CREDIT SUISSE

Extract from the Client Information Booklet
9. Data Protection Information

The following data protection information gives an overview of the collection and processing of your Personal Data (as defined below).
Translations in other languages of this section 9 of the Client Information Booklet, including Appendix 5 and 6 are available under:
http://www.credit-suisse.com/lu/en/private-banking.html

With the following information, we would like to give an overview of how we will process your Personal Data and of your rights according to data protection laws and regulations. The details on what data will be processed and which method will be used depend significantly on the services applied for or agreed upon.

1. Who Is Responsible For Data Processing and How Can I Contact Them?

The Data controller (hereinafter referred to as "**we**" or "the **Bank**") is:

CREDIT SUISSE (LUXEMBOURG) S.A.
5, rue Jean Monnet
L-2180 Luxembourg
Grand Duchy of Luxembourg
Phone: +352 46 00 11-1
Fax: +352 46 32 70

In case of any questions or requests concerning your Personal Data, you may contact either:

CREDIT SUISSE (LUXEMBOURG) S.A.
Data Protection Office Representative
5, rue Jean Monnet
L-2180 Luxembourg
Grand Duchy of Luxembourg
Phone: +3520 46 00 11-1
E-mail: luxembourg.data-protection@credit-suisse.com

or

CREDIT SUISSE AG, LONDON BRANCH
Credit Suisse Group Data Protection Officer
One Cabot Square
London E14 4QJ
United Kingdom
Phone: +44 20 7888 8888
E-mail: data-protection@credit-suisse.com

2. What Sources and Data Do We Use?

As a data controller, we process **Personal Data** (also referred to as "**Data**"), as defined below, that we collect directly from our clients in the context of our business relationship. We also process – insofar as necessary to provide our service – Personal Data that we obtain from publicly accessible sources (e.g. debt registers, commercial and association registers, press, internet), or that is legitimately transferred to us by other Credit Suisse Group companies or other third parties (e.g. a credit agency).

In order to facilitate, enable and/or maintain our business relationship, we collect and otherwise process Personal Data relating to the Client and any other person(s) involved in the business relationship, as the case may be, such as authorized representative(s), person(s) holding a power of attorney, beneficial owners, if different from the Client, any natural person who exercises control over an entity (control is generally exercised by any natural person who ultimately has a controlling ownership interest in an entity, "**Controlling Person**") and any person for the benefit of which the Client is holding an account as agent, nominee or similar (account holder for automatic exchange of information purposes, "**AEI Account Holder**"), each an "**Affected Person**".

Relevant Data processed by the Bank includes, but is not limited to, Client's/Affected Person's personal information (e.g. name/company name, residence/tax address, registered office and other contact details, date and place of birth, nationality/nationalities), identification Data (e.g. ID card details), taxpayer identification number (TIN), account number, Client number (CIF) and authentication Data (e.g. sample signature). Furthermore, Relevant Data could also relate to order Data (e.g. payment order), Data from the fulfillment of contractual obligations (e.g. sales data in payment transactions), information about Client's/Affected Person's financial situation (e.g. creditworthiness Data, value of property serving as collateral, rating, origin of assets), marketing and sales Data, documentation Data (e.g. consultation protocol), and other Data similar to the categories mentioned that the Bank becomes aware in connection with the business relationship with the Client ("**Personal Data**", "**Data**").

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. What Do We Process Personal Data for (Purpose of Processing) and On What Legal Basis?

We process Personal Data in accordance with the provisions of the EU General Data Protection Regulation ("**GDPR**"),[1] on the following legal grounds:

a. if processing of Personal Data is necessary for the performance of the contract(s) entered into with the Client or in order to take steps at the Client's request prior to entering therein:

Data is processed in order to provide banking and financial services in accordance with the **contract(s) with our clients or to take pre-contractual measures** in preparation thereof. The purposes of Data processing depend primarily on the concrete product (e.g. bank account, credit, securities, deposits, client

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 97/46/EC.

referral) and can include needs assessments, advice, asset management and support, as well as executing transactions and transmitting orders. You may find other details about the purposes of Data processing in the relevant contract documents and/or the General Terms and Conditions.

b. if processing of Personal Data is necessary for the purpose of compliance with a legal obligation to which the Bank is subject:

