

# Privacy statement

This privacy statement was amended on 1 March 2024

## ABN AMRO Bank N.V. and your personal data

This privacy statement tells you how we handle your personal data. Every time you make a payment, receive money, use internet banking, use our ABN AMRO app, email, chat, telephone us, or fill in and submit a form, for example when applying for a mortgage or personal loan, you are sharing data with us. You can trust us to do so with care. For some of the bank's apps, websites or services, the use of personal data may differ from what we describe in this privacy statement. For example, you are a job applicant or a user of the Tikkie app. In those cases, you will find a different privacy statement in the app, on the website or you will receive additional information with the specific (online) service. We think it is important that you are aware of this and are not surprised.

In addition, we 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. Of shareholders of these companies, or Ultimate Beneficiary Owners (UBOs) of these companies. We may also process data of individuals who, for example, act as guarantors for our clients.

This privacy statement is available online and easily accessible. Do you have a company that is a client of ours? And does this company have shareholders, contacts who correspond about your company or UBOs? If so, please provide this privacy notice to them. Then these persons can easily find out how we handle their personal data.

To enable payments, we process personal data of persons with whom we do not have an agreement. For example, consider the details of the person to whom you transfer money and who has a bank account with another bank.

Are you one of these individuals? Then this privacy notice is also meant for you.

### **Our contact for your questions on privacy**

We have a Data Protection Officer within our company. You can read how to contact us under the heading "Do you have a complaint, question or is something unclear?".

### **Who is responsible for your data?**

Responsible for your personal data is: ABN AMRO Bank N.V.

## What are personal data?

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

There are also special categories of personal data. These are data about your health and biometric data for example. Think of the use of facial recognition when onboarding as a customer to identify you. We may only use this personal data if the law states that it is allowed or if you give your explicit consent. Otherwise, we do not use special categories of data.

### Your personal data obtained from others

Suppose your partner also applies for a loan on your behalf. Then we may use the personal data we request about you, and in some cases we are even legally required to do so. It may also involve data from other sources. For example:

- (Public) registers containing your details, such as the Central Curate and Administration Register, the Land Registry, the BKR and the Chamber of Commerce;
- Public sources such as newspapers, the internet and sections of social media that are not private. We do this, for example, because we need to be able to investigate fraud or other forms of crime;
- Monitoring and compliance with [sanctions legislation](#);
- Files of other parties who have collected data about you, such as external marketing agencies or trade information agencies. We use this information if permitted by law.

## When do we use your personal data?

Of course, we are not allowed to request or use your personal data just like that. The law states that this is only allowed if there is 'a basis for processing'. This means that we may only use your personal data if there are one or more of the following reasons for doing so:

### Agreement

We need your personal data to conclude and also perform an agreement, 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 as part of payment services for contactless payments.

Are you the representative of your company and does or will your company have an agreement with us? Or are you the contact person, shareholder, director or UBO of this company or one of our business customers? If so, we use your personal data for reasons other than concluding or executing the agreement. We do this even if you are only a beneficiary of a payment from one of our customers.

### Legal obligation

There are many rules laid down by law that we as a bank must follow. These rules state that we must record your personal data and sometimes give it to others. We give here some examples of 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 need to take measures to prevent and combat fraud, tax evasion, terrorist financing and money laundering. What do you notice? For example, we ask you to identify yourself so that we know who you are. This is why we keep a [copy of your identity document](#) with a watermark. In this case, you may not hide the BSN and your passport photograph. Sometimes the bank asks for a copy of your passport, for example to be more certain that contracts have been signed by the right person or when applying for a new product. In that case, you may hide the BSN and photo and we will not keep the copy.

- We may also ask you questions about certain transactions, what your source of income is or ask for an explanation on what the origin of your assets is. You can find more information on the [website](#) of De Nederlandse Bank (DNB).
- There are laws that require us to retain your personal data, for example, the Civil Code (BW), the Financial Supervision Act (Wft), the Money Laundering and Terrorist Financing Act (Wwft) or the Bankruptcy Act.

