

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>



Table of Content

1.	Who Is Responsible For Data Processing and How Can You Contact Them?	4
2.	What Sources and Data Do We Use?	4
3.	What Do We Process Your Personal Data for (Purpose of Processing) and On What Legal Basis?	7
4.	Who receives Your Data?	7
5.	Will Data Be Transferred to a Third Country or an international organization?	7
6.	Use of electronic means of communication	7
7.	For How Long Will Your Data Be Stored?	7
8.	What Data Privacy Rights Do You Have	7
9.	Are You Obligated to Provide Data?	8
10.	To What Extent Is There Automated Decision-Making?	8
11.	Will Profiling Take Place?	8
12.	May we collect biometric Data from You?	9
<hr/>		
	Appendix 5	10
	Appendix 6	13

Data Protection Information

With the following information, we would like to give an overview of how we will process Your Data (as defined below) 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.

“You” and **“Your”** as used in this information refers to individuals (*and/or legal entities for the purpose of professional/banking secrecy only*):

- who themselves are our Clients; or
- who are involved in the business relationship, as the case may be, such as authorized representatives, persons 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”**); or
- with whom we come into contact, or in respect of whom we obtain personal data, in the usual course of dealings with You, our service providers, and our other business counterparties or transaction participants, which may include, without limitation, employees, directors, officers, beneficial owners and other personnel of such clients, service providers, business counterparties or transaction participants, in all cases outside the Credit Suisse Group (as applicable to You, **“Your Organization”**).

“Data Protection Legislation” means any law and/or regulation (including guidance and codes of practice issued by authorized data protection regulators) which is applicable to the processing of Your personal data by us, and which shall include, but is not limited to the EU General Data Protection Regulation (2016/679) (“GDPR”) and applicable EU member states’ national legislation amending and/or supplementing the GDPR.

1 Who Is Responsible For Data Processing and How Can You 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 (as defined below), 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
Email: luxembourg.data-protection@credit-suisse.com

or

CREDIT SUISSE SERVICES AG, LONDON
BRANCH
Credit Suisse Group Data Protection Officer
Five Canada Square
London E14 5AQ
Great Britain
Phone: +44 20 7888 8888
Email: data-protection@credit-suisse.com,

(hereinafter referred to as **“Data Protection Office”**)

2 What Sources and Data Do We Use?

Data from You:

We process **Personal Data** (also referred to as **“Data”**) about You, as defined below, that we obtain from You in the context of our business relationship with You (as applicable). We do this in order to facilitate, enable and/or maintain that relationship and/or to provide services to You or for other reasons specified below. In addition, in carrying on our business relationship with You, information may be collected about You by other means (e.g. recording of telephone calls, email communication journaling). In these circumstances, the information is not accessed on a continuous or routine basis.

Data from other sources:

We also process personal data about You that we obtain from publicly accessible sources (e.g. commercial registers, press including trade

press or paid for content, publicly available websites and other publicly available sources of information such as sanctions lists or lists of directors disqualifications) or that is legitimately transferred to us by other companies in the Credit Suisse Group or from other third parties. These may include third parties not related to You, such as settlement service providers, central securities depositories, exchanges, central clearing counterparties and other similar entities, databases, and third party service providers such as professional advisers, insurers and risk consulting firms.

Types of personal data:

The types of personal data we process may include, without limitation:

- identification details relating to You (*name/company name, date and place of birth/date and place of incorporation, nationality, gender, domicile/registered office*)
- contact details, including private and/or business phone numbers, postal and email addresses
- identification data such as passports, *bylaws and extract of commercial register*, National Insurance or Social Security numbers, driving license, ID cards, property register identification, social network user names, customer identifiers (CIF, IBAN/BIC), relationship identifiers (e.g. client segment and account currency), photographs
- authentication data such as sample signatures
- marital status, name of spouse, number of children (if applicable)
- tax status (e.g. tax ID)
- order data (e.g. payment data and account information)
- data from the fulfilment of our contractual obligations
- information about Your financial situation (e.g. source of wealth, incomes, benefits, mortgage information, shareholdings)
- video surveillance and telephone/audio recordings
- data relating to criminal convictions and offences (including excerpts of criminal register)
- data related to designation of Your status as a politically exposed person (PEP) and related information
- marketing and sales data (e.g. customer relationship documentation)
- data relating to Your habits and preferences
- dietary and access requirements (e.g. for event organization purposes)