As a bank, we are subject to various **legal obligations**, meaning statutory requirements (e.g. the Law of 5 April 1993 on the financial sector; the Amended Law of 12 November 2004 relating to fight against money laundering and terrorist financing; the Law of 18 December 2015 regarding the automatic exchange of information relating to financial accounts in tax matters; CSSF regulations and/or other applicable laws or regulations – all as amended from time to time). Purposes of processing include assessment of creditworthiness and solvency, identity checks (know-your-customer), fraud and money laundering prevention and detection, fulfilling control and reporting obligations under fiscal laws, regulatory reporting. For these purposes, the Bank may process Personal Data in relation to both the Client and any Affected Person, as the case may be.

c. if processing of Personal Data is necessary for the purposes of the legitimate interests pursued by the Bank, as the data controller, or a third party:

We process Personal Data beyond the actual performance of the contract or legal obligations, for the purposes of the **legitimate interests** pursued by the Bank, Branches of the Bank or a third party.

Examples:
- Improving products and services
- Asserting legal claims and defense in legal disputes
- Guarantee of the bank's IT security and IT operation
- Prevention and detection of frauds
- Video surveillance to protect the right of owner of premises to keep out trespassers, for collecting evidence in hold-ups or fraud, or to prove availability and deposits, e.g. at ATMs
- Measures for building and site security (e.g. access controls)
- Measures for business management and further development of services and products
- Risk (including credit risk), credit recovery, management and reporting
- Compliance, internal supervision and internal audit
- Creating statistics
- Marketing of our products and services (to the extent it does not involve profiling).

Whenever we intend to rely on legitimate interest as the legal basis for the processing of Personal Data, we will give due consideration to the Client's and any Affected Person's rights and freedoms.

d. if processing of Personal Data is based on your consent:

If we have been granted **consent** to process Personal Data relating to the Client or any Affected Person for certain purposes (e.g. for marketing of our products and/or services that involves profiling), the related processing of Data is based on the data subject's consent. Consent given can be withdrawn at any time. This also applies to withdrawing declarations of consent that were given to us before the GDPR came into force, i.e. before May 25, 2018. Withdrawal of consent does not affect the legality of Data processed prior to withdrawal.

4. Who Receives the Personal Data?

Within the Bank, every unit that requires Personal Data relating to the Client and any Affected Person (as the case may be) in order for the Bank to achieve purposes described in section 3 will have access to it. As regards to Clients serviced by the Branches of the Bank, the Bank processes Personal Data relating to the Client and Affected Persons, and shares such Personal Data with the Branches to which the Personal Data relates on a need to know basis. In this respect, the Bank and its respective Branch act as joint Data Controllers and have therefore entered into the joint data controllership agreement. As regards to the processing of Data by the Branches of the Bank please refer to **Appendix 6**, entitled "**Additional Data Protection Information relating to the Branches of CREDIT SUISSE (LUXEMBOURG) S.A.**".

The data recipients **outside the Bank** and its Branches are hereinafter referred to as "**Data Recipients**".

With regard to transferring Personal Data to Data Recipients, it is to be noted that, as a financial institution, we are bound by confidentiality obligations regarding all Client-related matters of which we acquire knowledge (professional secrecy pursuant to the section entitled "Data Protection and Professional Secrecy" of our General Terms and Conditions). We may pass on Personal Data only if legal provisions demand or authorize it or in case of Client consent (e.g. to process a financial transaction). Bearing in mind these requirements, please see the overview of all Data Recipients outside the Bank and the Branches of the Bank outlined in the **Appendix 5, entitled** "**List of Data Recipients**".

The Bank will implement appropriate organizational and technical safeguards to protect the Personal Data for which it acts as data controller at all times.

5. Will Data Be Transferred to a Third Country?

The Bank may transfer Personal Data to Data Recipients located **in third countries** (countries outside the European Economic Area). Such transfer takes place so long as:

- A country has been recognized by the EU Commission as guaranteeing adequate level of data protection (in particular, Switzerland), or
- It is necessary for the performance of a contract between the Client and the Bank or implementation of the pre-contractual measures taken at your request (e.g. for the purpose of carrying out your orders (e.g. payment and securities orders), even if the recipient country has not been recognized by the EU Commission as guaranteeing adequate level of data protection, or
- the Client has granted us an explicit consent, even if the recipient country has not been recognized by the EU Commission as guaranteeing adequate level of data protection.

