Privacy Statement of International Card Services (ICS) B.V.

This Privacy Statement was last updated on 9 February 2026.

This is the Privacy Statement of International Card Services B.V. ICS is a 100% subsidiary of ABN AMRO N.V. and is part of the ABN AMRO Group (“ICS”, “we”, “us”, “our”).

Table of contents

1 ICS and your personal data	page	2
2 For whom is this Privacy Statement intended?	page	2
3 The types of personal data that we process	page	2
4 When do we use your personal data?	page	2
5 What does ICS use your personal data for?	page	4
6 ICS and integrity testing	page	4
7 Profiling and automated decision making	page	5
8 Telephone calls and communication channels	page	6
9 What sort of messages will you receive from us?	page	7
10 With whom do we share your personal data?	page	7
11 How long do we keep your personal data for?	page	8
12 Transfer of personal data outside Europe	page	9
13 ICS and the use of new technologies	page	9
14 Security of your data	page	9
15 What rights do you have and what can you do?	page	9
16 Contact, questions or complaints about privacy	page	10
17 Amendment	page	10

ICS-391-EN-02/2026

1 ICS and your personal data

This Privacy Statement explains to you how we handle your personal data. You can trust us to do so carefully.

The entity responsible for your personal data is: International Card Services B.V. (ICS), Wisselwerking 58, 1112 XS Diemen. Chamber of Commerce (KVK) number: 33200596.

Our contact person for your questions about privacy

We have a Data Protection Officer within our company. You can read how to contact us under the heading 'Contact, questions or complaints about privacy'.

2 For whom is this Privacy Statement intended?

In this Privacy Statement, we explain which personal data we use, why we do so and how we handle your personal data.

This Privacy Statement applies to:

- Anyone who is or was a customer with us. This may include people, but also companies, such as sole proprietors or private limited companies, and the people who legally represent these companies or are contact persons for these companies.
- Anyone who has requested a product from us directly or via a co-brander, but ultimately did not become a customer (a prospect).
- Even if you are not an ICS customer, we can process your data. For example, if you are a contact person at a company that is a client of ours, a shareholder, or an Ultimate Beneficial Owner (UBO) of these companies.
- Anyone who is (has been) in contact with us, for example via our website, telephone or app.
- Anyone who visits our website.

Some apps, websites or services of ICS have different or additional rules on how we use your data. In these cases, you will find special conditions, a different privacy statement or additional information in the app, on the website or with the specific (online) service. This may be the case, for example, if you apply for a job at ICS.

3 The types of personal data that we process

Personal data says something about you. This may be information that directly relates to you, such as your name. Or it could be data that relates to you indirectly, such as your IP address. There are also special categories of personal data. This includes, for example, data about your health or facial recognition. We may only use these special forms of personal data if this is laid down by law or if you give your permission for doing so. Otherwise we cannot use these special forms of personal data.

We use the personal data that you provide to us, for example, if you apply for a credit card. Sometimes we also receive your data from other parties and use it.

Among other things, we may process the following personal data about you:

- **Identification details:** this is information such as your name, date of birth and place of birth, and Citizen Service Number (BSN).
- **Contact details:** think of your address, telephone number and email address.
- **Financial data:** this may include payslips, information about your payment behaviour and income, whether you are in a credit register, any payment arrears and whether you have other products within the ABN AMRO Group.
- **Transaction details:** for example, transaction overviews.
- **Data that we collect via cookies and similar techniques:** we collect, for example, your IP address, how you use our website and information about your internet browser.
- **Location details:** for example, the country from which you make a payment with your credit card.
- **Your interactions with ICS:** these are contact details, such as when you call, email or respond to our social media.
- **Data about your preferences:** we keep track of the news you want to receive.

Your personal data that we have received from others

We may use the personal data that we request from others about you or that we receive from others. Sometimes we even have to do so according to the law. This may also include data from other sources. For example:

- (Public) registers containing your data, such as the Central Guardianship and Administration Register, the Kadaster (Land Registry), the National Credit Register (BKR) and the Chamber of Commerce (KVK).
- Public sources, such as newspapers, the Internet and parts of social media that are not private. We do so, for example, to investigate fraud or other forms of crime.
- Monitoring and compliance with sanctions legislation.
- Files from other parties, such as external marketing agencies or credit agencies that have collected data about you. We will only use this information if it is lawful to do so.

