Privacy Statement

ABN AMRO Clearing Bank N.V., London Branch

1. Introduction on ABN AMRO Clearing Bank N.V., London Branch and your personal data

ABN AMRO Clearing Bank N.V., London Branch ("AACB") is responsible for your personal data and this privacy statement sets out how AACB handles your personal data (the "Privacy Statement"). It also informs you on the rights that you have as a data subject. AACB is registered with the UK data protection authority (the Information Commissioner's Office or "ICO") under number Z8741804.

Your data is handled with due care

You can be confident that we handle your personal data with due care. In the case of some AACB portals, apps, any instant messaging service or websites, the use of your personal data may differ from that described in this Privacy Statement. In such cases, a different privacy statement is provided in the portal, app, any instant messaging service or website or additional information is given in the specific online service.

We may only use your personal data if this is permitted by law or if your consent for this is obtained. In all other situations, AACB is prohibited from using personal data.

Accessibility of this Privacy Statement

This privacy statement is available online and is easily accessible. This can be shared with company's shareholders, contacts who correspond about your company or ultimate beneficial owners.

AACB's contact details for your questions on privacy

AACB is data controller/processor and can be contacted at:

> ABN AMRO Clearing Bank N.V., London Branch, 5 Aldermanbury Square, EC2V 7HR
> Email: AACB-UK-Privacy-Officer@abnamroclearing.com

2. Who is this Privacy Statement intended for?

Are you a client of AACB or have you contacted us for information on our products and services? Are you a guarantor or security provider for one of our clients? Are you a supplier or an intermediary? Do you work for one of our clients or a supplier? Then this Privacy Statement might be intended for you.

AACB may process personal data of persons who do not have an agreement with us. For example, when we capture - and use - personal data of contact persons at companies to whom we provide

our services, or shareholders of these companies, or ultimate beneficiary owners of these companies or a guarantor.

3. What is personal data?

Personal data says something about you. The best known personal data is name, (email) address, age and date of birth. Your bank account, phone number, IP address and your social security number) are also personal data.

Categories of Personal Data

There are several special categories of personal data. These include data concerning your health. Another special category concerns biometric data, such as facial recognition or your fingerprints.

Personal Data that we obtain from third parties

Businesses may contact us for information on products or services and may provide us with information which relates to you. In that case, we may use the data AACB has requested that concerns you, your business, partners, directors, shareholders, persons with significant control, guarantor(s), security providers beneficial owners, directors of associated businesses and directors of intermediaries and other suppliers.

We may also decide to use personal data obtained from other sources, such as:

- Public registers that contain personal data, such as Companies House;
- Public sources such as newspapers and, the internet and public sections of social media accounts;
- Monitoring and compliance with sanctions legislation;
- Data files from other parties that have collected personal data about you, such as intermediaries, external marketing firms or credit agencies. We use this information if permitted by law.

4. On what basis does AACB process Personal Data?

AACB is only allowed to process personal data if it is based on one of the “grounds” permitted by law. This means that we may only use personal data for one or more of the following reasons.

4. 1 Agreement

We may need your personal data to conclude an agreement for example with a business that you represent. If you are a representative, AACB may use your personal data for other reasons than the performance of the agreement. We do this even if you are only a beneficiary of a payment from one of our customers.

4.2 Legal obligation

The following are examples of legal obligations which AACB has:

- We have to take steps to prevent terrorist financing and money laundering. These include asking you and your related individuals to provide proof of identity so that we know who you are. This is why we keep a copy of identity documents.
- We may also ask you questions about certain transactions, what the source of income is or ask for an explanation on the origin of the assets.
- Other organisations may occasionally ask us to provide personal data. These organisations include law enforcement agencies, government entities, tax authorities or regulatory bodies around the world.
- If the law, regulation or other supervisory authority requirements stipulate that we must record or use your personal data, we are required to do so. In that case, it does not matter whether you are a client of ours or not. For example, we must check whether clients, and

the representatives of clients, are genuinely who they say they are. In addition, we must keep a record of personal data items for all partners, directors and signatories. We are not required to establish your identity if we only use your personal data because you are the payee of a payment made by one of our clients.

Legitimate interest of AACB or others

We also have the right to use your personal data if we have a legitimate interest in doing so. In that case, we must be able to demonstrate that our interest in using your personal data outweighs your right to data protection. We must balance all interests. Here are a few examples of when this might happen:

- we protect property and personal data belonging to you, to us and to others.
- We protect our own financial position (for example, by undertaking financial risk assessments), your interests and the interests of other clients (for example, in the event of an insolvency).
- We carry out fraud detection activities so that clients and AACB do not suffer losses as a result of fraud.
- We aim at organising AACB efficiently. We may centralise our customer and business management systems within ABN AMRO group, make use of other service providers, and conduct statistical and scientific research.