6. Use of electronic means of communication

The Bank may use any means of communication, including electronic means such as E-mail, to share, disclose and/or transfer Personal Data in order to achieve the purposes outlined in section 3. For further details relating to the use of electronic means of communication please refer to the section entitled "Data Protection and Professional Secrecy" in the General Terms and Conditions.

7. For How Long Will My Data Be Stored?

We will process Personal Data relating to the Client and any Affected Person (as the case may be) for **as long as is necessary for the purposes described in section 3**. It should be noted here that our business relationship is based on a long-term obligation, which is set up on the basis of periods of years.

If the Data is no longer required in order to fulfill contractual or statutory obligations, it is deleted, unless its further processing is required – for a limited time – for the following purposes:

- Fulfilling **obligations to preserve records** according to commercial and tax laws as well as financial sector laws and regulations. This includes in particular Luxembourg Commercial Code and Law of 5 April 1993 on the financial sector, as amended. In general, for this purpose we keep Personal Data relating to the Client and any Affected Person (as the case may be) for a maximum period of 10 years upon termination of the business relationship
- As a bank we can face **legal holds**,[2] which might require us to keep records for a longer period of time.

8. What Data Privacy Rights Do I Have?

Every data subject has the right to **access**, the right to **rectification**, the right to **erasure**, the right to **restrict processing**, the right of **object** and if applicable - the right to **data portability**. Furthermore, there is also a right to **lodge a complaint** with an appropriate Data protection supervisory authority.[3]

Every data subject can withdraw a consent granted to us for the processing of Personal Data at any time. This also applies to withdrawing declarations of consent that were made to us before the GDPR came into force, i.e. before May 25, 2018. Please note that the withdrawal only applies to the future. Processing that was carried out before the withdrawal is not affected by it.

Information on Your Right of Objection

1. <u>Right to Object to Data Processing for Direct Marketing Purposes</u>

In individual cases we process your Personal Data in order to conduct direct marketing. You have the right to object to the processing of your Personal Data for the purpose of this type of marketing at any time. This also applies to profiling, insofar as it is in direct connection with such direct marketing.

If you object to processing for the purpose of direct marketing, we will no longer process your Personal Data for this purpose.

[2] A legal hold is a process that an organization uses to preserve all forms of relevant information in case of pending or anticipated litigation, investigation and other legal proceedings.

[3] Luxembourg data protection authority: *the Commission nationale pour la protection des données* (CNPD) (https://cnpd.public.lu).

2. Individual Right of Objection

You shall have the right of objection, at any time, to processing of your Personal Data that is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party. This also applies to profiling.

If you submit an objection, we will no longer process your Personal Data unless we can give evidence of mandatory, legitimate reasons for processing, which outweigh your interests, rights, and freedoms, or processing serves the enforcement, exercise, or defense of legal claims. Please note, that in such cases we might not be able to provide services and/or maintain a business relationship with you anymore.

9. Am I Obliged to Provide Personal Data?

In the context of our business relationship, you must provide all Personal Data that is required for accepting and maintaining the business relationship and for fulfilling the accompanying contractual obligations or that we are legally obliged to collect. **Without this Data, we are, in principle, not in a position to execute a contract with you**.

In particular, anti-money laundering regulations require us to identify you on the basis of your identification documents before establishing a business relationship and to collect and put on record name, place and date of birth, nationality, address and identification details for this purpose. In order for us to be able to comply with these statutory obligations, you must provide us with the necessary information about you and/or Affected Persons, as the case may be, and documents in accordance with the applicable anti-money laundering legislation, and immediately disclose any changes over the course of the business relationship. If you do not provide us with the necessary information and documents, we cannot enter into or continue the business relationship you desire.

10. To What Extent Is There Automated Decision-Making?

In establishing and carrying out a business relationship, we generally do not use any automated decision-making. If we use this procedure in individual cases, we will inform you of this separately, as long as this is a legal requirement.

