and that they undertake, all obligations described herein.

The validity period of these terms and conditions shall commence on the day on which they are accepted by the Supplier, and shall end on the day on which the corresponding contract for the provision of service(s) awarded through the bidding process conducted through the Bank's Purchasing Portal is signed. This contract shall replace these terms and conditions, and its signature shall be mandatory for all parties on the date on which the Supplier is requested by the Bank to sign the contract following the award of the service, and to ensure the efficiency of this award.

In the event of any discrepancies between the clauses set forth in these General Outsourcing Terms and Conditions and those set forth in the corresponding specific contract for the provision of services or the Details of the award of the service replacing such contract, the clauses specifically set forth in the Specific Contract or Details of the Award shall prevail.

The initiation by the Supplier of the provision of the service awarded to it by the Bank shall imply their full confirmation and acceptance of these terms and conditions.

The Bank reserves the right to unilaterally amend these terms and conditions, and such amendments shall not affect any goods or services acquired prior to such amendments.

General terms and conditions

The SUPPLIER undertakes to:

1. Have the necessary authorisations, licences and administrative permits, as well as any certificates that enable them to conduct their activity, pursuant to the legislation in force at any given time.

2. Provide services through persons with suitable professional qualifications; effectively organise, control and manage tasks of their employees assigned to this service in order to provide a fully satisfactory service.

3. Use documents, materials, technical means and facilities put at their disposal (where applicable) with due diligence, correctly maintain them and refrain from using them for any purpose other than the provision of the service.

4. Keep all certifications, identifications and passwords required for the performance of their activities, without distributing or disclosing them to third parties. The SUPPLIER shall be obligated to return these, whether in physical or electronic format, once the service has been provided. The SUPPLIER acknowledges that any activity conducted using such certifications, identifications and passwords provided by the BANK shall be deemed to have been conducted by the former.

5. Restrict access to all information of which they have knowledge by virtue of the service to be provided to authorised personnel who require knowledge of such information in order to provide these services.

6. Ensure that their employees do not access computers, computer files or other sources of information owned by the BANK, if access to such items has not been expressly permitted.

7. Respect industrial and intellectual property rights, patents, the rights of brands and any other rights of the Owner of software and confidential information derived therefrom.

8. Obtain consent from their employees to disclose their personal data to the BANK for the development, control and management of the service, and such details may be included in files created for this purpose, therefore the security measures and procedures set forth by the BANK shall apply.

9. Strictly comply with any and all obligations as regards Social Security and other fiscal and employment obligations that could be generated by their personnel.

10. Keep up to date with payments of social security contributions for all personnel involved in the service being provided, expressly stated herein for the purpose of the provisions of Article 42 of the Spanish Workers' Statute, and undertakes to submit a copy to the BANK, prior to the commencement of the provision of the service, of the printout of the RED System (internet service for the exchange of information and documents between users and the Spanish social security general treasury) with the digital fingerprint of their association or registration on the Social Security system for each of their workers involved in the service being provided. The SUPPLIER also undertakes, for the duration of this contract and within a maximum of 15 days from the date of expiry of the period for voluntary payment of charges, to have the printout from the RED System with a digital fingerprint as a justification of payment of each fee accrued by the aforementioned employees.

11. Comply with the principles, rules of conduct, policies, prevention model and obligations provided for in the clause on "Sustainability, rules of conduct and model for compliance and prevention of corporate crime, money laundering, terrorist financing and corruption". It is expressly stated that the BANK considers fulfilment of this obligation to be fundamental and essential for the purposes of the due provision of the services to which this contract relates and for the continuation of the relationship established on the basis of this contract. The BANK reserves the right to conduct, either directly or through third parties, reviews to guarantee compliance with the aforesaid principles, rules of conduct, policies, etc., granting access to the necessary documentation and means to that end.

12. The SUPPLIER accepts the obligation to keep updated, for the duration of the provision of services, a general civil liability policy with a fully solvent insurance firm of recognised prestige, for an amount not less than €600,000 (SIX HUNDRED thousand euros).
    The SUPPLIER shall submit to the BANK a copy of its current insurance policy and a certificate from the insurance firm in line with the policy confirming that it is up to date with its insurance premium payments at the beginning of the provision of the corresponding service and every year during the provision of such service.

13. Inasmuch as the SUPPLIER is an obliged person in relation to Anti-Money Laundering and Counter-Terrorist Financing, and to the extent that the activities performed include one of the functions performed by said obliged person, the SUPPLIER hereby takes on the obligation to comply, in its capacity as an obliged person, with legislation on anti-money laundering and counter-terrorist financing. This compliance obligation must be accredited before the BANK if required to do so.

Control and supervision

The BANK may supervise and control the activities of the SUPPLIER as a consequence of this contract, and to this end may:

- Require from the SUPPLIER and/or its subcontractors, at any time, all information about the activity carried out.

