PRIVACY STATEMENT

WHAT IS THIS STATEMENT ABOUT?

The Bank collects, processes and stores Personal Data (as defined below) in relation to the client (the client himself/herself or, if the client is a legal person, the investors, shareholders, the ultimate beneficial owners, the officers, the authorised representatives, any User and any other data subject related to the client, together the "Data Subjects") in compliance with any data protection law applicable in Luxembourg and in particular the law of 2 August 2002, as modified, and as from 25 May 2018, the Regulation (EU) 2016/679 of 27 April 2016 ("GDPR"), and any Luxembourg implementing act of the GDPR (together the "Luxembourg Data Protection Legislation"). In this respect, the Bank, or any successor thereto, acts as a data controller.

WHO CONTROLS THE CLIENT'S PERSONAL DATA?

The controller of the client's personal data is:

BNP Paribas Wealth Management (Luxembourg) Luxembourg-Kirchberg
Espace Kennedy
46, Avenue J.F. Kennedy
L-1855 Luxembourg-Kirchberg

Phone: +352 2607 1
Email: gdpr_po@lu.abnamro.com
Website: www.wealthmanagement.bnpparibas/lu

DATA PROTECTION OFFICER

The Bank has a designated Data Protection Officer. The Data Protection Officer maintains the application of, and compliance with, the GDPR within the BNP Paribas organisation. This role has been allocated to the Privacy Office (dpo@bgl.lu). If the client has any questions, he should contact the Bank on gdpr_po@lu.abnamro.com.

WHAT IS PERSONAL DATA?

This Privacy Statement is about the use of personal data. But what exactly is meant by personal data? Personal data is information about the client as a person, such as his name, street address or email address, his age and his date of birth. Personal data also includes the client's bank account number, his phone number, his IP address and his social security number. This data says something about the client. The same goes for biometric data, such as the client's voice, fingerprint or behaviour.

Some data is highly sensitive, so much so that the law imposes strict requirements on the use of this data. This concerns special personal data, which include data about the client's health, offences or crimes he may have committed, or his sexual orientation. The Bank cannot process such special personal data unless it has to or is allowed to under the law, or the client has given the Bank his explicit consent to do so.

Personal data that may be processed by the Bank comprise:

(i) name, address, contact details, nationality, main business activity, photograph, civil status and family, occupation and work history, hobbies, public life related information, financial situation, credit related information, account information, telephone conversations and any type of electronic communications such as letters, emails and fax messages, tax identification number and any related tax information, national identification number, authenticating data, MiFID identifier, financial objectives, knowledge and experience in financial investment services, credit products and in any product or service offered by the Bank and any other information that has been provided by the client or the Data Subjects;

(ii) transactions performed in the client's account with the Bank or contemplated transactions, contracts entered into with the Bank and any other information related to the client's banking relationship with the Bank;

(iii) any information relating to the client or the Data Subjects resulting from the KYC/ AML checks carried out by the Bank pursuant to the modified law of 12 November 2004 relating to the fight against money laundering and terrorist financing;

(iv) any information relating to the client or the Data Subjects that may identify, directly or indirectly the client or the Data Subjects.

(together the "Personal Data").

DOES THE BANK USE ANY PERSONAL DATA FROM OTHER SOURCES?

The Bank effectively uses personal data that it obtained from sources other than the client himself. To illustrate: if the client's partner applies for a loan and the client co-signs the application, the Bank may have to ask for the client's personal data. But it may also decide to consult other sources, including:

- Public registers that contain the client's personal data, such as company registers, UBO and shareholders registers and similar;
- Public sources such as newspapers, the internet and social media that are not protected by privacy settings;
- Data files from other parties that have collected information about the client, such as external marketing
firms, risk management solutions like Worldcheck or credit agencies.

ON WHAT BASIS DOES THE BANK PROCESS THE CLIENT'S PERSONAL DATA?