Other organisations may sometimes request data from banks or we are obliged to provide data to them. Examples include the Tax Authorities (for information reporting purposes, a reporting obligation with the aim of preventing tax evasion, [CESOP](#) or DAC 6) and investigation services that request data for the purpose of criminal investigations such as financial fraud and in cases of money laundering or terrorism financing. Furthermore, banks, and therefore we too, sometimes have to share personal data with regulators, such as the Financial Markets Authority (AFM), De Nederlandsche Bank (DNB) and the European Central Bank (ECB). For instance, if they are investigating business processes or certain (groups of) customers. In the context of the Banking Disciplinary Act, we sometimes have to provide personal data to the Banking Disciplinary Foundation.

If the law or the regulator indicates that we must record or use your data, we are obliged to do so. In such cases, it does not matter whether you are a customer with us or not. For example, every bank must check whether customers or representatives of (business) customers are really who they say they are. Identification is again not necessary, for example, if we only use your personal data because you are a beneficiary of a payment from one of our customers and you are not a customer of ours.

#### **Legitimate interest of the bank or others**

We may use your personal data if we ourselves have a 'legitimate interest' in doing so. We must then be able to demonstrate that our interest in using your personal data outweighs your right to privacy. We therefore weigh up all interests. But when is this?

- We protect property and personal data belonging to you, to us and to others.
- We protect our own financial position (e.g. to assess whether you can repay your loan or if we sell your loan or other obligations), your interest and the interest of others (e.g. in case of bankruptcy).
- We do fraud detection to help prevent losses for you and for us due to fraud.
- You will receive relevant tips and offers on the bank's products and services. Regardless of whether you bank with us privately or professionally.
- We want to run our administration efficiently and improve our data quality. We do this to provide you with the best possible service. We also need to organise our banking systems optimally and efficiently to meet our legal obligations.

- We research how we can improve our current processes, (further) develop products and services and how we can better comply with legal obligations. To this end, we may use new technologies such as artificial intelligence. For each situation, we will consider which data we can use to develop, train and test new technologies. We are constantly looking for appropriate ways to keep your and our data as secure as possible.
- We do statistical research and sometimes collaborate with universities to do scientific research. The Economic Bureau of ABN AMRO does statistical research on macroeconomic trends such as growth of Dutch industry, consumer behaviour or economic impact on climate change, among others.

Someone else may also have a legitimate interest. Suppose someone has accidentally or under false pretences transferred money to your bank account. Then, under certain conditions, we may give your personal data to the originator of the payment. He can then ask you to refund the amount. You can find more information on the [website](#) of the Payments Association.

Even if you do not have an agreement with us, we may use your personal data because it is necessary to comply with the law or on the basis of a legitimate interest. Of course, we will first check whether this is the case, for example because of security purposes.

## The use of personal data, with or without your consent

We usually use your personal data without your legal consent. The law allows this. We do this because:

- this is necessary because of the agreement we have with you. After all, we need personal data from you to enter into and perform the agreement.
- the law requires us to use your personal data, for example to identify you as a customer.
- there is a legitimate interest of the bank or a third party, such as in fraud prevention and if we want to send you a message about Safe Banking.

Sometimes we do need to ask for your consent. We will then first explain to you what we use personal data for before you provide us with your personal data. We advise you to carefully read the information we give you on the use of your personal data first.

Have you given consent? And would you like to withdraw it? This can be done very easily. You can read how to do this for example in the form or in the app where your consent is explicitly asked for.

### **When do we ask for your consent? At least in the following cases:**

1. If we use biometric technologies, such as facial recognition for identity verification, for example.
2. If we place cookies and similar techniques on our websites and/or apps to provide you with personalised offers. You can read more about this in the [Cookie Statement](#).
3. If we want to send you commercial messages about products or services from one of our Partners, for example in the context of sustainable real estate. You can read more about this under "Tips and Offers".
4. If we send you commercial messages based on your individual payment details. You can read more about this under "Tips and Offers".