- Where the service is to be provided outside the premises of the BANK, the latter may periodically inspect, either directly and/or through third parties expressly authorised by the BANK, auditors, supervisory bodies of the BANK or third parties designated by the foregoing, the premises and documentation used by the SUPPLIER and/or its subcontractors, and it may advise adopting any other measure deemed necessary by the BANK to ensure due provision of the service.

- The BANK, its auditors, supervisory bodies or third parties designated by any of the foregoing shall have the power to access all relevant books, records and information held by the SUPPLIER and/or its subcontractors. Equally, the BANK, its auditors, supervisory bodies or third parties designated by any of the foregoing may verify, at the premises of the SUPPLIER and/or its subcontractors, the suitability of the systems, tools or applications used, as well as the information stored for the provision of the engaged service, in order to monitor and oversee the activity to which this contract relates.

- Where the SUPPLIER uses cloud services for the provision of the service to which this contract relates, the above provisions shall be without detriment to any rights of audit or access specifically set out in the “Information security” clause.

All of the above is irrespective of the organisational, managerial and disciplinary power that corresponds solely and exclusively to the SUPPLIER with respect to its employees, in its capacity as employer.

Commercial nature of the service provision

Both parties expressly accept that the business relationship is purely commercial in nature and are fully separate from employment regulations and jurisdiction.

The SUPPLIER shall provide services using its own workers. The payment of pay-rolls, indemnities, social security contributions and any other charges associated with all and any labour obligations arising from the agreed provision of the service using personnel at their disposal, shall be solely and exclusively borne by the SUPPLIER. Likewise, the payment of sanctions and all types of charges due to a breach of labour regulations or enforced by the authority charged by work inspections or labour courts and tribunals shall be solely and

exclusively borne by the SUPPLIER. The BANK shall be exempt from any liability for employees of the SUPPLIER related to occupational risks, particularly for any lack of fulfilment by such personnel of workplace security and occupational risk prevention standards set forth by the BANK for its own premises and personnel.

Independence of parties

The provision of a service does not constitute any dependency, corporate relationship or representation between Parties, who shall retain their full independence.

Each Party, during the course of their activities, shall represent an autonomous corporate organisation, and shall be responsible, directly or indirectly, for the fulfilment of all legally applicable obligations, particularly in respect of taxation and employment. Each party shall conduct its activities in their own name, and at their own risk and responsibility, and shall under no circumstances be authorised to act on behalf of the other Party or accept obligations of any type in the name or on behalf of the latter. All expenses and investments generated by each party during the course of their activities shall be borne by them and under their sole responsibility and risk, in addition to any taxes or levies imposed as a result of their activity.

Computer resources, industrial property and intellectual property

All materials, documents, technical resources, registered brands, trade names and logos provided by the BANK to the SUPPLIER for the provision of the service are considered to be the sole property of the BANK and shall not be used for any purpose other than the provision of such service. The SUPPLIER shall be responsible for their correct use, protection and safekeeping.

The SUPPLIER undertakes not to use under any circumstance any trade name or registered brand of the BANK or any of its Group companies, or the anagram or symbols of its corporate image or which are distinctive of the BANK, or any of its Group companies, without express written authorisation from the BANK.

Once the service has been provided, the SUPPLIER shall return to the BANK in full all materials, documents and technical resources provided for the provision of the service.

Liabilities

The SUPPLIER shall be liable to the BANK in all its corresponding activities and obligations, and any culpable or negligent acts, manipulation, fraudulent activity or undue access performed by its personnel, and shall hold the BANK harmless against any loss, fine, sanction or damages faced by the latter as a consequence of the non-fulfilment by the SUPPLIER of the obligations set forth for the provision of the service, derived from such service or claimed from the BANK by third parties. Consequently, the SUPPLIER agrees to pay for any amount charged as a sanction, damages for loss or injury, or for any other reason, requested from the BANK due to obligations undertaken by the SUPPLIER.

Employer liability and responsibility in terms of occupational health and safety as well as tax liability in terms of personal income tax withholdings and payments in kind of the SUPPLIER with employees involved in the provision of services, shall be solely and exclusively borne by the SUPPLIER, and the BANK shall remain exempt from any liability associated therewith. In the event that the BANK were required to accept pecuniary responsibility for a breach by the

SUPPLIER in these matters, the BANK may transfer the financial costs incurred in full to the SUPPLIER.

Likewise, the SUPPLIER shall hold the BANK harmless against any damages for loss or injury, sanction and/or expense derived from claims submitted by the persons affected, by the Spanish Data Protection Agency or those resulting from motions passed by competent authorities, as a result of a breach of current regulations on personal data protection or a breach of the obligations set forth during the provision of the service.