The Bank can only ask the client to provide or use the client's personal data for a reason. This is referred to as 'a basis for processing' in the law. The Bank uses the client's personal data for one or more of the following reasons:

(i) for the performance of the contracts entered into between the client and the Bank and the provision of the services subscribed by the client, or

(ii) to take steps at the request of the Data Subject prior to entering into a contract. The Bank uses the client's personal data so that it can conclude agreements with the client and meet its obligations under these agreements. The Bank concludes an agreement with the client, for instance, if the client wants to open a bank account with the Bank or take out a mortgage. The Bank needs to know all sorts of things about the client before it can transfer the money to him, or

(iii) for compliance with legal and regulatory obligations to which the Bank is subject (including but not limited to the obligations arising under the law of 18 December 2015 relative to the automatic exchange of information regarding the financial accounts in the field of taxation, under the law of 24 July 2015 relative to the Foreign Account Tax Compliance Act (FATCA), as modified, and under the MiFID Regulations). The Bank processes the client's personal data because the law requires this of the Bank. Under the law, the Bank is expected to learn as much about the client's financial position as possible to make allowance for any changes that may affect the client. The Bank also needs to take steps to prevent fraud, tax evasion, terrorist financing and money laundering. This obligation also requires the Bank to verify the client's identity so that the Bank can prove that it knows who the client is. That's why it keeps a copy of the client's valid ID on file, or

(iv) for the performance of a task carried out in the public interest, namely carrying out monitoring measures with respect to the client pursuant to the modified law of 12 November 2004 relative to the fight against money laundering and terrorist financing, or

(v) for satisfying the Bank's legitimate interests. For the legitimate interest to apply, the Bank's interest in using the client's personal data must effectively outweigh the client's right to privacy. In situations such as these, the Bank considers every possible interest. When does the Bank have a legitimate interest in using the client's personal data?

Examples:

- Protecting the client's and the Bank's property and personal data and that of others;
- Protecting the Bank's own financial position, for instance when it comes to loan repayments and protecting the interests of other clients;
- Seeking maximum efficiency (including administrative, organisational and IT efficiency) in the internal organisation of the Bank and the group of companies to which the Bank belongs ("BNP Paribas Group"), supporting efficient and effective management of the BNP Paribas Group and performing contracts in the interest of the client's investors, shareholders and ultimate beneficial owners.

There may also be situations in which another person may have a legitimate interest for which the Bank needs to use the client's personal data, for example when someone has accidentally transferred money to the client's bank account. In some instances, the Bank then has the right to provide the client's personal data to the person who transferred the money so that he or she can contact the client to rectify the situation, or

(vi) as far as necessary, on the basis of the client's consent.

The Bank usually uses the client's personal data because it needs to in the context of the agreement it has concluded or wants to conclude with the client, or because the law tells the Bank to use the client's personal data, or because the Bank or a third party has a legitimate interest in using the personal data. In these instances, the Bank won't ask for the client's consent. The law allows the Bank not to do so.

There may be cases in which the Bank needs to ask for the client's consent separately in order to use the client's personal data. The client should read the information the Bank gives the client about using his personal data carefully before the client gives the Bank his consent. The client can also withdraw his consent if he no longer wants the Bank to use his personal data. The client can withdraw his consent by sending an e-mail to gdpr_po@lu.abnamro.com. The client can only withdraw his consent if the Bank asked for his consent earlier. Please note that the client does not have this right if the Bank uses his personal data on the grounds of other potential bases (see also 'On what basis does the Bank process the client's personal data?').

The Bank always asks for the client's consent before it processes special personal data, unless the law requires it to process certain special personal data or allows it to process special personal data in particular cases.

Instances in which the Bank will ask for the client's consent:

1. If the Bank makes use of cookies and similar technologies.

2. If the Bank uses profiling if required by law.

3. To the extent that the Bank shall be legally required to obtain the client's consent with regard to certain types of processing, the client will be invited to complete and sign a declaration of consent. In case the client does not agree to sign the declaration of consent, either the client, without prior notice, or the Bank, with the prior notice foreseen in clause 18 of the Bank's General Terms and Conditions, may (without being obliged to) terminate the banking relationship.