- data from Your interactions with us, our branches, our internet websites, our apps, our social media pages, meetings, calls, chats, emails, interviews and phone conversations
- documentation data (e.g. file notes or meeting minutes from a consultation, client needs and product usage)
- data relating to Your current and past professional roles and employment, and education (e.g. corporate title, membership of professional associations or bodies, career histories or biographies, job function, knowledge and experience in investment matters, qualifications and skills)
- other data similar to the broad categories mentioned above

(“Personal Data” or “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, organization, 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 Your Personal Data for (Purpose of Processing) and On What Legal Basis?

We process Personal Data in accordance with the provisions of the Data Protection Legislation on the following legal grounds:

a) if processing of Personal Data is necessary for the fulfilment of contractual obligations

We may process Your Personal Data in order to **maintain our business relationship with You in accordance with our legal agreement(s) with You**. Such processing may take place in order to carry out obligations or exercise rights we may have pursuant to the legal agreement(s) with You, to take steps necessary in order to conclude a legal agreement with You or to take other steps at Your or Your representative's request prior to entering into a legal agreement with You. If You are our client, the level and nature of processing of Your Personal Data that we may carry out pursuant to this paragraph will likely depend on the specific product or service to be provided to You (and can include needs assessments and other assessments to provide advice and support to You, as well as to carry out transactions contemplated in, or necessary to fulfil, such legal agreement). You may find further details about the purposes of Data processing in the relevant contractual documents and/or the GTC.

b) Due to legal obligations

We are subject to various **legal and regulatory obligations**, including without limitation prudential and conduct regulation of banks, as applicable, regulation of financial markets, compliance with any court orders, investor protection regulations, securities regulations, laws relating to money laundering, terrorist financing, sanctions and any tax laws.

The purposes of processing may include, without limitation:

- identity checks, fraud and financial crime and market abuse prevention or detection. If fraud is detected, certain services may be refused.
- fulfilling control and reporting obligations under applicable financial regulations including securities regulations
- fulfilling requirements related to our licenses and regulatory permissions
- complying with investor protection or conduct of business regulation (such as carrying out suitability or appropriateness assessments)
- complying with regulatory record keeping obligations
- complying with regulatory obligations in relation to measuring and managing risks within the Credit Suisse Group.

c) For purposes of legitimate interests

We may process Your Personal Data for the purposes of the **legitimate interests** pursued by the Bank, Branches of the Bank or a third party, for example in:

- developing, deploying and supporting our products and services
- developing and furthering our business and business relationships, and keeping our clients and other stakeholders satisfied
- protecting our businesses and the integrity of the financial markets
- assessing, managing and reporting risk efficiently and effectively
- securing our systems, assets, infrastructure and premises
- exercising and defending our legal rights and position anywhere in the world
- complying with legal and regulatory obligations and cooperating with regulatory, judicial and other authorities and bodies around the world
- supporting other Credit Suisse companies in pursuing the above interests.

The purposes for which we may process Your Personal Data (in connection with the above interests) include the following without limitation:

- carrying on business relationships with clients and other parties
- providing services to clients
- performing obligations and exercising rights under and otherwise carrying out contracts, or taking pre-contractual measures with You or a third party
- management of the businesses and further development of services and products
- reviewing and optimizing procedures for needs assessment for the purpose of direct client discussions
- marketing or market and opinion research
- obtaining personal data from publicly available sources for client acquisition/review purposes
- compliance with licensing, permission and/or licensing exemption requirements and regulatory requests or guidance related to such licenses, permissions or exemptions
- compliance with applicable laws, regulations and judicial orders outside Luxembourg and/or the Branch locations
- compliance with regulatory guidance, policy statements, best practice and associated policy requirements and controls in connection with the carrying on business
- facilitation of and responding to, regulatory requests and supervisory visits, and otherwise acting in open and collaborative manner with competent regulatory authorities
- prevention of and investigations related to financial crime, including fraud, financing of terrorism and money laundering, and compliance with sanctions, including know your customer (KYC) and regular politically exposed persons (PEP) screening
- asserting legal claims and defenses in legal disputes
- carrying out conflict checks
- handling client complaints
- facilitating operational actions in connection with our business relationships (e.g. processing of payments, billing)
- validating the authority of signatories (e.g. when concluding agreements and transactions)
- risk control across Credit Suisse Group
- consulting with credit rating agencies to investigate creditworthiness and credit risks where we may have an exposure to You

