Privacy statement

This privacy statement was amended on 1 November 2021

ABN AMRO Bank N.V. and your personal data

This privacy statement sets out how we handle your personal data. You can be confident that we handle your personal data with due care. In the case of some of the bank's apps, websites or services, 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 app or on the website, or additional information is provided along with the specific online or other service. We want you to be are aware of this so that you can avoid unwelcome surprises.

What information can you expect to find in this privacy statement?

Are you a client of ours or have you shown an interest in a specific product, for example by making an application? If so, we use your personal data and this privacy statement applies to you. If you visit our website or use one of our apps, we will also use your personal data in those situations.

It can also happen that we process personal data relating to individuals who do not have a contract with us, for example, when we record and use personal data relating to contact persons at companies to which we provide services, shareholders of these companies or ultimate beneficial owners (UBOs) of these companies. We may also process personal data relating to individuals who, for example, act as guarantors for our clients.

This privacy statement is available online and can be consulted easily. If you run a company that is a client of ours, and your company has shareholders, contact persons who have correspondence regarding your company with other parties your company with other parties, or UBOs, please provide them with this privacy statement so that they can easily find out how we handle their personal data.

To enable payments to be made, we process personal data relating to individuals with whom we do not have a contract. Examples of such personal data include the details of someone to whom you transfer money and whose account is with another bank.

If you are one of these people, then this privacy statement is intended for you too.

Our contact for your questions about data protection
We have a designated Data Protection Officer. Information on how to contact us can be found in the section headed ‘Do you have a complaint, question or is something unclear?’.

Who is responsible for your personal data?
ABN AMRO N.V. is responsible for your personal data.

What is personal data?

Personal data is information that says something about you. The best-known forms of personal data are your name, address, email address, age and date of birth. Personal data also includes your bank account number, your phone number, your IP address and your citizen service number (BSN).

There are several special categories of personal data. These include data concerning your health, as well as biometric data, such as fingerprints or data used for facial recognition. We may only use this personal data if this is permitted by law or if you give your explicit consent for this. In all other situations, we are prohibited from using this personal data.

Personal data relating to you that we have obtained from others
Imagine that your partner applies for a loan in both your names. In that case, we may use the personal data that we request in relation to you, and in some situations we are in fact required to do this. We may also decide to use personal data obtained from other sources, such as:

- Public and other registers that contain your personal data, such as the National Credit Register and the Chamber of Commerce;
- Public sources such as newspapers, the internet and public sections of social media accounts; We do this because, among other things, we need to be able to investigate fraud and other forms of crime.
- Monitoring and compliance relating to sanctions legislation;
- Data files from other parties that have collected information about you, such as external marketing firms or credit agencies. We use this information where this is permitted by law.

When do we use your personal data?

Obviously, we may not request or use your personal data without good reason. By law, we are permitted to do this only if 'the processing has a legal ground'. This means that we may only use your personal data for one or more of the following reasons:

Contracts
We need your personal data for concluding and performing a contract, for example if you want to open an account with us or take out a mortgage. This also applies when we provide innovative services to you, for example in the context of contactless payment services.

Are you the representative of your company and has your company concluded, or does it want to conclude, a contract with us? Or are you the contact person, shareholder, managing director or ultimate beneficial owner (UBO) of that company or one of our corporate clients? If so, we use your personal data for other reasons than the conclusion or performance of the contract. We also do this if you are merely the payee of a payment made by one of our clients.

Legal obligation
The law lays down many rules that we have to comply with as a bank. These rules state that we have to record your personal data and occasionally provide it to others. The following are just some examples of the legal obligations we have to comply with:

- Under the Dutch Financial Supervision Act (Wet op het financieel toezicht - Wft), we must, for example, take measures to ensure borrowers do not overextend themselves. This means that we have to use your personal data to obtain a good picture of your financial situation. For example, we use your transaction data for this

purpose when we first enter into our contractual relationship with you. As part of our statutory duty of care, we send you product messages to keep you informed about changes affecting products, such as changes in interest rates. In addition, we contact you if we notice that certain risks associated with your product have changed since you took out the product. In this context, we may send you service messages containing information about secure banking.