4 When do we use your personal data?

We do not use your personal data whenever we like. The law states that this may only be done if there is 'a basis for processing' of your personal data.

We only use your personal data for:

Concluding and executing the Agreement with you

We need your personal data to conclude and implement an agreement with you. For example, if you want to apply for a credit card from us or if you already have one. This also applies when you use new services.

Are your details required for an agreement? What if do you not want to provide them, when the law does require it? Or is your data really necessary for the agreement? Then, unfortunately, we will not be able to conclude an agreement with you or we will have to terminate an existing agreement.

Are you the representative, contact person, shareholder, director or UBO (Ultimate Beneficial Owner) of a company that wishes to conclude an agreement with us or that already has one? We will, then, use your personal data for reasons other than for concluding or executing the agreement. This also applies if you are the sole beneficiary of a payment from one of our customers.

Complying with our legal obligations

We use your personal data to comply with our legal obligations. There are many rules laid down in the law that we as a bank must adhere to. Here are some examples of legal obligations we must meet:

- We must assess both your and our financial risks properly. That is why we check that you cannot borrow too much and that a credit card suits your financial situation. We use your personal data, such as your income data for this purpose. We will request this information from you or, if necessary, from other parties, such as the National Credit Register (BKR). We do so both when you apply for a credit card and during the term of your agreement, so that we can check whether you can continue to meet your obligations.
- We must also comply with European legislation and regulations when granting a loan and during the term of the agreement with you. We must clarify the financial risks faced by our clients and those for us when granting loans. We must also assess whether clients are continuing to meet their payment obligations during the term of a loan that you have taken out with us. We need information about your financial situation to do so. We can also request this information from you or from third parties (for example the BKR).
- We must inform you of edits to the terms and conditions.
- We must take measures to prevent and combat fraud, tax evasion, terrorist financing and money laundering. This includes, for example, monitoring unusual transactions. You can read more about this in Chapter 7 of this Privacy Statement.
- The rules require us to confirm your identity. What will you notice? For example, we will ask you to identify yourself, so that we know who you are. That is why we keep a copy of your identity document. In this case, you must not obscure your Citizen Service Number (BSN) or your passport photo. You may not apply a watermark.
- We may also ask you questions about certain payments, where your income comes from or exactly where your money originates. More information can be found on the website of De Nederlandsche Bank (DNB).
- We may also use personal data in the legally required reports to supervisory authorities.

Legitimate interest of ICS or of others

We may use your personal data if we have a 'legitimate interest' in doing so. We balance all the interests and ensure that the use of your personal data is proportionate. An overview of when there is a legitimate interest is provided below:

- We protect property and personal data belonging to you, us and others.
- We protect our own financial position. For example, we check whether you can repay your loan. We do so to protect our interests, your interests and those of others, for example in the event of bankruptcy.
- We use fraud detection to prevent damages as a result of fraud.
- We keep the financial sector safe. You can read more about this under the heading 'ICS and integrity testing'.
- We want to be able to keep our records up to date easily and improve our data quality, so that we can help you better. In order to comply with our legal obligations, we also need to organise our banking systems optimally and efficiently.
- We carry out research into how we can improve our current processes, (continue to) develop products and services and how we can better comply with our legal obligations. We sometimes use new technologies to do so, such as artificial intelligence. For each situation, we look at the data that we may use for the development, training and testing of new technologies.
- We will keep you informed of any changes to our products. You will also receive tips and news from ICS, whether you are a private or a business customer.
- We are always looking for the best ways to keep your data and our data safe.
- The ABN AMRO's Group Economics conducts independent statistical research, based on aggregated data, into macroeconomic trends, including, among other things, growth in Dutch industry, consumer behaviour and the economic impact of climate change. The ABN AMRO's Group Economics sometimes collaborates with universities to conduct academic research.
- Because we play an important role in society, we sometimes carry out research into subjects that are important to society, such as combating fraud more effectively, including in online banking.

Someone else may also have a legitimate interest. For example, if someone has accidentally transferred money to your credit card account, or has transferred money to it through deception. We may, under certain conditions, provide your personal data to the client handling the payment, so that they can ask you to pay the money back. More information can be found on the website of the Payments Association.

With your consent

Sometimes we ask for your consent to use your personal data. We only do so if there is no other basis for processing your personal data. We always explain to you first what we want to use your data for. Please read this explanation carefully before granting your consent.