- securing and operating Credit Suisse Group's IT systems
- video surveillance and measures to protect the rights of an owner of premises to keep out trespassers and to provide site security (e.g. access controls)
- performance of contracts (e.g. in respect Data of Affected Persons or Your Organization's personnel).

Whenever we intend to rely on legitimate interest as the legal basis for the processing of Personal Data, we will give due consideration to Your rights and freedoms.

d) **As a result of Your consent**

There may be circumstances where we ask for **Your consent** to process Your Personal Data. As long as You have granted us this consent, this processing is legal on the basis of that consent. You can withdraw Your consent at any time by contacting the Data Protection Office (see section 1 above). Withdrawal of consent does not affect the legality of Data processed prior to withdrawal.

4 Who receives Your Data?

Within the Bank, every unit that requires Your Data will have access to it in order for the Bank to achieve purposes described in section 3. As regards to Clients serviced by the Branches of the Bank, the Bank processes Your Data and shares such Data with the Branches to which the Data relates and vice versa on a need to know basis. In this respect, the Bank and its respective Branch act as joint Data Controllers. 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 GTC). 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"**.

5 Will Data Be Transferred to a Third Country or an international organization?

In certain circumstances, we may transfer Your Data to Data Recipients located in **third countries** (countries outside the European Economic Area). You understand that the data protection legislation in such third countries may not give You as much protection as the data protection legislation in the country where You are located.

For transfers to third countries which have not been determined by EU Commission as countries offering an adequate level of data protection, we will either rely on a derogation applicable to the specific situation (e.g. if the transfer is necessary to perform our contract with You such as when making an international payment), or implement standard contractual clauses approved by the EU Commission to ensure the protection of Your Personal Data.

Please contact our Data Protection Office if You would like to request to see a copy of the specific safeguards applied to the export of Your Data. Contact details are provided in section 3 above.

6 Use of electronic means of communication

The Bank may use any means of communication, including electronic means such as email, 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 GTC.

7 For How Long Will Your Data Be Stored?

We will process and store Your Personal Data **for as long as it is lawful** for us to do so. 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.

We will normally retain Your records for a minimum of ten years to comply with legal, regulatory and contractual requirements (for example Luxembourg Commercial Code and Law of 5 April 1993 on the financial sector, as amended), unless there is a particular reason to hold the records for longer, including legal hold¹ requirements, which require us to keep records for an undefined period of time.

8 What Data Privacy Rights Do You Have?

In relation to Your Personal Data, and to the extent permitted under the Data Protection Legislation You have the right:

- to request access to Your Personal Data
- to request the rectification of inaccurate or incomplete Personal Data

- to request deletion of Your Personal Data
- to request the restriction of the processing of Your Personal Data
- to data portability.

In addition to the above rights, you have the **right to object** at any time to:

- the processing of Your Personal Data for direct marketing purposes, and profiling to the extent related to direct marketing and
- the processing of Your Personal Data for the reasons set out in section 3 c) ("legitimate interest") of this statement (including profiling for these purposes), to the extent permitted under the Data Protection Legislation.

To exercise any of the above rights You do not need to use a particular form but you should write to our Data Protection Office in accordance with section 1 of this statement. We will then assess and respond to Your request to exercise Your rights.

Please note that some of the above rights are subject to limitations in some situations, and that the exercise of the above rights may affect our ability to continue a business relationship with You.

If applicable, You also have a right to make a complaint to the competent supervisory authority.²

You may also withdraw the consent granted to us for the processing of Your Personal Data at any time by contacting the Data Protection Office (see section 1 above). Please also see section 3 d) for further details on consent.