5. If we use automated decision-making based on profiling and the law states that we need your consent to do so.

The Payment Services Directive is a European law for payment transactions. This law also allows you to give third parties access to your payment data. If another party requests access to your payment data and account information so that you can use external (payment) services, you first give permission to the provider of this service. You will then confirm to us that this party obtains access to your account information at ABN AMRO. If you wish to add your accounts held at other banks to ABN AMRO Internet Banking and the ABN AMRO app, you will also give permission.

## What do we use your personal data for?

We use your personal data to make our organisation and our services as good, reliable and efficient as possible. This includes the following 7 purposes:

1. **Agreement.** To enter into and perform agreements with you. For example, without your personal data, we cannot offer you a current account, transfer money to or from your accounts for you or enter into a mortgage agreement with you.
2. **Research.** We investigate possible trends, problems, causes of errors and risks. For example, to check whether new and existing rules can be properly complied with. This allows us to prevent complaints and damage. It also allows us to intervene or warn in time if, for example, you can no longer repay your debts. We also need to test whether systems (that enable us to provide our services to you or that we need to use to comply with the law) are working properly or investigate whether new technologies help us to better comply with the law or serve you better, for example. We also research economic trends. Sometimes in collaboration with universities. This helps us better understand the economy. We do not share and/or publish research results or reports with other parties from which your personal data can be derived.
3. **Better or new products and services.** Do our products still match your needs and expectations? To investigate this, we use your personal data. We research trends and use personal data to analyse and further develop our products and services. We may use new technologies for this purpose.
4. **Marketing.** You will receive tips and offers that suit you and can benefit you as a customer. In doing so, we use personal data that we have received from you. For example, because you once requested information about sustainable products and services. Or because you are already a customer with us. We may also use personal data obtained from others. For example, from public data sources and from marketing agencies. Only if this is allowed by law.
5. **Safety and integrity of our bank and our industry.** We are obliged to safeguard the security and integrity of the financial sector. Therefore, we may use your personal data to combat or prevent (attempted) criminal or reprehensible behaviour. For example, in cases of fraud or terrorism. This allows us to safeguard our security and integrity, that of the financial sector, our employees and you as a customer. We may also use your data for our internal and external warning systems.
6. **Social responsibility.** As a bank, we play an important role in society. Within the limits of the law, we take our own responsibility and may also participate in partnerships with public parties and with other (financial) institutions. From our specific social position, we want to contribute positively to certain social problems such as violation of human rights, environment and climate. Examples are that we help clients make their operations more sustainable

of their home or business and participate in partnerships with other (financial) institutions in the field of combating terrorist financing or undermining crime and serious crimes.

7. **Legal Obligation.** 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.

The right to privacy protection is always central. We will always test whether use of personal data is permissible. Banks are one of the most regulated industries. This 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. Again, we always check first whether this is permitted.

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

#### **Other purposes**

We may use your personal data for purposes other than those for which you have given us the personal data. The new purpose must then fit with the purpose for which you initially gave us your personal data. This is called 'compatible use of data' in the law. The law does not say exactly when this is the case, but does provide pointers:

- Is there a clear link to the purpose for which you previously gave the personal data? Does the new purpose fit with it?
- How did we ever receive the personal data? Did we receive the personal data from you or by other means?
- What kind of personal data is involved exactly? Are they sensitive or less sensitive?
- What are the consequences for you? Is it to your advantage, disadvantage or does it not matter?
- What can we do to best protect your personal data? Consider anonymising, masking or encrypting your personal data.

#### **Our group and your personal data**

We may share your personal data within our group for certain purposes. This may be for internal administrative purposes such as optimising data quality and to improve our service to you, because the law says we must, to comply better with the law and more efficiently or to fulfil our duty of care. We aim to provide you as a customer with added value in our services if you bank with us both for business and private purposes. Also, the banking oath and legal obligations require us to always consider your customer interests in our decisions. For example, if you apply for a loan with us, it is necessary to know whether you already have a loan, current account or savings with one of our subsidiaries. This allows us to get a more complete picture of your financial situation for your own financial well-being and our group's risk management.

Another example is to better comply, as a group, 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.

ABN AMRO 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, ABN AMRO 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.