Would you like to withdraw your consent later? This is easy. You can read how to do so, for example, in the form in which your consent is requested explicitly.

We will ask for your consent first in these cases:

- If we use biometric technologies, such as facial recognition to check who you are.
- If we use cookies or similar technologies on our websites or apps so that we can send you personalised offers. You can read more about this in our Cookie Statement.
- If you have signed up for one of ICS' commercial newsletters.
- To send or offers from other companies.
- Before we share your data within the ABN AMRO Group for our marketing activities.
- If we use (only) automated decision making and profiling and the law states that we must request your consent for this first.

5 What does ICS use your personal data for?

We use your personal data for the following purposes:

- **Agreement.** We need your personal data to conclude and implement an agreement with you. For example, we cannot give you a credit card without your data. During the term of your agreement, we will also check whether you can continue to meet your payment obligation. That means that we can intervene or warn you in good time if we expect you will be unable to repay your credit card bill or repay in time.
- **Research to improve our internal operations, products and services.** We research trends and use personal data to analyse and continue to develop our products and services. Or to bring new products to market. Sometimes we use new technologies to do so. We carry out research to check whether new and existing rules are being observed correctly. In this way, we can prevent complaints and damage. We continue to test whether our systems are working correctly and whether new technologies can help us comply with the law or to assist you better.
- **Macroeconomic research.** ABN AMRO Group also conducts research into economic trends. Sometimes it does so in collaboration with universities. This helps us to gain a better understanding of the economy. We do not share or publish any research results or reports with other parties that could allow your personal data to be derived.
- **Marketing.** You will receive offers and news that suit you and may benefit you as a customer. In doing so, we use personal data we have received from you. For example, because you have previously requested information or because you are already a client with us. We may also use personal data that we have received from others. For example, from public sources and from marketing agencies. We only do this if we are permitted by law.
- **Security and the integrity of our bank and our sector.** We are required to monitor the security and integrity of the financial sector. For this reason, we may use your data to prevent or stop fraud, crime or undesirable behaviour. This means that we can ensure that the financial sector, ICS, our employees and you, as a customer, are protected. We may also use your data for our warning systems, such as the IVR and EVR.
- **Social responsibility and research.** As a bank, we have an important role to play in society. Within the limits of the law, we take responsibility for ourselves and can also participate in partnerships with public bodies and other (financial) institutions. Through our position in society as a bank, we would like to help tackle major problems, such as human rights, the environment and the climate. We also want to ensure that our customers remain financially secure, as far as the law allows.
- **Legal obligations.** We help to combat the financing of terrorism, money laundering and fraud. We do so, for example, by reporting unusual transactions or by identifying, stopping and, if necessary, verifying fraudulent transactions with you. In addition, (government) authorities from domestic or foreign sources can ask us for information, if they are investigating problems or criminal matters. We always check whether there is a good reason for their request first.

We may sometimes also use your personal data for purposes other than those which you have given it to us. We do not just do so at our own initiative. The new purpose must then be in line with the purpose for which you initially provided your personal data to us. The law calls this a 'compatible use of personal data'. The law does not say exactly when this is the case, but it does provide leads. We always use these leads. If there is no compatible use of personal data, we will not use your personal data for other purposes.

6 ICS and integrity testing

Event records

Suppose you are involved in the damage or loss of our property, there is a suspicion of fraud on your part, or the government or police are investigating you. Customer Due Diligence (CDD) checks based on the Dutch Financial Supervision Act (Wft) and the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft) may also reveal a breach of the regulations or show that you do not comply with the agreements with ICS.

These are examples of situations to which ICS needs to pay extra attention. We must be able to record and recall these situations, so that we can take appropriate measures or follow-up steps.

We call these types of situations 'events'. These are recorded in a special internal administration system - 'Event records'.

ICS has a legitimate interest in the processing of your personal data. The purpose of processing personal data is to keep the financial sector secure.

Internal Reference Register (IVR)

An Internal Reference Register (IVR) is linked to the Events records. This allows us to alert the relevant departments within the ABN AMRO Group if we believe that a client is seriously involved in a particular event. This warning remains within the ABN AMRO Group. Whether an event can be shared within our organisation via the IVR is tested against the GDPR rules.

Only authorised employees may view the events records and the IVR.