Personal data processing

Where, for the purposes of providing its services, the SUPPLIER has access or has the possibility to access personal data under the responsibility, custody and protection of the BANK, the SUPPLIER shall have the legal capacity of Data Processor in connection therewith.

For such cases, and in full compliance with that set forth in applicable national and regional legislation, the Parties wish to set out in this agreement the terms and conditions governing the processing of data by the SUPPLIER (hereinafter also referred to as the "Data Processor" or the "Processor").

Without prejudice to the foregoing, the Parties also wish to meet the requirements concerning relations with Data Processors set forth in Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, "GDPR") and in Organic Law 3/2018 on Personal Data Protection and Guarantee of Digital Rights.and, to that end, they agree as follows:

1. Purpose of data processing

By means of these clauses and provisions, the SUPPLIER, as Data Processor, is authorised to process on behalf of Banco de Sabadell, S.A., hereinafter also referred to as the "Data Controller" or the "Controller", any personal data required to comply with this contract.
Specifically, for each Specific Contract or Details of the Award, the various data processing activities to be carried out by the SUPPLIER shall be established for each service to be provided.

2. Identification of the data and data subjects concerned

For the implementation of the services to be provided, the Controller shall identify and make available to the Processor the type of data corresponding to the categories of data subjects, which shall be indicated in each Specific Contract or Details of the Award.

3. Duration

This data processing agreement shall remain valid and in effect for as long as the services to be provided remain in existence.

4. Obligations of the Data Processor

The Data Processor and all of its staff undertake to:

a. Use the personal data that are to be processed, or those collected for processing, for none other than the specific purpose of this authorisation. In no event shall the

purposes or uses of the data be modified, nor shall such data be used for personal purposes.

Should the Data Processor use the data for any other purpose, share such data or use such data in a manner that breaches the terms of this agreement, they shall also have the consideration of Data Controller, and shall be personally liable, without limitation, for any incurred infractions and for any damages that such actions may have caused to the Data Controller and/or the parties concerned.

b. Process the personal data to which they have access only in accordance with the written instructions received to such effect from the Data Controller, always complying with, at the very least, the same personal data protection policy and the policy on data retention security measures used for such purposes by the Data Controller. This commitment shall also apply to international transfers of personal data to a third country or to an international organisation.

   Should the Data Processor consider that any of the instructions infringe the GDPR or any provision in relation to data protection issued by the European Union or any of its Member States, the Processor shall promptly notify the Controller.

   Should any type of unlawful or improper practice be detected by any person discharging professional duties for the Data Processor (access to information that does not correspond to their duties, improper use of usernames and passwords, a user with more permissions than necessary, or any other practice), it shall be the responsibility and express duty of the Data Processor to promptly notify the Controller and send the latter a detailed report of the facts.

c. Not to share data with third parties, unless expressly authorised to do so by the Data Controller under legally acceptable circumstances.

   The Data Processor may share data with other Data Processors of the same Controller, pursuant to the instructions issued by the Controller. In such cases, the Controller shall identify, prior to such data sharing and in writing, the entity to which such data is to be shared, the data that is to be shared and the security measures that should be applied in order to share such data.

   No services referred to in the agreement may be subcontracted, in full or in part, to another Data Processor without the prior, written authorisation, given specifically for such purposes, of the Data Controller.

d. Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, always with the prior authorisation of the latter, the same data protection obligations as those stipulated for the Data Processor shall be imposed on that sub-processor. The Data Processor shall be fully accountable to the Data Controller, and shall be liable for the effective fulfilment by the sub-processor of obligations relating to data protection.

e. Uphold the duty of secrecy in relation to personal data to which they have had access by virtue of this authorisation, even after its expiration.

f. Ensure that persons authorised to process personal data have committed themselves, expressly and in writing, to uphold confidentiality and comply with the corresponding security measures, of which they must be appropriately notified.

For such purposes, the Data Processor undertakes to adopt, with respect to its employees or partners, the necessary measures to ensure that the latter are informed of the need to fulfil the obligations applicable to the former as Data Processor, which by extension are also applicable to such employees and partners, and to guarantee that any personal data that they gain knowledge of by virtue of this agreement shall remain secret even after this agreement is terminated, irrespective of the cause of such termination. To that end, the Data Processor shall give all necessary notices and warnings (through training, awareness-raising messages, etc.) and shall sign as many documents as necessary with its employees and partners, in order to guarantee fulfilment of such obligations.

The latter must be informed, in a comprehensible manner, of the existence of this agreement, the security rules affecting the performance of their duties, the consequences of any failure to comply with this agreement, the confidential nature of the information, and the duty of secrecy of personal data. The duty of confidentiality and secrecy shall remain in effect even after termination of the relationship with the Data Processor.