Even if you do not have an agreement with us, we may still use your personal data on the basis of a legitimate interest. We assess whether we may use personal data for marketing purposes on a case-by-case basis, and separately for each type of personal data and for each group of data subjects.

In addition, we also have the right to use your personal data if we have a "recognised legitimate interest" which permits us to process data for pre-approved purposes (including crime detection and prevention, national security and safeguarding vulnerable individuals) without a balancing test.

5. What does AACB use personal data for?

We use your personal data to help make our operations and our services as effective, reliable and efficient as possible.

Banks are one of the most regulated industries which means we have to comply with many rules. These are not only European or Dutch rules but also laws from other countries. This therefore also requires us to record, store and sometimes give personal data to authorised bodies.

5.1 Agreement

When we enter into agreements with you owe use this information for assessing and accepting clients, carrying out financial (including credit) risk assessments, risk reporting and risk management, as well as carrying out payment transfers. If we do not have the relevant personal data to verify the structure of the company, we cannot offer you our products. AACB may also use personal data to trace debtors and recover debt.

Have you not entered into an agreement with us? If so, we do not process personal data to conclude and perform an agreement with you. However, we may use personal data for other purposes, such as fraud detection. We always check first whether the use for other purposes is allowed.

Do we need personal data from you to conclude an agreement with you? Do you not want to give us personal data, even though the law says you must? Then, unfortunately, we cannot enter into an

agreement with you. In the (online) forms you may have to fill in, you will see which personal details are required.

5.2 Research
Within AACB, we study possible trends, problems, root causes of errors and risks, for instance to check whether new rules are properly observed. This helps us prevent complaints and losses. We also perform analyses with respect to personal data for statistical and scientific research, better or new products and services.

Do our products still meet your wishes and expectations? We carry out research in this area and may use personal data to do this. We study trends and use personal data with the aim of analysing and continuing to develop our products and services.

5.3 Marketing
You may receive offers from us, and news that is appropriate for your business. In this context, we use personal data that we received from you or your business, for instance because you requested marketing materials in the past or when your business is already a client of ours. We may also make use of personal data that we obtained from other parties.

5.4 Security and the integrity of AACB and our sector and compliance with legal obligations
We are required to guarantee the security and integrity of the financial sector, AACB, our employees, our clients and related individuals. We may therefore use your personal data to prevent, or combat attempted or actual criminal acts, such as fraud or terrorism.

5.5 Social responsibility and legal obligations
Given the nature of our business as a bank, we play a key role in society. We help to prevent terrorist financing, money laundering and fraud, for instance by reporting unusual transactions or by identifying and stopping potentially fraudulent transactions and verifying transactions with you if necessary. We are also required to know our customers and carry out checks on their identity and structure.

For businesses, this includes obtaining personal information on partners, directors, beneficial owners, persons with significant control, guarantors, directors of associated businesses and directors of any intermediaries. This helps us to understand your business better, and to protect the financial sector, AACB, our employees, our clients and related individuals from attempted or actual criminal acts.

We help fight terrorist financing, money laundering and fraud. For example, by reporting unusual transactions or by recognising, stopping and, if necessary, verifying possible fraudulent transactions with you. (Foreign) government bodies also request data from us if they want to investigate problems or criminal offences. We then check whether there is a good reason to do so.

Public authorities also ask us to provide personal data when they investigate problems or suspected criminal offences. In this context, we check whether it is a legitimate request. The banking and financial sector is a highly regulated industry. This means we have to comply with many rules. AACB must therefore also record and keep personal data for this purpose, and sometimes also provide personal data to the competent authorities. We always check first whether this is permitted.

5.6 ABN AMRO Group and personal data

AACB may share your personal data within the ABN AMRO group (the "**Group**") for internal administrative purposes and with a view to improve data quality and our services to you or because the law says we must, to comply better with the law and more efficiently or to fulfil our duty of care. Also, the banking oath and legal obligations require us to always consider your customer interests in our decisions. For instance, it may be important for us to know when you or the organization that you represent applies for a product offered by one part of the Group or that you or your organization has already accepted a product from another entity within the Group.

Another example is where we are required, as a group, to comply with rules against money laundering and terrorist financing. Personal Data may also need to be shared within our Group during fraud investigations. In all these cases, we first check whether this is allowed within the legal framework.

The Group uses central IT systems that allow sharing of relevant personal data between parent and subsidiary companies only for legitimate purposes. To this end, we have taken appropriate technical and organisational measures to ensure that the sharing of personal data is secure and shared only for those specific purposes so as to prevent further unlawful use of your personal data. For example, AACB and its group companies may share personal data in this way in order to respond adequately and within a specific timeframe to regulatory requests, always in compliance with privacy laws and any applicable local laws and regulations.