11. Will Profiling Take Place?

We process some of your Personal Data **automatically, with the goal of assessing certain personal aspects** (profiling). We use profiling for the following cases, for instance:

- Due to legal and regulatory requirements, we are obligated to combat money laundering, terrorism financing, and offences that pose a danger to assets or the integrity of financial markets. Data assessments (including on payment transactions) are also carried out for this purpose. At the same time, these measures also serve to protect you.
- We may use assessment tools in order to be able to specifically notify you and advise you regarding products. These allow communications and marketing to be tailored as needed – including market and opinion research.

- We may use scoring as part of the assessment of your creditworthiness. This calculates the probability that a Client will meet the payment obligations pursuant to the contract. This calculation may be influenced by the Client's earning capacity, expenses, pending liabilities, occupation, employer, term of employment, experience from the business relationship thus far, contractual repayment of previous credits, and information from credit information offices, for instance. Scoring is based on a mathematically and statistically recognized and established process. The calculated scores help us to make decisions in the context of product sales and are incorporated into ongoing risk management.

12. We may collect biometric Data from you

Biometric data is classified as sensitive Personal Data. Therefore your explicit consent will be required in a separate process to use your touch ID or other biometric identification to access certain applications, unless local laws implementing the GDPR provide otherwise.

CREDIT SUISSE

Extract from the Client Information Booklet Appendix 5

List of Data Recipients

1. Introductory note

The purpose of this document is to provide a detailed overview of the disclosure of Personal Data relating to the Client and Any Affected Person (as the case may be) to **recipients outside the Bank ("Data Recipients")**. This Appendix forms an integral part of the **Data Protection Information** issued by the Bank and may be updated from time to time. Accordingly, you will be notified of any update made to this Appendix 5.

2. Data Recipients outside the Bank

2.1 Within Credit Suisse Group

The Data Protection Information provided by the Bank includes some detail as to the purposes for which the Bank may processé Personal Data relating to the Client and any Affected Person (as the case may be). For the same or related purposes, in the context of outsourcing of certain functions and to ensure an efficient servicing of Clients' needs, the Bank may disclose your Personal Data to the following Credit Suisse Group entities that act as service providers to the Bank:

2.1.1 Credit Suisse AG, Credit Suisse (Schweiz) AG, Credit Suisse Services AG ("**CS CH**") –

Certain operational processes relating to the Bank are operated on the information technology (IT) platform of CS CH in Switzerland ("**Swiss IT Platform**"), where Personal Data is processed (e.g., storage), to the extent required in relation to the provision of services by CS CH to the Bank, to enable CS CH or the Bank to comply with regulatory reporting requirements as well as for operational, risk management (e.g., credit risk management), internal supervision, audit, compliance (e.g., anti-money laundering), Client event management and/or IT purposes on Credit Suisse Group level. In this regard, dedicated persons and/or teams of CS CH will have access to Personal Data on the Swiss IT Platform as well as process such Personal Data on a need-to-know basis. It may also be required for the Bank to provide Personal Data to CS CH by other means than via the Swiss IT Platform. Moreover, the Bank may outsource specific processes or tasks to CS CH (e.g., relating to operational processes, compliance (e.g., anti-money laundering), risk management (e.g., credit risk management), internal supervision, reporting, audit and/or IT) which require that dedicated persons and/or teams of CS CH get "read access" to the Bank's local IT system or client data system in Luxembourg, including access to Personal Data on a need-to-know basis.

Further, the Bank's E-mail infrastructure is operated by CS CH. Personal Data could therefore be viewed by employees of CS CH for maintenance purposes.

E-mails received and sent by the Bank (e.g., E-mails received from and sent to Clients or E-mails sent to Data Recipients) will, for a period not exceeding the maximum statutory safekeeping period for business correspondence, be stored in Switzerland by means of an automated procedure known as "Communication Journaling" by CS CH. Communication Journaling means that unalterable copies of e-mails are stored in a strictly confidential internal "Journaling Repository".

The above data sharing scenarios between the Bank and CS CH apply also in the context of **Branch Client Relationships** (as defined in the separate **Appendix 6,** "**Additional Data Protection Information relating to the Branches of CREDIT SUISSE (LUXEMBOURG) S.A.**"), in which case CS CH may provide services to the Branches of the Bank indirectly, i.e. via the Bank. Nonetheless, the Branches of the Bank (as defined in the separate **Appendix 6**) may further decide, for the same purposes as outlined above, to share Personal Data directly with CS CH (in particular – in the context of outsourcing of certain tasks directly to CS CH).