#### **ABN AMRO Insurance and other insurers**

If you have a payment account with us and you want to take out insurance with ABN AMRO Insurance (*joint venture* ABN AMRO and NN Group), we will share the data you provide with ABN AMRO Insurance in order to take out the insurance and to fulfil our legal obligations. We also do so if, in circumstances, we take out insurance with another insurer. The insurer's privacy policy will apply if you have taken out insurance.

#### **Mandatory data**

Do we need personal data from you to conclude an agreement with you? And yet you do not want to give them, even though the law says you must? Or are these personal data necessary for the agreement? Then, unfortunately, we cannot enter into an agreement with you. In the (online) forms you sometimes have to fill in, you will see which personal details are required.

Would you like us to delete your personal data from our systems? Unfortunately, this is not possible for mandatory or other personal data we need. For example, for the performance of the agreement you have with us. Or because we are obliged to keep your data by law. The bank may also have a legitimate interest.

#### **Camera images, phone calls, video banking, chats and chatbots**

If you visit a bank branch, we may make camera recordings of you. This is necessary to prevent burglary, theft and vandalism and for the safety of our customers and employees. It is also possible to contact us by phone, video banking and chat, for example for mortgage advice. We may make recordings of these conversations. We do this in order to:

- a) improve our services, e.g. to support our staff with new techniques, e.g. the automated summarisation and recording of telephone calls from our customer service department,
- b) coach and assess employees
- c) because of a legal obligation,
- d) provide evidence, or
- e) preventing fraud.

Recording falls under the same rules as other personal data. You can exercise your rights, such as the right to access.

## **Who do we share your personal data with?**

There are situations when we need to give your personal data to persons and entities involved in our services. You can read below who these are. Do you transfer money to another bank? Then, of course, your personal data will also end up there. There is no other way.

## **Our service providers**

We work with other companies that help us with our services, such as companies that develop internet tools and web applications. This means that these companies process personal data only on behalf of ABN AMRO.

Sometimes service providers process personal data for their own purposes but only if allowed by law with sufficient privacy safeguards. Example is the company that handles the IBAN Name Check.

To use and create an iDEAL profile, we work with Currence. This is the owner of iDEAL. When you create an iDEAL profile, ABN AMRO will share your selected IBAN numbers masked with Currence to save in your iDEAL profile to make it easier to select this account when making an iDEAL payment. Furthermore, ABN AMRO will share a unique identification number with Currence so that we can link the iDEAL profile to your bank profile and recognise it in subsequent transactions and/or authorisation requests. This unique identification number is different from your contract number and IBAN number. Currence's own privacy statement applies if you have created an iDEAL profile.

Sometimes we engage other parties who also provide services, such as lawyers, accountants or bailiffs. These parties are always responsible themselves for the use of personal data.

## **Intermediaries**

We also work with intermediaries. So you may have a mortgage with us, but may have taken it out through a broker. Or you may have taken out an ABN AMRO Insurance policy via a sub intermediary, such as Independer. This (sub)broker processes your personal data and is responsible for its use. Check the intermediary's website to find out how it handles personal data.

## **Competent (public) authorities**

Our regulators, the tax authorities, the public prosecutor, and other (government) bodies (national and international) may request personal data from you. The law states when we have to give them. Employees in the financial sector are bound by the Banking Disciplinary Act. In the context of a disciplinary case, personal data may be provided to the Banking Disciplinary Law Foundation.

## **Providers of financial services**

Do you want us to give your data to other providers of financial services? For example, to a company offering a particular financial service through an app? This is possible if you give your permission first. We are then obliged to provide your personal data to these third parties. We are not responsible for how these third parties handle your personal data. If you yourself share your data with others, for example by using payment methods of other parties, we are not responsible for the recipients' use of your personal data. The third parties' privacy policy will then apply.