9 Are You Obligated to Provide Data?

In the context of our business relationship, You may need to provide certain Personal Data that is required for accepting and carrying out a business relationship, fulfilling contractual obligations or that we are legally obliged to collect. **Without this Data, we may not be in a position to enter into a legal agreement, provide services, or initiate or maintain a business relationship.** For example, anti-money laundering regulations may 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 and documents in accordance with such regulations, and to 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 require.

10 To What Extent Is There Automated Decision-Making?

In establishing and carrying out a business relationship, we generally do not use any fully automated decision-making pursuant to the Data Protection Legislation. If we use this procedure in individual cases, we will inform You of this separately, provided 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).

For example we use profiling in the following ways:

- Due to legal and regulatory requirements, we are required to combat money laundering, terrorism financing, fraud, assess risk and offences that pose a danger to assets. 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.

¹ 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.

² Luxembourg data protection authority: *the Commission nationale pour la protection des données* (CNPDP) (<https://cnpdp.public.lu>).

12 May we 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.

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 Your Data 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.

2. Data Recipients outside the Bank

2.1 Within the Credit Suisse Group

In the context of outsourcing of certain functions, to ensure an efficient servicing of our Clients, to comply with legal and/or regulatory requirements and/or to pursue legitimate interests of the Bank and/or Credit Suisse Group we will share or otherwise process Your Data with the following Credit Suisse Group entities.

The following data sharing scenarios between the Bank and Credit Suisse Group entities 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 the relevant Credit Suisse Group entities 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 the relevant Credit Suisse Group entities.

2.1.1 Credit Suisse AG, Credit Suisse (Switzerland) Ltd., Credit Suisse Services AG (“CREDIT SUISSE CH”)

a) Processing of Data in the context of the outsourcing of certain functions and support activities

The Bank may use the information technology (IT) platform of CREDIT SUISSE CH in Switzerland (“Swiss IT Platform”) for certain operational activities including online banking services entailing the processing of Your Data (e.g. storage) on the Swiss IT Platform.

The Bank may furthermore outsource certain operational activities related to the following purposes and/or functions to CREDIT SUISSE CH entities, such as:

- operational tasks and processes
- compliance (e.g. anti-money laundering) (including data quality assessment)
- risk assessment and/or risk management (for example credit risk management)
- reporting (e.g. Client, regulatory, management)
- internal supervision, internal investigations and audit
- marketing and client event management
- including the related use of the Swiss IT Platform.

Accordingly, dedicated persons and/or teams of or at the service of CREDIT SUISSE CH will have access to Your Data on the Swiss IT Platform as well as process such Data on a need-to-know basis. It may also be required for the Bank to provide Your Data to CS CH by other means than via the Swiss IT Platform.

Further, the Bank’s email infrastructure and online banking applications are operated by CREDIT SUISSE CH. Your Data could therefore be viewed by employees of CREDIT SUISSE CH for maintenance purposes. Emails received and sent by the Bank (e.g. emails received from and sent to Clients or emails 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 CREDIT SUISSE CH. Communication Journaling means that unalterable copies of emails are stored in a strictly confidential internal “Journaling Repository”.

The Bank may outsource the function of the Group Data Protection Officer and related support activities to CREDIT SUISSE CH entities.

b) Processing of Data to comply with legal/regulatory requirements and/or to pursue legitimate interests of the Bank and/or Credit Suisse Group

Your Data is furthermore processed (e.g. stored) by CREDIT SUISSE CH, to the extent required in order to enable CREDIT SUISSE CH and/or the Bank to comply with regulatory (reporting) requirements and/or for operational purposes, data quality assessment, risk assessment and/or management (e.g. credit risk), internal supervision and investigations, audit, compliance (e.g. anti-money laundering), Client event management, reporting (e.g. Client, regulatory, management) and/or IT purposes. Accordingly, dedicated persons and/or teams of or at the service of CREDIT SUISSE CH will have access to Personal Data as well as process such Personal Data on a need-to-know basis.

2.1.2 Credit Suisse Services AG, London Branch

The Bank may outsource the function of the Group Data Protection Officer and related support activities to Credit Suisse Services AG, London Branch.

The Bank may further use the services of Credit Suisse Services AG, London Branch for the purposes of internal supervision and investigations.