- We have to take steps to prevent and combat fraud, tax evasion, terrorist financing and money laundering. These include asking you to prove your identity so that we know who you are. This is why we keep a photocopy of your identity document. We may also ask you questions about certain transactions or the source of your income, or ask for an explanation of the source of your assets. More information about this can be found on the website of the Dutch Central Bank (DNB).
- There are a number of laws that require us to keep your personal data. These laws include the Dutch Civil Code, the Dutch Financial Supervision Act (Wet op het financieel toezicht - Wft), the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme - Wwft) and the Dutch Bankruptcy Act (Faillissementswet).

Other organisations may occasionally ask banks to provide personal data, or we may be required to provide data to them. Examples include the Dutch Tax and Customs Administration (such as under a reporting obligation aimed at preventing tax evasion, or DAC 6), as well as investigative services that request data as part of investigations into crimes such as financial fraud, money laundering or terrorist financing. In addition, banks - and therefore we - are sometimes required to share personal data with supervisory authorities, such as the Netherlands Authority for the Financial Markets (AFM), the Dutch Central Bank (DNB) and the European Central Bank (ECB), for instance when they carry out research into business processes or specific clients or groups of clients. In the context of disciplinary law for banks in the Netherlands, we are sometimes required to provide personal data to Stichting Tuchtrecht Banken.

If the law or a supervisory authority stipulates that we must record or use your personal data, we are required to do this. In that case, it does not matter whether you are a client of ours or not. For example, every bank must check whether clients, and the representatives of clients (including corporate clients), are genuinely who they say they are. In addition, banks must keep a photocopy of an identity document for each of their clients. This means that we are not required establish your identity if, for example, we only use your personal data because you are the payee of a payment made by one of our clients.

Legitimate interest of the bank 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 therefore balance all the interests. We explain the situations in which this happens using a few examples:

- We protect property and personal data belonging to you, to us and to others.
- We protect our own financial position (for example, so that we can assess whether you are able to repay your loan, or in the event that we sell your loan or other commitments), your interests and the interests of other clients (in the event of a bankruptcy, for instance).
- We carry out fraud detection activities to help you and us avoid suffering losses as a result of fraud.
- You will be sent relevant tips and offers relating to the bank's products and services.
- We aim to keep efficient records and improve our data quality in order to provide you with the best possible service. We also need to ensure our banking systems are organised optimally and efficiently in order to meet our legal obligations.
- We conduct research to find out how we can improve our existing processes, develop products and services, and fulfil our legal obligations more effectively. We may use new technologies for this. We will consider which data we can use for developing, training and testing new technologies on a case-by-case basis.

- We constantly search for appropriate ways to ensure the highest possible level of protection for your data and for ours.
- We carry out academic research and statistical research. ABN AMRO Group Economics carries out statistical research into macro-economic trends such as industrial growth in the Netherlands or consumer behaviour, among other things.

Someone else may also have a legitimate interest. For example, someone might transfer money to your bank account accidentally, or might be tricked into doing so. In that case, we may, under certain conditions, provide your personal data to the person who issued the payment instruction. That person can then ask you to pay the money back. More information can be found on the website of the Dutch Payments Association (Betaalvereniging).

Even if you do not have a contract with us, we may still use your personal data either because this is necessary to ensure compliance with the law or on the basis of a legitimate interest. We will of course first check whether this is the case, for instance if your personal data is used for security purposes.

Using personal data with or without your consent

In most situations where we use your personal data, there is no legal requirement for you to give your consent for this, as the use of your personal data is permitted by law. In those situations, we use your personal data because:

- this is necessary because of the contract we have with you. This is because we need personal data relating to you for the conclusion and performance of the contract.
- The law states, for example, that we must use your personal data to identify you as a client.
- the bank or a third party has a legitimate interest in this, for example in the case of fraud prevention or if we want to send you a message about secure banking.

Sometimes, however, we are required to ask you for your consent. In such situations, we explain what we will use the personal data for before you provide us with your personal data. 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. For example, you can find information on how to do this in the form or app that explicitly requested your consent.