## **Potential buyers or investors**

We may also disclose personal data to other parties when we are considering transferring our legal position towards you to a potential buyer or investor. We do this, for example, if we want to sell your loan and this allows the other parties to make decisions about and for the transfer. Or if we sell a business unit of ABN AMRO and this allows other parties to make decisions about the acquisition. This is

a legitimate interest of ABN AMRO Bank and enables the acquiring party, for example, to fulfil its legal obligations. Once this party becomes your contracting party as a result of this purchase or acquisition, for example, this party will be the new data controller for the personal data it processes from you. Do you have any questions about how this party handles your personal data? If so, please contact this party. We may still need to retain data from you. For example, to comply with legal obligations, or for research or statistics.

### **Business partners**

Sometimes we collaborate with other parties, for example in the context of offering additional services such as solutions for sustainable real estate, cyber security and to enable mobile payments. We always check first whether sharing data with business partners is permitted. Sometimes we are jointly responsible with a business partner for the use of personal data (joint controllers). We make agreements with these parties about who fulfils which role, and how we jointly safeguard your privacy rights.

### **Other banks or entities involved in payment transactions**

We provide only the necessary personal data to other banks or parties in the payment chain involved in processing payments. The payment chain involves several parties such as the supplier of ATMs who may offer additional services to shops or a payment platform of a web shop. These parties are themselves responsible for the use of your personal data.

### **Investing**

Do you invest through us? Then we also provide your data to parties involved in carrying out investments.

## **What messages will you receive from us?**

If you are a customer with us, we will send you product messages and service messages. You will always receive these messages. We are also happy to send you marketing messages such as relevant tips and offers. Don't want this (any more)? Simply indicate that you do not wish to receive tips and offers.

### **Product messages and service messages**

If you are a customer of the bank, you will receive messages about the product or service you have purchased. We will send you information so that we can keep you informed about new product conditions or an interest rate change, for example.

You will also receive service messages from us about, for example, a new functionality in the ABN AMRO app, secure banking, malfunctions and we will send you notifications if, for example, a credit no longer suits your situation (update) as part of Customer Interest Central. This is required by law and is in line with what is expected of us by regulators. You will always receive product messages and service messages from the bank and cannot turn them off.

### **Tips and offers**

We like to think with you. This also means that we want to be relevant to you. You decide whether we can send you personalised tips and offers based on your individual payment details. We only do this with your prior consent. In order to send you tips and offers, we may use various sources:

1. The personal data we have received from you as part of the agreement such as your contact details, the details of your loan or mortgage.
2. When you visit our website, we examine how you use it. We do this, for example, through your IP address. We can then provide you with personally relevant offers. You must then have consented to the use

of cookies and similar techniques such as JavaScript. The use of social media depends on your privacy settings on the various social media sites.

3. Your individual payment details to send you personalised tips and offers only with your consent.
4. Other (public) sources of information such as from external marketing agencies. We will always check in advance whether the use of a (public) source of information is permitted for the purpose for which we intend to use it and is reliable.

Please note: As a visitor to our website, we may show you personalised banners on the website and in the ABN AMRO app if you have accepted cookies and similar techniques on our website. You can withdraw consent to cookies at any time. For more information see [Cookie settings](#)

Have you not given us consent to place advertising cookies and social media cookies? Then you may still see general advertising or personalised banners on the website or in the ABN AMRO app based on the factual information we have about you such as the products and services you have purchased from us. You can read more about cookies in our [Cookie Statement](#).

For sending product messages, service messages, tips and offers and newsletters, we may use innovative techniques to measure the reach of sent messages. You can read more about cookies and similar techniques in our [Cookie Statement](#).

If we send you messages about products or services from a party other than the bank, for example our business partners, we will only do so with your prior consent.

### **Social media**

We engage with customers and visitors to our websites about our organisation, products and/or services through our own communication channels, such as our chatbot and social media channels. We do this to provide useful and relevant information and/or answer questions. We use the social media channels WhatsApp, Meta, LinkedIn, X (formerly Twitter), Snapchat, TikTok and Pinterest. We also answer individual, relevant questions and comments from other participants. We use social media channels for marketing purposes. For more information on the use of cookies, similar techniques and your settings, please see our [Cookie Statement](#).