2.1.2 Credit Suisse (Poland) Sp. z o.o.

The services of CS Poland may be used in case of a sub-outsourcing of certain tasks by CS CH to Credit Suisse (Poland) Sp. z o.o. or any other Credit Suisse company in Poland, as the case may be, ("**CS Poland**"), in which case CS CH may be required to disclose Personal Data to CS Poland. In such cases, Personal Data may be processed by CS Poland.

The Bank may also directly outsource specific processes or tasks to CS Poland (e.g., relating to operational processes, compliance (e.g., anti-money laundering), risk management (e.g., credit risk management), internal supervision, reporting, audit and/or IT) which require dedicated persons and/or teams of CS Poland to obtain "read access" to the Bank's local IT system or client data system in Luxembourg, including access to Personal Data on a need-to-know basis.

The above data sharing scenarios between the Bank and CS Poland apply also in the context of Branch Client Relationships, in which case CS Poland provide services to the Branches indirectly, via the Bank and/or CS CH. Nonetheless, Branches of the Bank may further decide, for the same purposes as outlined above, to share Personal Data with CS Poland directly (in particular – in the context of outsourcing of certain tasks directly to CS Poland).

2.2. External recipients (Data Recipients outside the Credit Suisse Group)

2.2.1 In connection with payment or other transactions we carry out for you, or in cases where the Bank acts as custodian and/or broker in relation to financial instruments, the Bank may be required to transfer Personal Data relating to the Client and any Affected Persion (as the case may be) to **other financial service institutions or comparable institutions and/or authorities**, in Luxembourg, in countries where Branches of the Bank are established or abroad. Depending on the the transaction/service Data Recipients may include other entities in Credit Suisse Group, other banks (e.g., correspondent banks), operators of payments systems, sub-custodians and their service providers or processing units, issuers and their service providers, brokers, (stock) exchanges, processing units, central securities depositories, clearing institutions, brokers and the Society for Worldwide Interbank Financial Telecommunication ("**SWIFT**"). Such disclosure may be required to third parties to whom the Bank or any CS Luxembourg Branch has a reporting obligation (e.g., trade repositories, authorities or (stock) exchanges) in accordance with applicable legislation (e.g., European Market Infrastructure Regulation (" EMIR"), Markets in Financial Instruments Regulation ("MiFID")), to establish segregated accounts for you with a sub-custodian (as may be required by law) or to obtain investor and/or tax licenses/registrations or similar. Even in relation to transactions within Luxembourg or countries where Branches of the Bank are established, Personal Data may need to be disclosed in other countries (e.g., in case a Payment Transaction is carried out using SWIFT). The Data Recipients referred to before may be required to further disclose Personal Data to authorities or other third

parties in accordance with applicable law or regulations, e.g., for the purpose of anti-money laundering or combating terrorist financing.

2.2.2 We may also share your Personal Data with **information offices** (e.g., debt registers) and/or with third party providers for the purpose of investigating creditworthiness, credit risk and solvency (in particular, in credit business) and/or for regulatory reporting purposes.

2.2.3 Under certain circumstances, the Bank may be obliged to disclose Personal Data to **public entities and institutions** in Luxembourg, in the countries where Branches of the Bank are established or abroad (e.g., bank and/or financial sector supervisory authorities and tax authorities, criminal prosecution authorities) based on a legal obligation the Bank.