In which situations do we ask you for your consent? We will in any event ask you to give consent in the following situations:

1. When we use biometric technologies, such as facial recognition for identity verification.
2. When a third party asks for access to your payment details and account information so that you can use an external service such as a payment service. You must first give consent to the provider of that service and then confirm to us that this party is to be given access to your account information at ABN AMRO. When you want to add your accounts with other banks to ABN AMRO Internet Banking, the ABN AMRO app or the Grip app.
3. When we place cookies and similar technology on our websites and/or in apps in order to make you personalised offers. For more details, see our Cookie Statement.
4. When we want to send you commercial messages about products or services from one of our partners, for example in the context of doing business sustainably. You can read more about this under "Tips and offers".
5. When we send you commercial messages based on your individual payment details. You can read more about this under "Tips and offers".
6. When we make use of automated decision-making and profiling and the law states that we require your consent for this.

Important information

In certain situations we do not ask for your consent. This is the case if we require your personal data to comply with the law, if a legitimate interest exists, or if this is necessary in the context of the contract that we conclude with you. In such cases, however, you may submit an objection.

What do we use your personal data for?

We use your personal data to help make our organisation and our services as effective, reliable and efficient as possible. We do this for the following seven purposes:

1. **Contract**. To be able to enter into contracts with you and perform these contracts. If we do not have your personal data, we cannot offer you a current account or transfer money from or to your account for you, for example.
2. **Research.** We study possible trends, problems, root causes of errors and risks, for instance to check whether new and existing rules are properly complied with. This helps us prevent complaints and losses. It also allows us to intervene or issue a warning in time, for example if you are no longer able to repay your debts. We also need to test whether systems (that enable us to provide our services to you or that we have to use so that we can comply with the law) are working properly, and investigate whether new technologies are helping us to comply more effectively with the law or provide a better service to you. We also carry out research into economic trends. This helps us to gain a better understanding of the economy. We do not share research or reports from which your personal data can be extracted.
3. **New or improved products and services**. Do our products still meet your wishes and expectations? We use your personal data to carry out research in this area. We study trends and use personal data with the aim of analysing and continuing to develop our products and services. We may use new technologies as part of this.
4. **Marketing.** You receive tips and offers that are appropriate for you and can benefit you as a client. In this context, we use personal data that we received from you, for example when you requested information about sustainable products and services in the past, or because you are already a client of ours. In this context, we may also use personal data that we have received from other sources, such as public data sources and marketing agencies. We only do this if it is permitted by law.
5. **Security and the integrity of our bank and our sector.** We are required to guarantee the security and integrity of the financial sector. We may therefore use your personal data to prevent or combat attempted or actual criminal or undesirable acts, such as fraud or terrorism. This enables us to guarantee the security and integrity of the financial sector, our organisation, our employees and you, as the client. We may also use your personal data for our internal and external warning systems.
6. **Social responsibility.** As a bank, we play a key role in society. We want to help our clients make the transition towards sustainability so that they can contribute to a sustainable economy. Within the limits of the law, we participate in alliances with public parties and with financial and other institutions. Through these alliances, we want to use our special position within society to make a positive contribution in tackling certain social problems. Examples include cooperating in the fight against terrorist financing or subversive and serious crime.
7. **Legal obligation.** 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. Public authorities based in the Netherlands and other countries also ask us to provide personal data when they want to investigate problems or criminal offences. When they do this, we check whether they have good reason to do so.

The right to the protection of personal data always comes first. We always check whether the use of personal data is permitted. The banking sector is one of the most heavily regulated industries. This means we have to comply with many rules. Besides European and Dutch rules, these rules also include the laws of other countries. We must therefore also record and keep personal data for this purpose, and sometimes also provide personal data to the competent authorities. Once again, we always check first whether this is permitted.

If you have not concluded a contract with us, we will not process your personal data in order to enter into and perform a contract with you. We may, however, use your personal data for other purposes, such as fraud detection. We always check first whether using your personal data for other purposes is permitted.

Other purposes
We may use your personal data for other purposes than the purpose for which you supplied the personal data to us. In that case, the new purpose must be in line with the purpose for which you initially provided your personal data to us. The law refers to this principle as ‘compatible use of personal data’. The law does not specify exactly when a use is compatible, although it does provide guidance:

- Is this purpose clearly related to 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 is concerned exactly? Is the personal data in question considered sensitive to a greater or lesser degree?
- How would you be affected? Would you benefit ,what is the privacy impact?
- What can we do to ensure the highest possible level of protection for your personal data? Possibilities include anonymising, masking or encrypting your personal data.