## **ABN AMRO and the use of new technologies**

As a bank, we are constantly looking for more efficient, secure and reliable techniques that support us to offer our products and services to you or to better comply with the law, or what our regulators expect from us. If we want to use new technology such as artificial intelligence, we always first test whether its use complies with the law, is ethically and socially responsible and reliable.

Sometimes it is necessary for us to use profiling. Profiling is allowed as long as we follow the rules. Below you can read about what and when we do this.

### **Profiling**

The GDPR defines 'profiling' as follows: "Any form of automated processing of personal data in which certain personal aspects of a natural person are evaluated on the basis of personal data, in particular with the aim of analysing or predicting job performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or travel."

So the law allows profiling. This is a general definition under the GDPR. So it is not the case that the bank will use your personal data to evaluate your professional performance or health.

### **Fraud prevention**

We have extensive knowledge and experience in the field of fraud prevention. Unfortunately, we face increasingly sophisticated forms of fraud. We can take measures to prevent fraud as best we can, including the use of profiling. For security reasons, we cannot go into detail about the measures to be taken.

### **Unusual transactions**

As a bank, we have to comply with the Wwft. This is the Money Laundering and Terrorist Financing (Prevention) Act. Therefore, we pay special attention to unusual transactions and those that by their 'nature' carry a higher risk of money laundering. For example, we look for transactions that deviate from your normal transaction pattern or transactions that have characteristics of money laundering or terrorist financing. If we suspect that a transaction is unusual as defined by law, we must report it to the authorities. This investigation and any reporting do not take place in a fully automated way. There is human intervention: specialised bank employees are closely involved. Again, we do not go into detail about how transactions are looked at. Criminals could take advantage of this.

### **Duty of care, client centricity, and risk management by the bank**

To prevent overcrediting among customers and intervene more quickly when customers are in danger of getting into payment difficulties, we can use profiling. We then first make a list of the most common characteristics of customers who have encountered financial difficulties. These characteristics make up the profile. Then we look at whether there are customers who fit this profile. Finally, we determine what we can do to prevent these customers from experiencing payment difficulties and how we can contribute (i) to customers who need extra help with their day-to-day banking and (ii) offer vulnerable customers ways to stay or regain financial health. The supervisory authority with responsibilities relating to the duty of care and client centricity expects banks to continuously and actively monitor the financial situation of its customers to prevent overcrediting. We always check the use of your data against the requirements of privacy legislation.

### **Customer acceptance and product acceptance**

How do we use profiling when you want to purchase a product and during the lifetime of your product? We explain this using an example. Suppose you have a credit with us:

1. To properly assess the risks for you and us, we carry out a risk analysis. We do this if you are a new customer, but also if, as an existing customer of ours or an ABN AMRO group company, you want to buy other products from us. We know from experience that certain characteristics indicate whether you can easily repay a loan. For example, whether you have a job or debts. We assess these characteristics in the risk analysis.
2. Customers who can normally repay a loan share some characteristics. And so do customers who cannot. Based on your characteristics, a profile is created.
3. We compare your data with our existing profiles. We then estimate the risk of whether you can repay the loan.

### **Marketing**

We also use profiling to inform you about the bank's products and services. For example, we make a customer selection based on a customer group that has taken out a mortgage. We inform this group of customers, for example, about making their home more sustainable and the options for taking out a loan for renovation.

When we send you tips and offers, we try to find out where your interests lie based on a number of characteristics. For example, we will look at an age category and whether you already have other products with us. We will always first check whether you have objected to the use of personal data for marketing purposes and/or registered a right to object to receiving tips and offers.

Of course, we test the use of personal data against privacy rules. You can always object to profiling for direct marketing purposes. If you do not have an agreement with us, we will check whether direct marketing is permitted in certain situations.

### **Automated decision-making**

We may use automated decision-making when we enter into an agreement with you, for example for an online credit.

When we make a decision that has legal consequences for you or significantly affects you, this is done with the intervention of one or more authorised bank employees. This is also the case if the process leading to the decision is automated or if profiling may have been used. An example is customer acceptance or reporting unusual transactions to the authorities.