5.7 Other Purposes

AACB may use your personal data for other purposes than the purpose for which you or your business supplied the personal data to us. In that case, the new purpose must be in line with the purpose for which you or your business initially provided your personal data to us. The law refers to this principle as *compatible use of personal data*. Although the law does not specify exactly when the use is compatible, it does provide guidance. You may think of the following:

- Is there a clear correlation with the purpose for which you initially provided the personal data? Is the new purpose appropriate to the initial purpose?
- How did we originally receive the personal data? Did we obtain the personal data directly from you or in another way?
- What kind of personal data are we talking about exactly? Is the personal data in question considered sensitive to a greater or lesser degree?
- How would you be affected? Would you benefit, suffer or neither?
- What can we do to ensure the highest possible level of protection for your personal data? Examples include anonymisation and encryption.

6. When would AACB use personal data with or without your consent?

In most cases, AACB uses your personal data without obtaining your consent as permitted by law. Sometimes, however, we are required to ask you for your consent. Before you give consent, we recommend that you carefully read the information we provide concerning the use of your personal data. If you have given consent and you want to withdraw this consent, you can do that very simply by contacting us as set out in paragraph 1.

We make use of cookies and similar technology on our websites and/or in client portals. For more details, see our Cookies clearing. Personal data is captured to allow us to improve our online services to you.

7. When does AACB require personal data?

If we need personal data from you in order to conclude an agreement with you and you refuse to provide this data even though this is required by law, we cannot enter into an agreement with you. If an agreement already exists, we must terminate the agreement with you.

Do you want us to remove your personal data from our systems? Unfortunately, we cannot remove required personal data. We need this data, for instance for the performance of the agreement you have with us, or because we are required to keep this data by law or owing to a legitimate interest of AACB.

7.1 Camera Images, Telephone Calls, Chat Messages and Video Chat Sessions

If you visit us, we may capture images of you on camera. We do this for security purposes. We may also record your telephone calls with us. We do this for the purpose of improving our services or because of a legal obligation and for the prevention and detection of crime. We handle video and audio recordings with due care. They are subject to the same rules as other personal data. You may exercise your rights, such as your right of access.

7.2 Other Parties Using your personal data

There are situations in which we need to provide your personal data to other people and entities involved in the provision of our services. These are described below.

- ***Our service providers***
  We work with other companies that help us provide services to our clients. This is referred to as outsourcing. We are not permitted by law to pass your personal data to them without good reason. This is governed by legal rules. We therefore carefully select these companies and clearly agree with them on how they are to handle your personal data. We remain responsible for your personal data held by us or on our behalf.

- ***Intermediaries***
  We also work with intermediaries who introduce clients and organizations to us. Such intermediaries process your personal data and are responsible for how they use your personal data. Please visit the relevant intermediary's website to find out how it handles personal data.

- ***Competent public authorities***
  Our supervisory authorities, law enforcement agencies, government entities, tax authorities or regulatory bodies around the world may ask us to provide data relating to you. The law specifies when we are required to provide this data.

- ***Purchasers***
  In the event that we propose to transfer your agreement to a third party financial services provider, we may share personal information with the proposed transferee of our agreement, to allow decisions to be made relating to that transfer and for the purposes of that transfer. This is within the legitimate interests of AACB, and to allow any such transferee to meet their legal requirements.

7.3 Social Media

We use social media channels to publicise our organisation, products and/or services with clients, users of portals and visitors to the website. We do this so that we can offer useful, relevant information and/or answer questions we receive through social media. We use the internet and social media channels, such as LinkedIn for this purpose.

7.4 Automated decision-making
We may use automated decision-making if we enter into an agreement with you.

If we make a decision that has legal consequences for you or affects you to a significant degree, this will be done with the intervention of one or more competent bank employees. Examples include client acceptance or the reporting of unusual transactions to the authorities.

If, at any time in the future, we want to use automated decision-making that has legal consequences for you or affects you to a significant degree, we will make this clear to you beforehand. We will inform you of your rights, such as your right to obtain an explanation of the decision reached by automated means, your right to express your point of view, your right to challenge the decision and your right to obtain human intervention.

7.5 Security
We go to great lengths to ensure the highest possible level of protection for your information:

- We invest in our systems, procedures and people;
- We make sure that our working methods are in keeping with the sensitive nature of your information;
- We train our people how to keep your information safe and secure;
- For security reasons, we are unable to provide details of the precise measures we take. But you may have come across some of the following procedures we use to protect your personal data:
    - Security of our online services;
    - We follow a rigorous process to establish your identity (authentication);
    - Requirements for sending confidential documents;
    - Security is our shared priority. If, for example, you encounter breaches in our security; you can report them to us confidentially through our website.

8. Is Personal Data handled outside of the UK?
UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. However, we may transfer your personal in certain circumstances (including as set out in the next paragraph). Accordingly, your personal data is processed outside of the UK too.