Our group and your personal data
We may share your personal data within our group for specific purposes. We may do this for internal administrative purposes (such as optimising data quality), to improve our services to you, to fulfil a legal obligation, to enable us to comply more effectively and efficiently with the law, or to fulfil our duty of care. Moreover, the banker's oath requires us to consider your interests as a client whenever we make decisions. If, for example, you apply to us for a loan, we need to know whether you already have a loan from, or current account or savings account with, one of our subsidiaries. This allows us to gain a more complete picture of your financial situation. To give another example, we may also share your personal data to enable us to better comply, as a group, with the rules aimed at combatting money laundering and terrorist financing. It may also be necessary for us to share personal data within our group in connection with a fraud investigation. In every case, we first check whether sharing your personal data is permitted within the legal parameters.

ABN AMRO Verzekeringen and other insurers

If you have a current account with us and you wish to take out insurance with ABN AMRO Verzekeringen(a joint venture between ABN AMRO and NN Group), we will share the data you provide with ABN AMRO Verzekeringen so that you can take out the insurance and we can fulfil our legal obligations. We also do this in some circumstances when we take out insurance with another insurer. If you have taken out insurance, the insurer's privacy statement applies.

Required personal data
If we need personal data from you in order to conclude a contract with you, and you refuse to provide this data even though this is required by law or it is required for the contract, we will unfortunately not be able to enter into the contract with you. The required personal data is specified in the online forms and other forms we occasionally need you to complete.

Do you want us to remove your personal data from our systems? We are unfortunately unable to remove required or other personal data that we need, for instance for the performance of the contract you have with us, or because we are required by law to keep your personal data. The bank might also have a legitimate interest.

Camera images, telephone calls, video banking and chat sessions, and chatbots
If you visit a branch of our bank, we may capture images of you on camera. This is necessary to prevent burglary, theft

and vandalism and to ensure the safety of our clients and employees. We can also be contacted by telephone or through video banking or chat sessions, for instance for mortgage advice. We may record these conversations. We do this for the following purposes:

a) to improve our services, for example so that we can coach or assess the performance of our employees,
b) we have a legal obligation,
c) in order to be able to provide evidence, or
d) to prevent fraud.

The rules that apply to other personal data also apply to the making of recordings. You may exercise your rights, such as your right of access.

Who do we share your personal data with?

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. If you transfer money to another bank, your personal data will also end up with that bank. This is unavoidable.

Our service providers
We work with other companies that help us provide services, such as the IBAN Name Check service. This is referred to as outsourcing. We are not permitted to pass your personal data on to them without good reason. There are rules that banks must comply with. We carefully select these companies and reach clear agreements with them on how they are to handle your personal data. We remain responsible for your personal data. Transaction Monitoring Netherlands (TMNL) was jointly established by several Dutch banks in order to tackle financial and economic crimes more effectively. TMNL helps ABN AMRO to improve the detection of financial crime and terrorist financing. Combined transaction monitoring by TMNL began in 2021. Currently, this only concerns payment transactions (including business payment transactions). It is possible that, in time, all transactions processed by the participating banks will be monitored by TMNL. More information can be found on the TMNL website.

Sometimes we engage other parties that also provide services, such as lawyers, auditors or bailiffs. These parties bear their own responsibility for their use of your personal data.

Intermediaries
We also work with intermediaries. It is therefore possible that you have a mortgage with us, but you took it out through a mortgage broker. This intermediary processes your personal data and is responsible for how it uses your personal data. Please visit the intermediary's website to find out how it handles personal data.

Competent public authorities
Our supervisory authorities, the Dutch Tax and Customs Administration, the Netherlands Public Prosecution Service and other national and international public authorities may ask us to provide personal data relating to you. The law specifies when we are required to provide this data. Persons employed in the financial sector are bound by the disciplinary law for banks in the Netherlands. Personal data may be provided to Stichting Tuchtrecht Banken in the context of disciplinary proceedings.

Financial services providers
Do you want us to give your personal data to other providers of financial services, such as a business that offers a specific financial service through an app? This is possible if you give your consent first. We will then be required to provide your personal data to these third parties. We are not responsible for how these third parties handle your personal data. If you share your personal data with other parties yourself, for example by making use of means of payment offered by other parties, we are not responsible for how those parties use your personal data. The privacy statements of those third parties apply instead.