The External Reference Register (EVR)

ICS also cooperates with other financial institutions through the Incident Warning System for Financial Institutions (Incidenten Waarschuwingssysteem Financiële Instellingen). This is a warning system that financial institutions in the Netherlands have created. With this system, financial institutions can check whether someone:

- has previously committed fraud
- has attempted to commit fraud
- otherwise poses a threat to the security of the banking sector

This system operates externally. You can read more about this warning system and how it works on the website of the Dutch Banking Association (NVB). The rules that determine how banks and, therefore, also ICS can use the external warning system have been approved by the Dutch Data Protection Authority. You can also read these rules on the NVB website.

If ICS chooses to have someone included in the IVR or EVR, this person will be informed of this by letter. In this letter, we will explain why the registration was made, what this can mean and what rights a person has such as, for example the right to object.

If you want to become our customer or apply for a new product from us or another company within the ABN AMRO Group, we will check whether you are listed in the IVR or EVR. Only employees dealing with the acceptance of customers and products may check these lists. They will only receive a notification if you are on the list. Only a limited number of authorised employees have access to the details of the reasons for inclusion on the lists. Based on this information, ICS determines whether you can become a customer or receive the product and, if so, under what conditions.

The Client Acceptance en Anti-Money Laundering (CAAML) list

We also record when we have had to say goodbye to you if the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act stipulates that we must terminate our contractual relationship with you. This happens, for example, if you do not tell us enough about where your funds come from, or if you are involved in money laundering or terrorist financing. In these situations, we can place your data on the CAAML list. This registration is only effective within the ABN AMRO Group.

The purpose of this is to remember that we stopped working with you because we are no longer able to comply with the rules of the Wwft. We also have a legitimate interest in this.

If ICS chooses to include someone on the CAAML list, this person will be informed of this by letter. In this letter, we will explain why the registration was carried out, the duration of the inclusion, what this can mean and what rights a person has such as, for example, the right to object.

7 Profiling and automated decision making

Automated decision making

Automated decision making means that a computer or a system makes decisions and a human being reviews those decisions and may change them.

We may use automated decision making when entering into an agreement with you.

We may sometimes use automated decision making without significant human intervention. This is called solely automated decision making. The law allows this. This happens, for example, when we stop a payment because we think that fraud is occurring, as with online payments. These decisions are then taken entirely automatically.

If we make an exclusively automatic decision that has legal consequences for you, we will let you know in advance. We will explain your rights in this situation to you. For example, you may ask for an explanation of the decision, give your opinion, object and ask whether a person is still looking at it.

Profiling

Profiling means that we use a computer or system to look at your data to predict how you are likely to behave or what your preferences are.

ICS may apply profiling in certain cases. Sometimes it is necessary to do so before we can enter into an agreement with you, because we must comply with the law or because we want to defend your interests or the interests of someone else. Some examples of where we can use profiling are given below.

Combatting money laundering and terrorist financing

As a bank, we must comply with the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft). We are required to screen customers and their transactions to detect criminal activity. We can use profiling for this purpose. For security purposes, we cannot explain the measures that we are taking in detail.

Unusual transactions

We pay extra attention to transactions that are different from normal or that have a greater risk of money laundering by their nature. For example, if a payment does not match your regular payment behaviour, or if a payment is similar to those found in money laundering or terrorist financing. If we believe that a transaction is unusual, as referred to in the Wwft, we must report this to the authorities. This investigation and any report will not take place in a fully automated manner. There is human intervention: specialised bank employees are closely involved in this. We do not say exactly how these transactions are examined, so that criminals cannot exploit them.

Fraud prevention

We have a great deal of knowledge and experience in the area of combatting fraud. We can take measures to prevent fraud as effectively as possible, including the use of profiling. For security purposes, we cannot explain the measures that we are taking in detail.

Payment traffic fraud detection

With fraud detection we try to prevent possible damage as a result of fraud for the client and ICS. We can also use profiling in this instance. However, we cannot promise that our system will detect and stop all fraud. You remain responsible for the use of your credit card, as stated in our terms and conditions.

Duty of care, Client Centricity and risk management at ICS

We can use profiling to provide customers with excessive lending and to intervene more quickly when they are at risk of payment difficulties. We first make a list of the characteristics that are common among customers with financial problems. We call these characteristics as a whole a profile. We then check whether there are any customers who fit this profile. The supervisory authority responsible for the duty of care and Client Centricity expects banks to continuously and actively monitor their clients' financial situations to identify and prevent (possible) repayment problems. We always ensure that the use of your data complies with the privacy regulations.