The aforesaid obligation to inform the employees and partners of the Data Processor must be fulfilled in such a way that enables documentation to be generated and made available to the Data Controller demonstrating fulfilment of said obligation, keeping the documentation demonstrating fulfilment of the obligation referred to in the previous paragraph at the latter's disposal.

The Data Processor undertakes to provide the Data Controller with all of the information required to demonstrate fulfilment of its obligations, and shall notify the Data Controller of any membership of an approved code of conduct, or of any certification mechanism that can guarantee fulfilment of its obligations relating to personal data processing.

g. Ensure that persons authorised to process personal data receive the necessary training in relation to personal data protection.

The persons performing professional duties for the Data Processor must be aware of the importance of the data that the Data Controller makes available to the Data Processor, process such data in a secure manner, and be trained and qualified for each and every stage of the data processing for each and every duty that they perform. Such persons must exercise all possible diligence and take appropriate measures to protect access to the data, in compliance with the duty of good faith to which they are contractually obligated.

h. Assist the Data Controller with responses to requests to exercise rights by applying all appropriate technical and organisational measures, in line with the nature of the processed data, in particular requests for exercising data subjects' rights to access, to rectification, to erasure ("right to be forgotten"), to portability of their personal data, to restriction of processing, to object to data processing, and to object to automated individual decision-making, including profiling.

Should the data subjects concerned send a request to exercise any of the rights referred to in the preceding section to the Data Processor, the latter must send a notification of such event to the email address indicated below. Such notification should be sent promptly and no later than the business day immediately following receipt of such request, together with any other information that may be relevant to attend to such request.

Email: ejercicioderechosprotecdatos@bancsabadell.com

i. Provide to the data subjects, at the time of the data collection, the information relating to any data processing that is to be carried out in the event that, pursuant to that agreed and in line with the instructions issued by the Data Controller, the Data Processor should be required to collect personal data. The wording and format in which such information is to be provided must be agreed with the Controller prior to initiating the data collection process.

j. Report data breaches.

The Data Processor shall be under the obligation to ensure implementation of the security requirements set forth in this agreement, and to notify the Data Controller of any incident affecting the information, documentation and/or personal data under the direct or indirect responsibility of the Data Controller.

Where the Data Processor or any person involved in the services detects an incident leading to the accidental or unlawful destruction, theft, loss, alteration or damage to the data, or in the event of any unauthorised access to such data, or should the data have been used in an improper manner, the Data Processor shall promptly contact the Data Controller and inform them of the details of the incident and the parties concerned, furnishing all relevant information for the documentation and disclosure of the incident and, at least, the following information (where available):

1. Description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
2. The name and contact details of the data protection officer or other contact point where more information can be obtained.
3. Description of the potential consequences.
4. Description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.

The above disclosure must take place by sending an email to SeginfoCsirt@bancsabadell.com indicating as the subject matter "NOTIFICACIÓN SEGURIDAD PROVEEDOR" ("SUPPLIER SECURITY NOTIFICATION"); the message must be encrypted using a mechanism approved by the Controller. On a supplementary basis, the Processor may call the number +34 609 20 66 04, the lines of which are open at all times every day of the year.

Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The Data Processor shall be responsible for taking all necessary actions to contain and resolve the incident.

The Data Controller shall regularly monitor the status of the incident's resolution and the Data Processor shall undertake to provide any requested reports.

k. Lend support to the Data Controller for the performance of data protection impact assessments, where appropriate.

l. Lend support to the Data Controller for the performance of prior consultations with the supervisory authority, where appropriate.

m. Permit and give every reasonable opportunity to the Data Controller in order for the latter, in compliance with its supervisory capabilities, to conduct on its own account, either directly or through designated third parties, reviews to verify compliance with the policies and security measures required by this agreement for the protection of information and personal data. Reviews may be carried out in the information systems and data processing facilities of the Data Processor or by gathering information that corroborates the Data Processor's compliance. The auditors of the Controller, as well as the supervisory bodies of the Controller or any third party designated by the foregoing, shall have the same supervisory powers and capabilities as the Controller.

In any case, the Data Processor must keep at the disposal of the Data Controller all documentation (in physical or electronic format) demonstrating or certifying fulfilment of its obligations under this agreement.

The Data Processor shall also be required to provide proof that it has carried out the corresponding risk assessments and, where appropriate, the pertinent data protection impact assessments.

In order to facilitate and even prevent the need for a review by the Data Controller, the Data Processor may provide the corresponding certifications, whose scopes of application shall include the services and staff offered by the latter to the Data Controller. Should the Data Processor decide to provide the aforementioned certifications, they shall also provide the relevant documentation, certification and scope of application, and submit reports relating to the audits to which they are subject pursuant to such certification.