Potential buyers or investors
We may also transfer personal data to other parties if we contemplate transferring our legal position in relation to you to a potential buyer or investor. We do this, for example, if we want to sell your loan (so that the other parties can make decisions regarding the transfer) or if we sell a business unit of ABN AMRO (so that the other parties can make decisions regarding the acquisition). This is a legitimate interest of ABN AMRO Bank and it enables the acquiring party to comply with its legal obligations, for example. Once this party has become the party to your contract as a result of, say, a purchase or acquisition, that party will be the new controller and will therefore be responsible for the personal data it processes in relation to you. You can contact this party if you have questions about how it handles your personal data. We may need to keep some data relating to you, for example so that we can comply with legal obligations or for research or statistical purposes.

Business partners
From time to time we work with other parties, for example as part of our sustainability strategy or in order to enable mobile payment. In such cases, we always check first whether sharing information with business partners is permitted. Sometimes we share joint responsibility for the use of personal data with a business partner (joint controllers). We reach agreement with these parties on who plays what role, and how we jointly safeguard your data protection rights.

Other banks or entities involved in payment transactions or making investments
We provide necessary personal data to other banks or parties involved in payment transactions. If you invest through us, we will also provide your personal data to parties that are involved in making the investments.

What messages do we send you?

If you are a client of ours, we will send you product messages and service messages. You will always receive these messages. We are also keen to share relevant tips and offers with you. If you are not interested, you can easily indicate that you do not wish to receive any tips or offers.

Product messages and service messages
If you are a client of the bank, you will receive messages about the product or service you have purchased. We will then send you information to keep you informed about new product conditions or a change in the interest rate, for example.

You will receive service messages from us concerning matters such as secure banking and outages, and we will also send you messages if, for example, a loan you have is no longer appropriate to your situation (update) within the context of client centricity. This is a legal requirement and it is also in keeping with what the supervisory authorities expect us to do. You always receive product messages and service messages from the bank and are not able to opt out of this.

Tips and offers
We want to support you, and this includes being relevant to you. You decide whether we can send you personalised tips and offers based on your individual transactions. We will only do this if you have given your consent. In order to send you tips and offers, we may use information obtained from various sources:

1. The personal data that we received from you in the context of the contract, such as your contact details and details of your mortgage or other loan.
2. When you visit our website, we examine how you use it. We do this on the basis of information such as your IP address. We can then make you offers that are relevant to you personally. In that case, you must have agreed to the use of cookies and similar technology such as JavaScript. The use of social media depends on the privacy settings you use on social media sites.

3. Your individual transaction details so that we can send you personalised tips and offers. We only do this if you have given your explicit consent.
4. Other sources of information (including public sources), such as external marketing agencies. We will always check first whether a public or other source of information can be used reliably.

Important! If you have accepted cookies and similar technologies, we may display personalised banners when you visit our website. As a result, even if you have indicated that you do not want to receive tips and offers, you might still see banners and advertisements on our website and third-party websites based on the consent you gave for cookies. If you have not given us permission to place advertising cookies and social media cookies, you may still see general advertisements. These banners will then be shown in a generic form and will not be based on your personal data. For more information about cookies, please see our Cookie Statement.

When you visit the website, you may choose to subscribe to a newsletter service, for example. Every message you receive will include the possibility of unsubscribing. Messages about products or services offered by parties other than the bank will only be sent to you if you have given your prior consent.

Social media
We use our own communication channels, such as our chatbot and social medial channels, to discuss our organisation, products and/or services with clients and visitors to our websites. We do this so that we can offer useful, relevant information and/or answer questions. We use social media channels such as WhatsApp, Facebook, Instagram, LinkedIn and Twitter. In addition, we answer individual, relevant questions and comments from other social media users. We also use social media channels for marketing purposes. For more information about the use of cookies, similar technologies and your settings, please see our Cookie Statement.

Profiling and the use of advanced technologies

As a bank, we are constantly on the lookout for more effective, secure and reliable technologies that help us offer our products and services to you, comply more effectively with the law, or better fulfil our supervisory authorities' expectations. Sometimes, the use of new technology requires us to make use of profiling. Profiling is permitted as long as we adhere to the rules. Below we explain why we do this, and when.