We may use automated decision-making without human intervention. The law allows for this. These may include decisions that lead to the non-execution of transactions because they may be fraudulent, for example in iDEAL transactions. These decisions may be made on the basis of a fully automated process without human intervention.

If we apply automated decision-making that has legal consequences for you or significantly affects you, we will clearly indicate this in advance. We will let you know what rights you have, for example the right of receiving an explanation of the automated decision, the right to have your views known to us, the right to challenge this decision and the right to human intervention

## **How do we ensure your data is safe?**

We do our utmost to protect your personal data as much as possible:

- We continuously invest in our systems, procedures and people.
- We ensure that our way of working matches the sensitivity of your personal data.
- We train our people to handle your personal data securely.

Precisely because of your safety, we cannot go into detail about the exact measures we take. Examples of security measures you may have encountered:

- Securing our online services.
- Establish who you are (authentication) in two steps.
- Control questions when you call us.
- Requirements on how to send confidential documents.
- Additional secure messages in the ABN AMRO app and Internet Banking for confidential information.

Security is something we also want to continue working on together with you. For instance, have you experienced security leaks? You can report this to us confidentially via the [secure banking](#) page on our website.

## ABN AMRO and integrity testing

### Warning system used by the bank

Suppose you are involved in the damage or loss of our property, there is a suspicion of fraud or the government or the police are investigating you. There may also be certain outcomes of Customer Due Diligence (CDD) checks under the Wft and Wwft or you are not complying with agreements with the bank.

These are examples of occurrences that require the bank's particular attention. The bank must be able to record and remember them so that it can take appropriate action or follow-up steps. The bank has a legitimate interest in doing so.

Such occurrences are called "events". They are recorded in a special internal administration of the bank, generally called "Event Administration", which can only be accessed by authorised staff.

### The Internal Referral Register (IVR)

Linked to the Event Administration is an Internal Referral Register (IVR). This ensures that if we feel a customer's involvement in an event is serious enough, we can alert our relevant departments. This also applies to our group companies. This alert only has internal effect (within our organisation). Whether an event can be shared within our organisation via the IVR is tested against the GDPR rules. In that case, among other things, we explicitly inform about the reasons for inclusion, the consequences of the inclusion for the customer and his or her relationship with us and with our group companies. We also inform about the duration of the recording and the customer's rights, for example 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 Referral 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.

this external alert system, you will be informed about registration and how to exercise your (privacy) rights in accordance with these rules.

If you want to become a customer with us or you want to purchase a new product from us or one of our group companies, we test against these registers. Only those dealing with customer and product acceptance are allowed to test against these lists. These employees only receive a signal if you are registered. Only a limited number of authorised staff have the details of the reasons for inclusion on the lists. It is always considered from this information whether the bank can accept this customer or grant the product and if so - under what conditions.

## Transfer of personal data outside the EEA

### **Do we also share your personal data outside Europe?**

Your personal data is also processed outside Europe. This is subject to additional rules. This is because not all countries have the same strict privacy rules as Europe.

### **Sharing of personal data within our group**

We may share your personal data outside Europe within our group. We do this on the basis of our global internal policy, the [Binding Corporate Rules](#) (BCRs). These are published on our website and are periodically amended if required by laws and regulations. The Personal Data Authority must approve an updated version before it is published on our website.

### **Sharing personal data with other service providers**

Sometimes we give your personal data to other companies or bodies outside Europe. For example, as part of an outsourcing agreement. We then ensure that we have concluded a separate agreement with those parties that complies with European standards, such as the EU Standard Contractual Clauses, and additional requirements. In addition, we assess on a case-by-case basis whether it is necessary to implement organisational and technical (such as encryption) security measures so that your personal data is adequately protected.

### **International payments and international investment**

You may have to deal with our international financial services. For example, when you transfer money abroad or when you have investments abroad through us. In that case, foreign parties may request your personal data from us, such as local regulators, banks, governments and investigative authorities. They do this, for example, to conduct investigations. Incidentally, additional rules apply to the use of personal data if you purchase investment products from us. Read the provisions in article 11.3 of the Investment Conditions for this.