Under the law of 18 December 2015 regarding the automatic exchange of information relating to financial accounts in tax matters, as amended, we are obliged to report certain Personal Data relating to the Client, any **AEI Account Holder** or **Controlling Person**, as the case may be, in connection with the Automatic Exchange of Information ("**AEI**"), to the Luxembourg Tax Administration ("**LTA**"). This reporting is completed on an annual basis, and the LTA further transfers such Personal Data to the competent tax authorities in any reportable jurisdiction(s), in which the reportable person is resident for tax purposes. Also for the purposes of the AEI, the Bank is deemed to be data controller within the meaning of statutory regulations on data protection. The Personal Data that the Bank is required to disclose to the LTA includes: name(s), address(es), country/ies of residence for tax purposes, tax identification number(s) ("TIN(s)"), date(s) and place(s) of birth, account number(s), the name of the Bank, account balance(s) or value(s) as of the end of the relevant calendar year or other appropriate reporting period if the account(s) was/were closed during the year, in the case of (a) custodial account(s), the total gross amount of interest, dividends and other income generated with respect to the assets held in the account(s), the total gross proceeds from the sale or redemption, and in the case of (a) depository account(s), the total gross amount of interest paid or credited regarding the Client and/or the Affected Person, as applicable. The Client's failure to provide Personal Data required for the purposes of the AEI to the Bank may trigger a reporting in multiple jurisdictions.

Further, the Bank is subject to various US tax regulations and agreements, such as the US Foreign Account Tax Compliance Act ("**FATCA**") and the Qualified Intermediary regime ("**QI**") requiring the Bank to provide certain information relating to a **US Client** (as defined in the respective legislation) to the US Internal Revenue Service ("**IRS**") on a yearly basis ("**US Tax Reporting**"). Under the QI regime the reporting relates to US Clients with US securities, under FATCA the reporting relates to any bank assets/financial accounts held by US Clients. Under FATCA the US Tax Reporting obligation exists towards the LTA which passes such information on to the IRS. Under QI, in connection with US securities the US Tax Reporting is provided to CS CH which in turn passes on such information to the US sub-custodian which then passes the information on to the IRS. For US Tax Reporting purposes the Bank must report the Client's/any Controlling Person's name and address, a copy of any IRS Form W-9 "Request for Taxpayer Identification Number and Certification", TIN, assets, gross income and gross proceeds, as well as any other information which may be required at any given time for the fulfillment of the US Tax Reporting obligations to which the Bank is subject.

2.2.4 We may use external service provider(s) ("**Third Party Sevice Providers**"), located in Luxembourg or in the countries where CS Luxembourg Branches are established, for the purpose of physical **documents lifecycle management**, including archiving and destruction thereof.

We may share limited Personal Data with Third Party Service Providers, located in Luxembourg or in the countries where CS Luxembourg Branches are established, which support us with issuance, management and mailing of **Client invoices**, or which we have entrusted with the production and preparation of the yearly **Client tax reporting, respectively**.

Such Third Party Service Providers are selected by us with due care and are subject to confidentialy obligations.

2.2.5 The Bank may be required to disclose Personal Data to the following **third parties** in Luxembourg, in the countries where CS Luxembourg Branches are established or abroad:
- legal counsels – in particular, in the context of pending or reasonable foreseeable legal proceedings (including complaints to authorities), as the case may be, against the Bank or initiated by the Bank
- public notaries – in particular, for mortgage transactions and inheritance-related cases
- other professional advisors and external auditors

all being subject to confidentiality and/or professional secrecy obligations.

3. Other recipients of Personal Data

Other recipients of Personal Data can be any units for which you have released us from professional secrecy by means of **a separate consent**.

CREDIT SUISSE

Extract from the Client Information Booklet
Appendix 6

Additional Data Protection Information
Relating to the Branches of CREDIT SUISSE (LUXEMBOURG) S.A.

Preamble

The Data Protection Information issued by the Bank including the Appendix 5 ("**List of Data Recipients**") ("**Data Protection Information**") applies accordingly, with the deviations referred to below, to Personal Data processing operations relating to the Client and other Affected Persons, as the case may be, conducted in the context of a business relationship between the Client and a respective Branch of the Bank ("**Branch Client Relationship**"):

Credit Suisse (Luxembourg) S.A., Succursale en France
86 Boulevard Haussmann
CS 40047
75008 Paris
France
Phone: +33 (0)1 70 39 00 00
Fax: +33 (0)1 70 39 04 30
(hereinafter referred to as "the **France Branch**"),

Credit Suisse (Luxembourg) S.A., Nederlandse Vestiging
1071 DC, Amsterdam
The Netherlands
Phone: +31 (0) 20 606 8000
Fax: +31 (0) 20 606 8001
(hereinafter referred to as "the **Netherlands Branch**"),

Credit Suisse (Luxembourg) S.A., Sucursal em Portugal
Avenida da Liberdade, n.º 180-A, 8.º andar
1250-146 Lisboa
Portugal
Phone: +351 21 310 92 10
Fax: +351 21 310 92 11
(hereinafter referred to as "the **Portugal Branch**"),

Credit Suisse (Luxembourg) S.A., Ireland Branch
Kilmore House, Park Lane, Spencer Dock
Dublin 1
Republic of Ireland
Phone: +353 1 523 5913
(hereinafter referred to as "the **Ireland Branch**"),

hereinafter referred to as "**Branch(es) (of the Bank)**".