Profiling
The GDPR defines profiling as: "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

The law allows profiling. The definition given is a general definition within the meaning of the GDPR. The bank will not use your personal data to evaluate your performance at work or your health.

Fraud prevention
We have a great deal of knowledge and experience in the area of fraud prevention. Unfortunately, we are faced with increasingly sophisticated forms of fraud. We may take measures to prevent fraud where possible, which may include the use of profiling. For security reasons, we are unable to provide details of the precise measures to be taken.

Unusual transactions
As a bank, we have to comply with the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme - Wwft). We therefore pay particular attention to unusual transactions and to transactions that - by their nature - result in a relatively high risk of money laundering. For example,

we examine transactions that are not in line with your normal transaction and transactions that share the same characteristics as money laundering or terrorist financing. If we suspect that a transaction meets the legal definition of an unusual transaction, we must report it to the authorities. This examination - and any reporting - are not fully automated and do not take place without human intervention, as specialised bank staff are closely involved. Once again, we cannot go into detail on how transactions are examined because criminals could misuse this information.

Duty of care, client centricity, and risk management by the bank
We may use profiling to ensure clients do not overextend themselves and to enable us to intervene soon when clients are in danger of experiencing payment difficulties. In that case, we first make a list of the most common characteristics of clients who have found themselves in financial difficulties. These characteristics are combined to create the profile. We then check whether there are any clients who meet this profile. Finally, we determine what we can do to prevent these clients from experiencing payment difficulties and how we can help them. The supervisory authority with responsibilities relating to the duty of care and client centricity expects banks to monitor the financial situations of their clients actively and continuously in order to prevent clients from overextending themselves. We always check the use of your data against the criteria laid down in the data protection legislation.

Client acceptance and product acceptance
How do we make use of profiling when you apply to purchase a product and during the term of that product? The following example explains how we do this. Imagine that you apply for a loan from us:

1. We perform a risk assessment so that we can properly judge the risks run by you and by us. We do this for new clients and also for existing clients who want to buy additional products. We know from experience that certain characteristics can indicate whether you are able to repay a loan easily. These characteristics include whether you have a job or any debts. We assess these characteristics as part of our risk assessment.
2. Clients who are normally able to pay back a loan share a number of characteristics, as do clients who are normally unable to repay loans. Your characteristics are used as a basis for creating a profile.
3. We compare your information with our existing profiles. Finally, we assess how likely it is that you will not be able to repay the loan.

Marketing
We also use profiling to inform you about products and services provided by the bank. For example, we can select specific clients based on a group of clients that have taken out mortgages. We inform this group of clients about matters such as making their homes more sustainable and possibilities for taking out a loan to fund renovations.

When we send you tips and offers, we try to work out what your interests are, based on various characteristics. We then look at specific aspects, such as your age category and whether you already have any other products from us. We will always first check whether you have objected to the use of personal data for marketing purposes.

Obviously, we check the data protection rules to determine whether personal data may be used for that purpose. You can always object to the use of profiling for direct marketing purposes. If you do not have a contract with us, we determine whether direct marketing is permitted in specific situations.

Automated decision-making
We may use automated decision-making if we enter into a contract with you for, say, an online loan.

We do not make any decisions that produce legal effects concerning you or significantly affect you without the intervention of one or more competent bank employees. This also applies if the process that led to the decision is automated or if profiling was used. Examples include client acceptance or the reporting of unusual transactions to the authorities.

There are situations in which we use automated decision-making without any human intervention. This is permitted by law. These situations may, among other things, concern decisions not to execute transactions, such as iDEAL transactions, because they might be fraudulent. These decisions may be taken on the basis of a fully automated process without any human intervention.

If we want to use automated decision-making that produces legal effects concerning you or significantly affects you, 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. One example of a product for which the bank uses automated decision-making is the Rood Staan overdraft facility.

How do we ensure your personal data is secure?

We go to great lengths to ensure the highest possible level of protection for your personal data:

- We invest in our systems, procedures and people.
- We make sure that our working methods are in keeping with the sensitive nature of your personal data.
- We train our people how to keep your personal data safe and secure.