## How do we determine the retention period of your personal data?

We keep personal data in any case as long as necessary to achieve the purpose.

The General Data Protection Regulation and Implementation Act (AVG) has no concrete retention periods for personal data. Other laws may well contain minimum retention periods that we must comply with. Think, for example, of the general administration obligation for companies (as stated in the Civil Code), tax legislation or legislation that applies specifically to financial companies (Financial Supervision Act).

How long we keep personal data varies. It can vary from months to years. In many cases it is 7 years after the end of your relationship with ABN AMRO. We keep personal information from a prospect for a maximum of 1 year. After the end of the retention periods, the personal data is deleted or anonymised. There are reasons to

to keep certain personal data for longer. This applies, for example, to our risk management, for security reasons or because of claims, investigations or lawsuits.

If personal data is kept for longer, we take measures to ensure that it is only used for the purposes for which a longer retention period is necessary.

## 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 entail?

### **Right of objection**

If we use your personal data on the basis of a "legitimate interest", you have the right to object. You may not want us to use your personal data for profiling. Yet sometimes we may do so even if you object. For example, to fight fraud, manage risks or investigate unusual transactions. Of course, we comply with the law in doing so.

However, you can always object to the creation of a personalised customer profile for direct marketing purposes. You can do so via your cookie settings and privacy preferences in Internet Banking or via the ABN AMRO app.

### **Right of objection for marketing**

Do you no longer wish to receive offers for our products and services? If so, you can unsubscribe at any time. You can also do this with every marketing message. You can easily exercise this right.

Are you not (or no longer) a customer of the bank and want to use the right to object to marketing? If so, you can submit a request via the [Customer Rights page](#) on our website.

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

- You have the right to request an overview of all personal data we use about you.
- Is your personal data not correct? If so, you can ask us to change your personal data.
- You can always ask us to delete your personal data. However, we cannot always do this and we do not always have to. For example, if the law requires us to keep your personal data for longer.
- You can also ask us to temporarily restrict the processing of your personal data. This can be done in the following cases:
  - You think your personal data is incorrect.
  - We wrongly use your personal data.
  - We no longer need your personal data, but you still need it (e.g. after the retention period) for the establishment, exercise or substantiation of a legal claim).
  - When you object.

### **Right to data portability (right to transferability of personal data)**

Would you like to have the personal data you have given to us that we automatically store for the performance of a contract? You can, but only if we process your personal data on the basis of your consent or on the basis of the agreement we have concluded with you. This is called 'data portability'.

### **Pay attention to the security of your personal data**

- Check what the party you want to give your personal data to will use it for. For example, read the privacy statement on that party's website.
- Do you want to receive your personal data? Then make sure your own equipment is secure enough and has not been or cannot be hacked, for example. Your financial data could be very interesting to criminals.

Would you like to receive or give your personal data we hold about you to another party? Then submit a request to us via the [Customer Rights page](#) on our website.

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

If you have a complaint about the use of your personal data, please follow ABN AMRO's complaints procedure through the appropriate steps. We will be happy to help you. ABN AMRO follows the [escalation ladder](#) from the Personal Data Authority to handle complaints as an organisation.

More information on ABN AMRO's complaints procedure can be found [here](#). Do you prefer telephone contact? You can call 0900 - 00 24 (usual call charges) or from abroad on +31 10 241 17 20. You can also submit your question and/or complaint via chat.

If you are not satisfied and your complaint has already been dealt with through ABN AMRO's [Complaint Management](#)? Then it is possible to contact the Data Protection Officer at [privacy.office@nl.abnamro.com](mailto:privacy.office@nl.abnamro.com). You also have the right to file a complaint with the Personal Data Authority.

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

### **Read it at another time?**

You can save our privacy statement on your phone, tablet or computer and send it as a pdf file to your email address.

### **Modification of privacy statement**

If changes occur in the law or in our services and products, they may affect the way we use your personal data. In that case, the privacy statement will be amended and we will inform you accordingly. We will mention this on our website and in the ABN AMRO app.