Accordingly, dedicated persons and/or teams of or at the service of Credit Suisse Services AG, London Branch will have access to Personal Data as well as process such Personal Data on a need-to-know basis.

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

CREDIT SUISSE CH may sub-outsource certain tasks to Credit Suisse (Poland) Sp. z o.o. or any other Credit Suisse company in Poland, as the case may be, ("**CREDIT SUISSE Poland**"), in which case CREDIT SUISSE CH may be required to disclose Your Data to CREDIT SUISSE Poland. In such cases, Your Data may be processed by CREDIT SUISSE Poland.

The Bank may also directly outsource certain activities to CREDIT SUISSE Poland (e.g. relating to operational processes, compliance (e.g. anti-money laundering), risk assessment and/or management (e.g. credit risk management), internal supervision, reporting, audit and/or IT). Such outsourcing may require dedicated persons and/or teams of or at the service of CREDIT SUISSE Poland to obtain access to the IT systems used by the Bank and/or client data systems in Luxembourg, including access to Your Data on a need-to-know basis.

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 – if applicable through its service providers – may be required to transfer Your Data to **other financial service institutions or comparable institutions and/or authorities**, in Luxembourg, in countries where Branches and/or the service providers of the Bank are established or abroad. Depending on the transaction/service Data Recipients may include other entities of the Credit Suisse Group, other banks (e.g. correspondent banks), operators of payments systems, credit card service providers, sub-custodians and their service providers or processing units, issuers and/or other target investments and their service providers, brokers, (stock) exchanges, processing units, (proxy) voting (advisory) service providers, central securities depositories, clearing institutions and the Society for Worldwide Interbank Financial Telecommunication ("**SWIFT**"). Such disclosure may be required to third parties to whom the Bank or any CREDIT SUISSE Luxembourg Branch has a reporting obligation (e.g. trade repositories, authorities or (stock) exchanges, central (regulatory) registers) 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, Your 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 Your 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), search engines, internet platforms and/or with third party providers for the purpose of investigating creditworthiness, credit risk and solvency (in particular, in credit business) and/or for the purpose of gathering information for regulatory 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.

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 CREDIT SUISSE 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 In connection with the outsourcing of certain activities to CREDIT SUISSE CH Entities, CREDIT SUISSE CH Entities may further outsource certain IT support activities requiring access to limited Personal Data (e.g. maintenance, development) to third parties, namely Q-Perior AG, Switzerland (or any successor entity) in relation to a fee calculation software

2.2.5 We may use external service provider(s) ("**Third Party Service Providers**"), located in Luxembourg or in the countries where CREDIT SUISSE 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 CREDIT SUISSE 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.

We may use Third Party Service Providers providing messaging functionalities located in Luxembourg, Switzerland or abroad to enable a secure communication with You and/or within the Credit Suisse Group entities (e.g. by way of **Secure Email**.)

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

2.2.6 The Bank may be required to disclose Personal Data to the following third parties in Luxembourg, in the countries where CREDIT SUISSE Luxembourg Branches are established or abroad:

- legal counsels – in particular, in the context of pending or reasonably 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 (e.g. tax advisors, external evaluators) 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**.

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)**”.

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>

Important Information

This document has been produced by CREDIT SUISSE (LUXEMBOURG) S.A. ("Credit Suisse") with the utmost of care and for information purposes only. This document and the information provided therein are for the exclusive use of the intended recipient. This document does not constitute or contain an offer or invitation to enter into any type of financial transaction.

Neither this information nor copies of it may be sent to, taken into, or distributed in the United States or distributed to any US person (within the meaning of Regulation S of the US Securities Act of 1933 in its applicable form). This document may not be reproduced, either in part or in full, without the written permission of Credit Suisse.

Copyright © CREDIT SUISSE (LUXEMBOURG) S.A. All rights reserved.

**CREDIT SUISSE (LUXEMBOURG) S.A.**

Registered office: 5, rue Jean Monnet, L-2180 Luxembourg

R.C.S. Luxembourg B 11756

Contact:

Postal address: P.O. Box 40, L-2010 Luxembourg

Phone: +352 46 00 11-1

Fax: +352 46 32 70

Version: July 2019

www.credit-suisse.com