For security reasons, we are unable to provide details of the precise measures we take. Some of the security measures you may have come across include:

- Security of our online services.
- We follow a two-step process to establish your identity (authentication).
- Security questions when you call us.
- Requirements for sending confidential documents.
- Extra secure messages for confidential information in the ABN AMRO app and Internet Banking.

Security is our shared priority. If, for example, you encounter breaches in our security, you can report this to us confidentially through the 'Secure banking' page on our website.

Warning system used by the bank
Imagine that you are involved in damage to, or the loss of, our property, that there are suspicions that you have committed fraud, that you are being investigated by the authorities or the police, that client due diligence (CDD) carried out into you under the Dutch Financial Supervision Act (Wft) and Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft) has led to certain outcomes, or that you have failed to keep to the arrangements you agreed with the bank.

These are all examples of incidents to which the bank must pay special attention. The bank must be able to record and remember these incidents so that it can take appropriate measures or further action. The bank has a legitimate interest in this.

Incidents of this kind are referred to as “events". These events are recorded in a special internal record kept by the bank, generally referred to as "event records", which can only be accessed by authorised employees.

The internal reference register
An internal reference register (Dutch acronym: IVR) is linked to the event records. Consequently, if we believe a client's involvement in an event is sufficiently serious, we can warn the appropriate departments and group companies within ABN AMRO. This warning does not have any effect outside our organisation. We check the GDPR rules to determine whether it is permissible to share a specific event through the internal reference register within our organisation. When a

client is included in this register, we provide specific information about the reasons for the inclusion in the internal reference register, the consequences of inclusion for the client and also the client's relationship with us and our group companies, as well as the duration of the inclusion and the client's rights, such as the right to object.

The CAAML list
We also record if we have been forced to terminate our contractual relationship with you in accordance with the provisions of the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act, for example because you failed to provide us with sufficient information about where your money comes from or you are involved in money laundering or terrorist financing. In such cases, we may record your data in the CAAML list. This record is similar to the internal reference register in that it has no effect outside ABN AMRO. The aim of this record is to enable us to remember that we were forced to terminate our relationship with you because we could no longer fulfil our obligations under the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act. Once again, we have a legitimate interest in this. If you are included in the CAAML list, you will be explicitly informed about this, as well as, among other things, the reasons for inclusion, the consequences for your relationship with the bank and its subsidiaries, and the duration of the inclusion and your rights, such as the right to object.

The external reference register (ERR)

In addition to this, financial institutions in the Netherlands, including ABN AMRO, have developed a warning system that, in contrast to the event records, internal reference register and CAAML list, also has an effect externally.

This system allows the banks to check whether a person:

- has ever committed fraud,
- has tried to commit fraud,
- or forms a threat to the safety and security of the banking sector in some other way. For more information about this warning system and its workings, please visit the website of the Dutch Banking Association (NVB). The rules governing how banks, and therefore ABN AMRO, can use the external warning system have been approved by the Dutch Data Protection Authority. These rules can also be found on the website of the Dutch Banking Association. If you are included in this external warning system, you will be provided with information about your inclusion in the register and how to exercise your data protection rights.

We check these registers if you apply to become a client of ours or you decide to purchase a new product from us or one of our group companies. Only people who handle client acceptance and product acceptance are permitted to check these lists. These employees will be alerted by a signal if you are included in the register. Only a limited number of authorised employees have access to details of the reasons for inclusion in the lists. This information is always used as a basis when assessing whether the bank can accept a client or grant a product, and determining the applicable conditions.

Do we also share your personal data outside Europe?
Your personal data is processed outside Europe too. Additional rules apply in that case. This is because not all countries have the same strict data protection rules as we do in Europe.

Sharing personal data within our group
We may share your personal data outside Europe within our group. Our sharing of personal data is governed by our global internal policy, the Binding Corporate Rules (BCRs). These are published on our website and have been approved by the Dutch Data Protection Authority (Dutch DPA).

Sharing personal data with other service providers
We may occasionally share your personal data with other companies or organisations outside Europe, for instance in the context of an outsourcing contract. In that case, we ensure that we have concluded separate contracts with those parties,

and that these contracts comply with the European standard, such as the EU's standard contractual clauses, and additional requirements.