FOR WHAT PURPOSES MAY THE BANK USE THE PERSONAL DATA:

The Bank shall process Personal Data to enable the Bank to process the client's payment instructions, to assess and accept the client and to manage client relationships, to manage accounts, loans, credit cards, investment services and related products and services, to execute transactions of any kind; to enter into and execute agreements with the client, to prevent misuse and fraud, to secure communication channels; to perform analysis and establish statistics and tests with respect to Personal Data; to manage risks, disputes, collections, debt recovery, complaints and litigations; to demonstrate business transactions and communications, to develop commercial offers; to manage transactions surveillance and monitoring and comply with legal obligations to have adequate and professional systems in place in respect of relevant local and European laws and reporting obligations; to conduct a risk assessment as prescribed by applicable legal provisions by collecting and archiving required documentary evidence regarding the identity and business activity; to conduct a risk management control and global supervision of risk exposure on a real time basis; to comply with any regulatory obligations from national regulators and from the European Central Bank; to enable the client to make use of a state-of-the-art IT system for its banking operations and in general to comply with all relevant EU and local rules and regulations applicable to the Bank, such as (without limitation) concerning the fight against the money laundering and terrorism financing, exchange of tax information, MiFID II, Payment Services Directive II etc.

(together the "Purposes").

DOES THE BANK USE THE CLIENT'S PERSONAL DATA FOR OTHER PURPOSES THAN FOR WHICH IT WAS INITIALLY PROVIDED?

The Bank has the right to use the client's personal data for other purposes than for which he initially provided it to the Bank. This is, however, subject to the condition that the new purpose must be in line with the purpose for which the client initially provided his personal data to the Bank. The law refers to this principle as 'compatible use of personal data's. The law does not specify exactly when a use is compatible, although it does provide referencepoints for when the use of personal data is either compatible or not.

The Bank will first assess whether it has the right to reuse the client's personal data based on the law looking at the following reference points:

- Is there a clear correlation with the purpose for which the client initially provided the personal data? Is the new purpose appropriate to the initial purpose?

- How did the client originally provide the personal data to the Bank ? Did the client provide the personal data himself or did the Bank obtain it from a different source?

- What kind of personal data are we talking about exactly? Does it concern highly confidential information or it is not as sensitive?
- What would be the implications for the client if the Bank were to use the personal data for a different purpose? Would the client benefit, suffer or neither?
- What can the Bank do to protect the client's personal data as best it can if it re-uses it, for instance by rendering it anonymous or encrypting it?

USE OF THE CLIENT'S PERSONAL DATA FOR DIRECT MARKETING PURPOSES

The Bank wants to offer the client relevant products and services that suit his needs. To make this happen, the Bank uses the personal data the client has provided to the Bank and personal data from other sources (see also 'Does the Bank use any personal data from other sources?').

If the Bank uses the client's personal data for direct marketing purposes, the client has the right to object.

PROFILING

The Bank uses profiling for fraud prevention, investigations into unusual transactions, risk management and client acceptance, and for administrative purposes (for instance to determine what service model or category applies to the client under Mifid II), for (direct) marketing purposes and for security purposes.

Profiling and fraud prevention

The Bank has a wealth of knowledge and experience in the area of fraud prevention. The Bank is faced with increasingly sophisticated types of fraud. By observing how money is used to commit fraud, the Bank learns what conduct or circumstances lead to a certain type of fraud. The sum of the characteristics the Bank observes when a certain type of fraud is committed adds up to a profile. This profile is used to identify activities that meet those characteristics. Activities that are identified through this procedure are subjected to further investigation. The Bank can then take measures to prevent fraud as well as it possibly can or – if fraud has been committed – hand the case over to the competent authorities.

Unusual transactions

The Luxembourg Anti-Money Laundering and Counter Terrorist Financing Laws dictate that the Bank pays special mind to unusual transaction patterns and activities and to transactions that – by their nature – result in a relatively high risk of money laundering. If the Bank qualifies transactions or activities as unusual within the meaning of the law, these transactions must be reported to the authorities. To do so, the Bank is required to prepare and keep a client risk profile so that transactions that don't match with the knowledge the Bank has about the client and their risk profile are identified and reported where needed.

Risk management

Regulators expect Banks to make a greater effort to put a stop to excessive lending or to take faster action when clients are threatening to run into financial trouble. The Bank can also use profiling techniques to identify such instances. The Bank can first make a list of the most common characteristics of clients who find themselves in financial difficulties. The sum of these characteristics adds up to a profile. The Bank checks whether it has any clients that meet this profile. The Bank could then determine which actions need to be taken to help clients that show these characteristics.