Should the Data Controller detect any security breaches that are incompatible with the provision of the service, according to the risk assessment carried out by the same, depending on the severity of such breaches, they may require the Data Processor to promptly resolve the detected issues by preparing a remediation plan that should come into effect within a certain period of time, which shall be no longer than 3 months.

The foregoing is without prejudice to the ability to carry out any other audits or reviews in order to verify fulfilment of other obligations contained in this agreement.

n. Implement and comply with security measures of an organisational and technical nature deemed appropriate to guarantee a level of security that is proportionate to the risk that could arise from the data processing, in order to guarantee the security and integrity of personal data and prevent their alteration, loss, unauthorised processing or access, taking into consideration the state of technology, the implementation costs, the nature of the stored data, the scope of the data processing and the risks to which the data is exposed, as well as the impact that this may have on the rights and freedoms of natural persons, whether risks deriving from human actions or from the physical or natural environment, thereby also complying with requirements set forth in prevailing legislation.

The Data Processor shall be subject to certain security measures that shall be appropriate for the protection of personal data and other information, which shall be carried out by the

Data Processor in line with the results of the risk assessment performed by the Data Controller, taking into consideration the state of technology, the implementation costs, the nature of the stored data, the scope and purposes of the data processing and the risks to which the data is exposed.

Specifically, the Data Processor shall apply the security measures set forth in the "Information security" clause.

The Data Processor shall provide the Data Controller with at least the following information, in writing:

- The purposes and means of the intended processing.
- The implemented security measures.
- The impact assessment, where one has been performed by the Data Processor.
- Any other information requested by the Spanish Data Protection Agency and held by the Data Processor.

In all cases, and without prejudice to the security measures set forth above, the Data Processor shall implement mechanisms to:

a) Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
b) Restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
c) Regularly test, assess and evaluate the effectiveness of the technical and organisational measures in place for ensuring the security of the processing.
d) Pseudonymise and encrypt personal data, if any.

o. Intended use of data

Once the service to which the contract relates has been provided in full, the Data Processor undertakes, at the discretion of the BANK, to:

* return the personal data and any electronic files containing such data, once the service has been provided. Returning such data shall entail deleting all data existing in computer equipment used by the Data Processor; or
* destroy the data once the service has been provided. Once destroyed, the Data Processor shall certify such destruction in writing and shall submit the certificate to the Data Controller.

Similarly, the Data Processor shall, upon conclusion of the contractual relationship with any person with whom they have performed a professional duty;

- ensure that such person returns and does not keep in any manner the information and electronic files of the Data Controller;
- confirm the foregoing in writing or using any similar means permissible by the current law;
- promptly withdraw all authorisations relating to data processing.

Notwithstanding the foregoing, the Data Processor shall be entitled to keep a copy, with the data duly blocked, for as long as any responsibilities relating to the performance of the services may arise.

p. Undertake to hold the Data Controller harmless against any claim that may be filed against the latter due to a breach by the Data Processor and/or its subcontractors of that set forth in this agreement and in prevailing legislation on personal data protection, and agree to pay, without limitation, the amount in the form of a penalty, fine, compensation, damages or interest that may be imposed on the Data Controller, including lawyers' fees, in relation to such breach.

5. Obligations of the Data Controller.

The Data Controller shall:

a) Submit the personal data to which the data processing authorisation refers to the Processor.

b) Carry out, where appropriate, an assessment of the impact of the processing operations to be carried out by the Processor on the protection of personal data.

c) Carry out any corresponding prior consultations.

d) Ensure, both prior to and throughout the data processing, the Processor's compliance with the GDPR.

e) Oversee the data processing, including the performance of inspections and audits.

Information security

Should the SUPPLIER need to access and use the BANK's technology systems, understood as the full set of software items (programmes), hardware items (machines) and electronic media in place, the SUPPLIER undertakes to comply at all times with the Information Systems Security Policy that the BANK has in place at any given time and, in particular, at the present time, with the current Protocol on the Use of Information and Communications Technology in Banco Sabadell Group ("*Protocolo de Utilización de la Tecnología de la Información y de las Comunicaciones en el Grupo Sabadell*"). To that end, the BANK hereby provides the SUPPLIER with a copy of the aforesaid *Protocol*, and the latter acknowledges receipt thereof, which shall be fully valid and in effect for the SUPPLIER for the purposes of that set forth in both this clause and in the clause entitled "Liabilities", from the time of the first access and use of the technology systems, as defined in the *Protocol*, by the SUPPLIER. The SUPPLIER undertakes to inform its employees of the content of said protocol prior to initiating the provision of the service to which this contract relates.