CREDIT SUISSE

The variations set herein are as follows:

1. In the context of the Branch Client Relationship, on the basis of the established service provisioning model whereby services are provided jointly by the respective Branch responsible for the overall relationship management and the Bank, in particular, for the maintenance and management of Client accounts, **the respective Branch and the Bank** will act as **joint data controllers** in relation to the Client's or any Affected Person's (as the case may be) Personal Data processed in the context of such Branch Client Relationship.

2. This Appendix 6 forms an **integral part** of the Data Protection Information.

3. All references to "legal" or "statutory" obligations included in the Data Protection Information and Appendix 5 shall be deemed to include all legal, regulatory and/or statutory obligations to which the respective Branch is subject under the laws or regulations of the relevant jurisdiction.

4. The Branches will transfer, disclose or share Personal Data relating to the Branch Client Relationship to/with the Bank on a need-to-know basis. For details regarding **Data Recipients** outside the Bank and the Branches, please see the Appendix 5 ("**List of Data Recipients**").

5. Personal Data will be processed by the respective Branch of the Bank for as long as it necessary for the purposes described in section 3 of the Data Protection Information. In addition to the obligation to preserve records the Bank is subject to, as described in section 7 of the Data Protection Information, the Branches of the Bank may be subject to the Data **retention requirements** applicable in **the respective jurisdictions**, and the Branches of the Bank need to comply with obligations to preserve records according to **local civil, commercial and tax laws,** as well as **financial sector laws and regulations**:

- the **France Branch**: In line with respective provisions in the French Civil Code and the French Commercial Code, in general the France Branch keeps Client and Affected Persons' Personal Data for a time period of maximum 10 years upon termination of the business relationship. However, in some limited situations, as per specific French Civil Code provisions, in case of postponement of the applicable statute of limitations, suspension, or interruption of such statute of limitations, a maximum period of 20 years period applies, starting from the date when the right was born.

- the **Portugal Branch**: Portuguese commercial and tax legislation in general set the obligation to maintain records for the purposes of accounting, administration and tax management for a period of 10 years. This relates to Client and Affected Persons' Personal Data upon termination of the business relationship. Other deviating minimum and maximum retention periods can apply.

- the **Netherlands Branch**: In line with the Dutch Civil Code and the State Taxes Act, in general, the Netherlands Branch keeps Client and Affected Person's Personal Data for a time period of maximum 7 years upon termination of the business relationship, or from the moment the underlying agreement has lost its actual value. Other deviating minimum and maximum retention periods can apply.

- the **Ireland Branch**: There is an obligation to maintain records for a period of not less than 5 years after the date on which the Ireland Branch ceases to provide services to the Client or the date of the last transaction with the Client (if any), whichever is the later. Other deviating legal obligations may apply, which might require the Ireland Branch to keep records for a longer period of time.

The fact that **legal holds** can be faced which might trigger a requirement to keep records for a longer period of time, as explained in section 7 of the Data Protection Information, may also apply to **the respective Branch** in the context of Branch Client Relationship.

6. In order to exercise the **data subjects rights** described in section 8 of the Data Protection Information, you may reach out to contact persons listed in the Data Protection Information. In addition, you have a right to lodge a complaint with the **respective Data Protection Authority**:

- in **Portugal** – the *Comissão Nacional de Protecção de Dados (CNPD),* https://www.cnpd.pt
- in **France** – the *Commission Nationale de l'Informatique et des Liberté (CNIL),* https://www.cnil.fr
- in **the Netherlands** – the *Autoriteit Persoonsgegevens*, https://www.autoriteitpersoonsgegevens.nl.
- in **Ireland** – the *Data Protection Commissioner,* https://www.dataprotection.ie.