Client and product acceptance

The Bank may use profiling if the client wants to buy a product, for instance to make a risk assessment as part of a loan application. Banks know from experience that certain aspects may serve as indicators of the creditworthiness of a client or a potential client. These aspects include whether or not a client has a job or another form of income or whether or not they have any debts and so on. The Bank will consider these aspects if the client applies for a loan. Clients who have no trouble meeting their payment obligations share a number of characteristics based on which a profile is put together. Applying this profile to a loan applicant gives the Bank an indication of the applicant's potential risk of default.

The Bank does this for new clients as well as for existing clients who want to buy additional products or services.

At the on-boarding of new clients, the Bank might apply risk parameters to profile (prospect) clients resulting out of risk assessments and apply due diligence measures in accordance with the risk rating of clients. This is in accordance with the Luxembourg Anti-Money Laundering and Counter Terrorist Financing Laws.

Profiling and direct marketing

The Bank also makes use of profiling to send the client offers that meet his needs. If the client has contracted a mortgage from the Bank earlier, the Bank does not want to make him an offer for a product he already has. So, the Bank first thinks about the characteristics a potentially interested client may have. The Bank looks at such aspects as whether a client has taken out a mortgage earlier, or whether a client has bought other products from the Bank, and so on. The Bank will only select clients who have a certain profile for the relevant marketing campaign. Before the Bank uses profiling, it makes sure that its use meets the Bank's privacy rules.

Right to object to profiling

In some cases, the client has the option to request that the Bank does not use his personal data for profiling purposes. The Bank does not always have to honour the client's request. The Bank has the right to use profiling in specific instances, for example in the context of fraud prevention, risk management or investigations into unusual transactions. The Bank adheres to the statutory provisions. The client always has the right to object to the Bank's direct marketing activities.

REQUIRED PERSONAL DATA

If the Bank is required by law to process the client's personal data or if the Bank needs it to effectively perform the agreement with the client and the client refuses to provide it, the Bank cannot enter into an agreement with the client. If the Bank needs additional personal data from the client during the term of an agreement and the client does not provide this data, the Bank has the right to terminate its agreement with the client with the prior notice foreseen in clause 18 of the Bank's General Terms and Conditions. The forms the Bank occasionally needs the client to complete tell the client which personal data is required.

The client and in general any Data Subject may at its discretion refuse to communicate certain Personal Data to the Bank, thereby precluding the Bank from using such Personal Data. However, such refusal or preclusion may be an obstacle to the entry into or to the continuation of the relationship between the Bank and the client. The Bank will inform the client in the event the communication of Personal Data would become mandatory under certain circumstances.

CAMERA IMAGES, TELEPHONE CALLS AND (VIDEO) CHATS

The Bank may capture the client on video when he visits the Bank or the client's voice may be recorded when the client calls the Bank. The law allows the Bank to do so subject to conditions; video images are allowed, for instance, in the context of safety and security. The Bank can record telephone calls if the law dictates that it keeps recordings or if the Bank uses recordings to improve its services. The recording may be used in court or other legal proceedings with the same value in evidence as a written document. The Bank treats video and audio recordings with due care. They are subject to the same rules as other personal data. The client also has the same rights.

DOES THE BANK SHARE THE CLIENT'S PERSONAL DATA WITH OTHERS?

There are situations in which the Bank needs to provide the client's personal data to others, such as persons and bodies that are involved in the Bank's service provision. If the client transfers money to another bank, his personal data will obviously be provided to that bank. That's inevitable.

The client data, including the Personal Data, are or may be transmitted to the following Addressees (the "Addressees"):

(i) The BNP Paribas Group

(ii) The Bank's lawyers, notaries, bailiffs, external auditors or advisors/consultants etc., in order to comply with its legal obligations and to defend its legitimate interest.

(iii) Third-party service providers that provide IT or other services to BNP Paribas that may be located in countries outside of the European Union for which the European Commission did or did not render adequacy decisions. Depending on the situation, the Bank will enter with the concerned third-party service providers into the relevant contractual clauses or the standard data protection clauses that would be required under the Luxembourg Data Protection Legislation and provided the instructions of the Bank are complied with.