International payment transactions and cross-border investing
In some situations, you make use of our international financial services, for instance if you transfer money abroad or if you hold investments abroad through us. In such situations, foreign parties, such as local supervisory authorities, banks, government bodies and investigative authorities, may ask us for your personal data, for instance so that they can carry out an investigation. Additional rules governing the use of personal data apply if you purchase investment products from us. For details, see the provisions of Article 11.3 of the Investment Conditions.

How do we determine the period for which your personal data is stored?

We keep personal data in any event for as long as is necessary to achieve the purpose.

The General Data Protection Regulation and the Dutch GDPR Implementation Act (Uitvoeringswet AVG) do not give specific data retention periods for personal data. Other legislation may specify minimum data retention periods, however, which we must comply with. Such legislation includes the general requirement for businesses to keep records, as set out in the Dutch Civil Code, tax laws or laws governing financial enterprises in particular (such as the Dutch Financial Supervision Act).

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 ABN AMRO 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.

When personal data is kept for longer than the storage periods, we take measures to ensure this personal data is only used for purposes that require a longer retention period.

What rights do you have, and what can you do?

What rights do you have when it comes to your personal data? And what do these rights mean?

Right to object
If we use your personal data based on a legitimate interest, you have the right to object. It may be the case that you do not want us to use your personal data for profiling. In certain situations, however, we are permitted to do this even if you object, for instance to prevent fraud, manage risks or investigate unusual transactions. In such situations, we will of course comply with the law.

You may object to the creation of a personalised client profile for direct marketing purposes at any time. You can do this by changing your cookie settings and privacy preferences in Internet Banking or the ABN AMRO app.

Right to object to processing for marketing purposes
If you no longer want to receive offers for our products and services, you can unsubscribe at any time. All marketing messages include this possibility, and you can opt-out easily.

If you are not, or are no longer, a client of the bank and you want to exercise your right to object to the processing of your personal data for marketing purposes, you can submit a request through the ‘Clients’ rights’ page on our website.

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

- You have the right to demand an overview of all personal data relating to you that we use.
- 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 do not always have to comply with your request, 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 restrict the processing of your personal data on a temporary basis. This is possible in the following situations:

  - You believe that your personal data is incorrect.
  - We use your personal data wrongfully.
  - We no longer require your personal data but you still need your personal data (for example following the storage period) in order to bring, exercise or substantiate a claim.
  - If you submit an objection.

Right to data portability
Do you want to receive the personal data that you have provided to us and that we store by automated means for the purpose of performing a contract? We can arrange this, but only if we process your personal data on the basis of your consent or on the basis of the contract we concluded with you. This is referred to as data portability.

Please keep your personal data secure

- If you want to provide your personal data to any party, please check the purpose for which that party wants to use your personal data. For example, you can read the privacy statement on that party's website.
- If you want to receive your personal data, please make sure that your own equipment is adequately secure and has not been, and cannot be, hacked. Your financial information may be worth gold to criminals.

If you want to receive the personal data we hold on you or arrange for it to be passed on to another party, you can submit a request to us through the 'Clients' rights' page on our website.

Do you have a complaint or question, or is anything unclear?

If you have a complaint about the use of your personal data, please follow the appropriate steps of ABN AMRO's complaints procedure. We are here to help. When handling complaints as an organisation, ABN AMRO follows the escalation ladder provided by the Dutch Data Protection Authority (Dutch DPA).

You can find more information about ABN AMRO's complaints procedure here. If you would prefer to talk to us by phone, you can call us on 0900 - 0024 (within the Netherlands only, usual call charges) or on +31 10 241 17 20 from outside the Netherlands. You can also submit your question and/or complaint in a chat session.

If you are not satisfied with the solution and your complaint has already been dealt with by ABN AMRO's Complaints Management department, you may contact the Data Protection Officer by sending an email to privacy.office@nl.abnamro.com. You also have the right to take your complaint to the Dutch Data Protection Authority.

If you have specific questions about this privacy statement, you can contact the Data Protection Officer.

Do you want to read this privacy statement at another time?
You can save our privacy statement on your smartphone, tablet or computer. You can also send a copy (in PDF format) to your email address.

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 the privacy statement and notify you of these changes. We will post any changes on our website or in the ABN AMRO app.