Where during the course of the provision of the services the SUPPLIER must have access to or use the technology systems of the BANK, the SUPPLIER shall in each case apply the security measures set forth in the Information Security Clauses for the Service/SUPPLIER classed as Type A, B or C pursuant to the wording of such clauses, which are recorded in the deed executed before the Notary Public of Sabadell Mr Javier Micó Giner on 28 November 2017, under his protocol number 11,193, a photocopy of which the SUPPLIER declares to have received sufficiently in advance so as to assess and validate its application prior to signing this contract.

Should the service to be provided require software developments by the SUPPLIER, the latter must also comply with the measures set forth in the CLAUSE SUBJECT TO DEVELOPMENT SERVICES ("CLÁUSULA CONDICIONADA A SERVICIOS DE DESARROLLO") of such deed.

Where the SUPPLIER partially or fully subcontracts the services to be provided, the subcontractor in question shall also be required to comply with the principles set forth in the CLAUSE SUBJECT TO FULL OR PARTIAL SUBCONTRACTING OF THE SERVICE ("CLAUSULA CONDICIONADA A LA SUBCONTRATACIÓN TOTAL O PARCIAL DEL SERVICIO CONTRATADO"), which is also included in the aforementioned document.

Where the SUPPLIER makes full or partial use of cloud computing services for the provision of its services, the following shall apply and be specified in each case in the corresponding Specific Contract:

- whether it is a public, private, hybrid or community cloud and its geographical location.

- the Bank may require the SUPPLIER to produce a business continuity plan for the services provided under this contract and to fulfil the following auditing and right of access obligations, in accordance with the EBA Recommendations EBA EBA/REC/2017/03 of 28 March 2018 or any others that may amend or supplement those in the future, in addition to those set forth in the "Control and supervision" clause.

- As such, the SUPPLIER undertakes to provide the BANK, its statutory auditor, the supervisor, or any third party appointed by any of the foregoing for that purpose, with full access to the facilities (head offices and operations centres), including the full range of devices, systems, networks and data used for providing the services (right of access), as well as unrestricted rights of inspection and auditing related to the services (right of audit). No contractual arrangement shall obstruct or hinder the enforcement of both rights, nor prevent the BANK and/or the supervisor from carrying out their supervisory function and/or objectives.

The party intending to exercise its right of access should before a planned onsite visit provide notice in a reasonable time period of the onsite visit, unless an early prior notification has not been possible due to an emergency or crisis situation. The SUPPLIER is required to fully cooperate with the BANK, its statutory auditor, the supervisor and any third party appointed by any of the foregoing in connection with the onsite visit.

The BANK may also consider, at any time, whether to require the SUPPLIER to adopt specific measures, which the SUPPLIER undertakes to implement once notified of the requirement, in order to protect data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture.

Confidentiality

Confidential information (hereinafter, "Confidential Information") shall include all data, documents and information of any type disclosed verbally, in writing, or through any other transmission means by the BANK or any natural or legal person acting in its name or on its behalf, to the SUPPLIER. The SUPPLIER undertakes and obligates itself, before the BANK, to comply with the following obligations:

a) Maintain confidentiality and reveal Confidential Information only to those directors and employees (a) who are directly involved in the provision of the service, (b) who have a vital need to know such information in order to perform the aforementioned service, and (c) who undertake to adhere to the provisions contained herein, in particular those regarding Confidential Information.

b) Not to use revealed Confidential Information for any purpose other than the provision of the service.

c) Not to disclose Confidential Information provided by the BANK to third parties without its prior written consent.

d) Furthermore, the SUPPLIER:
- shall not acquire any rights over Confidential Information of the BANK or of third parties to which it has had access during the execution of the Service, and
- shall not refuse to return such Confidential Information to the BANK.

If the BANK should request it in writing, the SUPPLIER shall return (or destroy, if so requested) all documents and other written material or any other means of transmission that have been revealed to them or put at their disposal, together with any copies thereof, and shall delete from any computers under their control any and all documents or files that contain or reflect Confidential Information, such that all information that is deleted cannot be recovered at any time. Any Confidential Information, whether verbal or forming part of written assessments, reports, studies or other documents created by or for the SUPPLIER shall be subject to the terms and conditions of the corresponding contract concluded for the provision of the service.

The following shall not be considered Confidential Information:

a) Information outside of the public domain at the time of its disclosure, or which becomes public, except when such information is made public as a consequence of a breach by the SUPPLIER of the obligations corresponding to it for the provision of the service.
b) Information already in the possession of the SUPPLIER before being received through the BANK, and that does not qualify as Confidential Information.
c) Information that has been independently created by the SUPPLIER (as evidenced through written communications from the SUPPLIER or its advisers).
d) Information that has been, in full or in part, requested from the SUPPLIER, due to legal provisions or judicial rulings or rulings reached by public bodies, provided that the BANK is promptly notified of such requirements when legally possible.