(iv) Public, governmental, administrative or judicial entities in Luxembourg (such as the Administration des contributions directes, Courts, prosecutors, Commission de Surveillance du Secteur Financier, Luxembourg Central Bank, Commission nationale pour la protection des données, etc.) or abroad (such as the European Central Bank, Dutch Central Bank, US Internal Revenue Service, foreign courts or tribunals, etc.).

The list of Addressees can be found on the Internet website of the Bank (www.wealthmanagement.bnpparibas/lu/en/luxembourg.html). This list may be updated from time to time and the client will be duly informed. Client data and Personal Data are shared only on a need-to-know basis and the Addressees that have been engaged by the Bank are required to adhere to the same strict security and technology standards and can only have access to the client data and the Personal Data Subject to confidentiality obligations.

RIGHTS OF DATA SUBJECTS

Right of access, right to rectification, right to be forgotten, right to restriction

Subject to the conditions of the Luxembourg Data Protection Legislation, the client and any Data Subject have a right to access their Personal Data. The Client has the right to obtain from the Bank a confirmation whether or not personal data concerning him are being processed, access to the data and the following information: purposes of the processing, the categories of personal data concerned, the recipients to whom the personal data have been or will be disclosed, the considered period for which the personal data will be stored, the existence of the right for request, rectification, erasure or restriction, the right to complain to a supervisory authority, any available information to the source and the existence of profiling as well as the significance and consequences.

The client and any Data Subject may ask for a rectification of their Personal Data in cases where such Personal Data are inaccurate and incomplete (including when these Personal Data are transferred to a third party including a public or a governmental entity such as the Administration des contributions directes in Luxembourg).

The client has the right to obtain from the Bank the erasure of personal data: when the personal data are no longer necessary to the purposes of the banking relationship with the Bank, when the client withdraws consent, when the client objects to the processing and there are no overriding legitimate grounds, when the personal data have been unlawfully processed and when the personal data have to be erased for compliance reasons with a legal obligation. The Bank cannot always delete it, nor does it always have to honour a request for deleting information, for instance if the law requires the Bank to keep the client's personal data for a longer period of time.

The client and the Data Subject can ask the Bank to temporarily restrict the Bank's use of their personal data. The client and the Data Subject can do that if they think that their personal data is incorrect, the Bank is not supposed to use their personal data or when the Bank wants to destroy their personal data, but they need it (for instance after the retention period). In case the client instructs the Bank to restrict or stop a Personal Data processing or to erase Personal Data which makes difficult, in the Bank's opinion, to continue the banking relationship, either the client, without prior notice, or the Bank, with the prior notice foreseen in clause 18 of the Bank's General Terms and Conditions, may (without being obliged to) terminate the banking relationship.

RIGHT TO OBJECT TO DIRECT MARKETING, RIGHT TO OBJECT TO USE OF PERSONAL DATA BASED ON A LEGITIMATE INTEREST ON THE PART OF THE BANK OR A THIRD PARTY

The client and any Data Subject also have the right to object to the processing of the Personal Data by the Bank, in particular for marketing purposes. In addition, the client can notify the Bank at any time of the fact that he no longer wishes to receive offers for the Bank's products and services. The client and the Data Subject also have the right to object to the use of their personal data for profiling purposes. The Bank may refuse their objection, for instance if it uses profiling to prevent fraud. If the Bank processes the client's personal data based on a legitimate interest, the client also has the right to submit an objection. The data shall no longer be processed unless the Bank demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedom of the client or for legal claims.

RIGHT TO DATA PORTABILITY

Where relevant, as from 25 May 2018, the client and the Data Subject have the right to request the portability of their Personal Data. The Bank can arrange that the client and Data Subject receive the personal data they have provided to it and that the Bank has entered into its automated systems for the purposes of performing an agreement. The Bank will not do this unless it processes the client's or Data Subject's personal data to his consent or to the agreement the Bank has concluded with him. This is referred to as data portability.

The client is urged to keep his personal data safe and secure The Bank urges the client to check whether any party he wants to provide his personal data to can be trusted and keeps his personal data as safe as the Bank does. If the client wants to receive his personal data, he should make sure that his own equipment is safe enough and is not prone to hacking. The client's information may be worth gold to criminals.