Your personal data may be transferred to and processed by AACB's branches, subsidiaries and operations outside the UK for the purposes outlined in this document. Personal data transfers outside the UK are governed by ABN AMRO Bank's Binding Corporate Rules (the "**BCR's**"), as a safeguard to ensure data transfers are carried out accordingly. Personal data transfers are also carried out in compliance with local laws, and may be carried out for the reasons set out in UK GDPR. For the privacy statements of our Non-UK entities, please click on the following link (if applicable):

- ABN AMRO Clearing Bank NL: (https://www.abnamro.com/clearing/en/home/information/privacy-statement-%20clearing);
- ABN AMRO Clearing Bank Chicago;
- ABN AMRO Clearing Bank Singapore;
- ABN AMRO Clearing Bank Sydney;
- ABN AMRO Clearing Bank Hong Kong;
- ABN AMRO Clearing Bank Brazil.

Sharing personal data with other service providers
We may occasionally share personal data with other companies or organisations outside UK, for instance with network parties for tax reclaim purposes or in the context of an (outsourcing) agreement. In that case, we ensure that either the country has adequate equivalent protections, or that we have concluded separate agreements with those parties, and that these agreements comply with the UK standard.

International payment transactions and cross-border investing
There are situations in which our clients make use of our international financial services, for instance to transfer money abroad or holding investments abroad through us. In such situations, foreign parties, such as local supervisory authorities, banks, government bodies and investigative authorities, may ask us for personal data, with regards to investigations for example. Additional rules governing the use of personal data apply if your organization purchases investment products from us.

9. How do we determine the period for which personal data is stored?
We have to comply with UK legislation in relation to minimum data retention periods for personal data. Such legislation includes the general requirement for businesses to keep records, as set out in the Conduct of Business Sourcebook (FCA Handbook) and Companies Act 2006, tax laws, Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended ("MLR") or laws governing financial enterprises in particular (like the FCA).

The length of time we keep personal data varies from a few months to many years. In many cases it is kept for seven years after your relationship with us ends.

Personal data is deleted or anonymised once the retention periods have ended. Certain personal data may be kept for longer for various reasons, for instance as part of our risk management, for security reasons, or in connection with claims, investigations or lawsuits.

10. What rights do you have?
If you want to exercise the rights as listed below, please submit a request to us by contacting us.

Right of access, right to rectification, right to be forgotten, right to restriction of processing
You have the right to demand an overview of all data relating to you that we handle. If your personal data is incorrect, you can ask us to change your personal data. You can ask us to erase your personal data at any time. We are not always able to do this, however, and we do not always have to agree to this, for example, if we are required by law to keep your personal data for a longer period of time. You can also ask us to temporarily restrict our use of personal data. You can do that if:

- You think the personal data is incorrect;
- We are not supposed to use your personal data;
- We want to destroy your personal data but you still need it (for instance after the storage period has ended).

Right to Data Portability
You have the right to data portability. This right applies when personal data of the individual is used to carry out a contract where the individual himself and not the business it represents is party to that contract, or when the individual has been asked for his or her consent for the processing of the data. AACB concludes an agreement with the business you represent or are related to and not with you individually. For this reason (except in limited circumstances where you may be a sole trader or sole director of a company) this right does not apply to you as a contact person at companies to which we provide services and with whom we are in correspondence, partner, director,

shareholder, person with significant control, guarantor, security provider or beneficial owners of these companies, and also directors of associated businesses, directors of any intermediaries.

11. Do you have a complaint, question or is something unclear?

If you have a complaint about the use of your personal data, please follow the appropriate steps of AACB's complaints procedure by completing the form located on our website (https://www.abnamro.com/clearing/en/complaint-form). We are here to help. You can find more information about AACB's complaints procedure here.

If you would prefer to talk to us by phone, you can call us on: +44 203 880 41214

If you are not satisfied with the solution and your complaint has already been dealt with by AACB's Complaints Management department or if you have specific questions about this privacy statement, you may contact the Data Protection Officer by sending an email to AACB-UK-Privacy-Officer@abnamroclearing.com.

You also have the right to take your complaint to the UK's supervisory authority, the Information Commissioner's Office. For more details, you can visit their website at ico.org.uk. If you have specific questions about this privacy statement, you can contact the Data Protection Officer by sending an email to AACB-UK-Privacy-Officer@abnamroclearing.com.

12. Do you want to read this Privacy Statement at another time?

You can save this Privacy Statement on your smartphone, tablet or computer.

Changes to the Privacy Statement

Changes to the law or our services and products may affect the way in which we use your personal data. If this happens, we will make changes to AACB's Privacy Statement and post a new version of the Privacy Statement on our website as well as retaining on AACB's website previous versions of the Privacy Statement.