The SUPPLIER shall inform its personnel and collaborators of the obligations set forth on confidentiality. The SUPPLIER shall advise as often as necessary and sign as many documents as necessary with its personnel and collaborators in order to ensure that such obligations are complied with. The SUPPLIER shall be liable to the Bank if such obligations are breached by those employees or collaborators.

The duties of confidentiality set forth shall be effective perpetually, and shall remain in force after the termination, for whatever reason, of the relationship between the BANK and the SUPPLIER.

Sub-outsourcing

The SUPPLIER undertakes not to fully or partially assign, delegate or sub-outsource this contract or any of the rights or obligations arising in connection herewith.

Notwithstanding the foregoing, if during the term of the contract, a need should arise to sub-outsource a part of it, the SUPPLIER shall notify the BANK, at least one (1) month prior to the date on which the intended sub-outsourcing is to take place, of the identification details of the SUPPLIER to which it will sub-outsource, as well as a description of the specific service to be

sub-outsourced, so that the BANK may, if appropriate, proceed to authorise such sub-outsourcing.

The SUPPLIER undertakes to enter into a contract for the provision of services with subcontractor(s) to regulate the services sub-outsourced to them, and in particular, with respect to the protection of personal data, to follow the instructions for personal data processing, which must in all cases comply with the instructions of the BANK in this regard, to not use the data for purposes other than those set out in the aforesaid contract, to not disclose the data under any circumstances to third parties, to adopt the security measures to be implemented in the processing in accordance with prevailing data protection legislation, and to fulfil all ensuing responsibilities in the event of any personal data protection breaches.

All of the foregoing shall be without prejudice to the fact that in all cases the SUPPLIER shall be liable to the BANK for any breach by its subcontractors and in particular for any acts, errors or negligence in the compliance with labour, trade union, social security, occupational hazard prevention and health and safety obligations by any subcontractor(s), their representatives, employees or workers, none of which shall be attributable under any circumstances to the BANK, which may file a claim for recovery against the SUPPLIER if any consequences of such cases are attributed to it.

Assignment

Neither Party may fully or partially assign this contract or the obligations or rights deriving from it, except with the express prior consent of the other Party. However, assignment shall not be deemed to exist where a contractual position is assigned between companies that are part of Banco Sabadell Group, applying the meaning of 'group' set out in Article 42 of Spain's Code of Commerce.

Sustainability, rules of conduct and model for compliance and prevention of corporate crime, money laundering, terrorist financing and corruption

Sustainability: In line with Banco Sabadell Group's description of itself as an institution committed to policies and actions that respect human and workers' rights and that is against the exploitation of people, and as part of the implementation of Banco Sabadell Group's policies on human rights and rights of suppliers, the SUPPLIER undertakes to adhere to and put in practice, both during the provision of the services to which this contract relates and during its day-to-day professional activities, the content of the "Policies, codes and rules" of Banco Sabadell Group published on the corporate website (www.grupbancsabadell) in the "Sustainability" section and in particular with regard to the content of the (i) Banco Sabadell Code of Conduct, (ii) Banco Sabadell Code of Conduct for Suppliers, (iii) Human Rights Policy, (iv) Sustainability Policy, (v) Equality Plan, as well as (vi) the ten principles of the United Nations Global Compact in the areas of human rights, labour, environment and anti-corruption, of which Banco Sabadell Group is a signatory.

Rules of conduct: the SUPPLIER shall comply with the principles and rules of conduct applicable within its sector when providing the services to which this contract relates.

Compliance and prevention of corporate crime, money laundering, terrorist financing and corruption:

The SUPPLIER declares to be aware that Banco Sabadell Group has adopted an organisational and management model that includes control and oversight measures for the prevention of compliance risks and, more specifically, the commission of crimes, including those related to

corruption, money laundering and terrorist financing, which are applicable to the entire Banco Sabadell Group (hereinafter also referred to as the "Model"), whose effectiveness requires the involvement of partners and suppliers of goods and services to Banco Sabadell Group companies and their subcontractors.

The Model includes the following standards and rules, among others: (i) Banco Sabadell Code of Conduct, (ii) Banco Sabadell Code of Conduct for Suppliers, (iii) Compliance Policy, (iv) Banco Sabadell Group Corporate Crime Prevention Policy, (v) Anti-Corruption Policy, and (vi) Anti-Money Laundering and Counter-Terrorist Financing Policy (hereinafter, "Compliance Regulations"). The Compliance Regulations are available on the corporate website (www.grupbancsabadell.com) in the "Sustainability" section and their provisions are binding on Banco Sabadell Group.

Pursuant to the aforesaid Compliance Regulations, the SUPPLIER undertakes:

- To provide the goods/services to which this contract relates in accordance with the applicable legal obligations and, in particular, the laws, bylaws, regulations and codes applicable in relation to anti-money laundering, counter-terrorist financing and anti-corruption, which include, among others, Law 10/2010 of 28 April on anti-money laundering and counter-terrorist financing (*Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo*) and its implementing regulations, as well as the prohibitions in relation to corruption set out in the Spanish Criminal Code.