The client and/or Data Subject should submit any requests to receive his personal data or to provide them to others to gdpr_po@lu.abnamro.com.

The client and/or Data Subject can submit a request in regard to these rights at the e-mail address gdpr_po@lu.abnamro.com.

DOES THE CLIENT HAVE A COMPLAINT OR WANT TO ASK A QUESTION?

The client and/or Data Subject can contact the Bank if they have any questions about the Privacy Statement. The Bank is happy to help. If the client and/or Data Subject does not agree with how the Bank treats his personal data, he can submit a complaint by e-mail to gdpr_po@lu.abnamro.com. The client and/or Data Subject also has the right to take the complaint to the Luxembourg Data Protection Authority (Commission Nationale pour la Protection des Données - CNPD), 1, Avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette, tel.: (+352) 26 10 60-1.

PERSONAL DATA PROTECTION

The Bank goes to great lengths to protect the client's personal data as best it can. The Bank invests heavily in its systems, procedures and people. The Bank makes sure that its working methods are appropriate to the sensitivity of the client's personal data. And the Bank trains its people in how to keep the client's personal data safe and secure.

It's precisely because of the client's safety that the Bank cannot give any details on the exact security measures it takes to protect the client. But the client may have come across some of the following procedures the Bank uses to protect the client's personal data:

- Security of the Bank's online services
- Two-step authentication
- Security questions when the client calls the Bank
- Requirements for sending confidential documents

Security is the Bank's and the client's shared priority. The Bank invites the client to report any weaknesses in its security to it gdpr_po@lu.abnamro.com.

PROCESSING OF PERSONAL DATA OUTSIDE EUROPE

The client's personal data may be processed outside the European Union too. Given that non-European countries do not always have the same strict privacy rules as the Bank does, processing personal data outside the European Union is subject to additional rules.

Sharing personal data with companies of the BNP Paribas Group

The Bank and the companies of the BNP Paribas Group decide or may decide to share personal data with each other, even when the companies of the BNP Paribas group are located outside Europe.

Sharing personal data with other service providers

Third-party service providers that provide IT or other services to BNP Paribas that may be located in countries outside of the European Union for which the European Commission did nor did not render adequacy decisions (see also 'Does the Bank share the client's personal data with others?`).

International payment transactions and cross-border investing: sharing personal data with third parties, including other banks, government bodies or competent authorities

The Bank's financial services may stretch across borders, for instance if the client makes a payment to a person with a foreign bank account or if the Bank makes cross-border investments for the client.

Local regulators, foreign banks, government bodies and investigative services may request the Bank to provide personal data, for instance in the context of an investigation (see also 'Does the Bank share the client's personal data with others'?).

HOW LONG DOES THE BANK KEEP THE CLIENT'S PERSONAL DATA?

The Bank starts from the premise that it keeps personal data as long as needed to achieve the objective for which it was provided to it. The Bank may also have other reasons for keeping personal data.

The period for which the Bank keeps the personal data, which is referred to as the retention period, depends on the following criteria:

- The General Data Protection Regulation does not specify concrete retention periods for personal data. Other legislation may in fact specify minimum retention periods. If they do, the Bank is under the obligation to observe these periods. Such legislation includes tax laws or laws governing financial enterprises in particular.

- The Bank also keeps personal data to be able to make a case for its position if it becomes involved in a lawsuit or other legal proceedings in or outside Luxembourg. The Bank may keep personal data in its archives until a claim is barred by the lapse of time and legal proceedings can no longer be lodged against the Bank.

IF THE CLIENT WANTS TO READ THE PRIVACY STATEMENT AT ANOTHER TIME

The client can save the Bank's Privacy Statement onto its smartphone, iPad or computer. Alternatively, the client can send it to his email address in PDF format.

CHANGES TO THE PRIVACY STATEMENT

The Bank may change the way it uses the client's personal data over time due to changes in laws and regulations or in the Bank's products and services that will directly affect its use of the client's personal data.

More specific information in relation to the processing of Personal Data and any updates or changes in relation thereto is provided to the client via the website of the Bank, by any notification letter or notification in the statements of accounts. The client is invited to access regularly such website in order to be duly informed of the relevant changes.