- Not to offer, promise, deliver, solicit or accept, nor as at the date of this contract's entry into effect to have offered, promised, delivered, solicited or accepted, either directly or indirectly, any undue consideration, benefit or advantage to/from any "Civil Servant" and/or individual, whether national or foreign, for the purpose of influencing the actions of the authority or public institution or in any way to obtain an undue advantage within the framework of this contract.

- To promptly notify the BANK, using the specific crime reporting channel put in place by the BANK for this purpose, accessible through the link https://canaldenunciasgrupo.bancsabadell.com, any data or information that could be indicative of the actual or potential commission of a crime or a breach of the Compliance Regulations in connection with the execution of this contract and which affects or could affect any of the Banco Sabadell Group companies and/or the natural persons associated therewith. Moreover, it also undertakes to extend this obligation, under the same terms, to its subcontractors, if any, by providing them with the web address indicated above. The source of the information shall be kept in confidence at all times, pursuant to prevailing data protection legislation, without prejudice to the fulfilment of any applicable legal obligations.

- To manage, investigate and, as appropriate, penalise any incident occurring within its line of business, at all times complying with applicable legislation in all legal aspects concerned. The SUPPLIER shall observe applicable legislation, including but not limited to that applicable to labour matters, personal data protection and the protection of informants, as the case may be.

- To promptly notify the BANK of any breaches of any of the obligations described in this clause. In the event of a breach, the BANK reserves the right to require the SUPPLIER to immediately adopt appropriate corrective measures by common agreement between the Parties. Any infringement or breach of that stipulated herein, even if occasional or isolated,

shall constitute a severe breach of this contract and may be grounds for its termination, in accordance with the Contract Termination clause.

***** Same text up to this point. From this point onwards, there are 2 options: Option A, where the SUPPLIER has a corporate crime prevention model or programme with measures and principles equivalent to those of Banco Sabadell Group, in which they case they shall undertake to comply with their own model, or Option B, where the SUPPLIER has no such model or programme, in which case they shall undertake to comply with Banco Sabadell Group's Corporate Crime Prevention Policy. *****

In line with these provisions, the SUPPLIER declares:

Option A:

- **That it has its own prevention and compliance model or scheme in place for the prevention of compliance risks and, especially, corporate crime, in line with legal regulations, and that such model or scheme includes measures equivalent to those set out in the aforesaid Banco Sabadell Group Compliance Regulations. In this respect, the BANK may require the SUPPLIER to give proof of the existence the aforesaid model or scheme, at any time, for the purpose of verifying compliance with this clause. Should the BANK consider that the model or scheme evidenced by the SUPPLIER does not contain measures that can be considered equivalent to those set out in Banco Sabadell Group's Compliance Regulations, the SUPPLIER shall, from that point onwards, undertake to immediately comply with the aforesaid Compliance Regulations upon simple demand of the BANK until such a time as its model or scheme includes the aforesaid measures deemed equivalent by the BANK.**

- **That it agrees and undertakes to act without circumventing the control and oversight measures, as well as the principles and terms, contained in its model for the organisation and management of compliance risks and corporate crime prevention.**

Option B:

- **That it undertakes to act in accordance with the aforesaid Banco Sabadell Group Compliance Regulations.**

Penalty clause for the delivery of materials

In the event that the BANK were to determine that the material received does not exactly match the material requested and approved according to the delivered sample or standardised material, should the date on which the material is delivered be insufficient to correct the situation, the Bank reserves the right to apply a penalty equivalent to 40% of the total amount payable by the SUPPLIER for the purchased undelivered material within the established time frame.

Similarly, provided that the requested product is delivered by the SUPPLIER after the date specified upon ordering it, the Bank reserves the right to apply a penalty of 1% of the total amount payable by the SUPPLIER for each day delivery is withheld.

Applicable law and conflict resolution

This contract shall be subject to the Spanish legislation in force at any given time, and in the event of any disputes or complaints, the Parties shall submit to the authority and jurisdiction of the courts of law of Alicante, with express waiver, as necessary, of their own jurisdiction or venue.

Details of the representatives of the legal entities entering into this contract

The undersigned, representing the legal entity or entities entering into this contract, are hereby informed that their personal data shall be processed by the BANK and the SUPPLIER, respectively, for the sole purpose of managing and executing this contract, on the legal basis of this contract. They shall be entitled to exercise, through the respective registered offices, their rights of access, rectification, objection, erasure, restriction and portability, pursuant to that set forth in Regulation (EU) 2016/679 and in Organic Law 3/2018 on Personal Data Protection and Guarantee of Digital Rights.