Customer and product acceptance

We can use profiling for customer and product acceptance purposes. When you apply for a product, we first look at the possible risks, both for you and for us. We also do so if you are already a customer and want a different product or limit. We know from experience that certain things indicate whether you can repay a loan easily, such as whether you have a job or debts. We assess these matters.

Customers who are normally able to repay a loan often have certain common characteristics. This also applies to people who are struggling to repay their debts. A profile is drawn up based on your characteristics.

We compare your profile with our existing profiles. We then estimate whether you can repay the loan.

Marketing

We use profiling to provide you with appropriate offers. For example, do you already have a particular product? Then you will not receive any new offers for that. Based on a number of characteristics, we try to find out where your interests lie. For example, we will look at an age category and whether you already have other products with us. You will only receive an offer from us if you fall into a particular group. First of all, we always check whether you have objected to the use of your data for marketing or if you no longer wish to receive offers.

8 Telephone calls and communication channels

Telephone calls

If you call us, we will ask for some information. Sometimes, you will get our virtual assistant on the line first. It will also ask for information, so that we can help you more quickly and more effectively. If the virtual assistant passes the conversation on to an employee, they will immediately know how to continue helping you.

We can record your telephone call. We do so:

- to improve our service, for example to coach or assess employees
- to comply with a legal obligation
- to have evidence, where necessary
- to prevent fraud

We handle these audio recordings with care. They are subject to the same rules as other personal data. You can exercise your rights, such as the right to access.

Communication channels

We talk to customers and visitors through our own communication channels, such as the chatbot and social media. We do so to provide useful information and to answer questions. We also respond to personal and relevant questions or comments from others. We also use social media for marketing purposes.

9 What sort of messages will you receive from us?

You may receive different types of messages from us. Think of product and service messages, newsletters and offers. We sometimes use smart technologies to measure the reach of the messages we send.

Product messages and service messages

If you are a customer of ours, you will always receive messages from us about our products and services. This will, for example, keep you informed of new terms and conditions or let you know if there is anything new in the ICS app. You will always receive these messages and you cannot unsubscribe from them.

We may use your personal data for these messages on the grounds of our legitimate interest, because it is sometimes required by law, or because it is necessary to comply with our agreements with you. This depends on the type of message that we send.

Tips, newsletters and offers

If you have given your consent, we will also be happy to send you marketing messages, such as tips, newsletters and offers. These messages can sometimes also be about offers from other companies. What if you no longer want to receive these messages? Every newsletter or offer contains a link so that you can unsubscribe easily.

We may use different types of information for sending news and offers:

- The personal data you have provided to us, such as your contact details.
- Information about the products that you have with us.
- Other (public) information sources, such as external marketing agencies. We will always check in advance whether the use of a (public) source of information is reliable and permitted for its intended purpose.
- When you visit our website, we examine how you use it. We do so via your IP address. We can then make you personally relevant offers. However, you must have agreed to the use of cookies and similar technologies, such as javascript. You can read more about cookies in our Cookie Statement. The use of social media depends on your privacy settings on the various social media sites.

Do you visit our website and have you accepted cookies? Then we can show you personal banners. You can always withdraw your consent to cookies and similar technologies.

What if you have not given us permission to set advertising and social media cookies? You may still see general advertising or personalised banners on the website or on third-party websites based on the current 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.

10 With whom do we share your personal data?

There are situations in which we share your personal data with others. You can find out who these are below.

ABN AMRO Group and your personal data

ICS is part of the ABN AMRO Group. We may share your personal data within our group for certain purposes. This is permitted for our own administrative purposes, such as optimising data quality and improving our service to you, and because the law requires this. It also helps us to comply with laws and our duty of care better.

Here are a few examples:

- We always take your interests as a customer into account, because this is required by law and our duty of care. Are you applying for a credit card? For example, we will check whether you already have a loan with the ABN AMRO Group and whether you meet your obligations. This gives us a good idea of your financial situation. This is necessary for your own financial well-being and for the risk management of the ABN AMRO Group.
- To comply with regulations against money laundering and the financing of terrorism. For example, we share information about possible illegal activities when you use your credit card within the ABN AMRO Group if you are also a customer there.
- In the event of a fraud investigation, personal data may be shared within the ABN AMRO Group. This only happens when it is genuinely necessary and according to the regulations. We have taken steps to keep your data secure and to ensure that it is only used for the right purpose. In this way, ABN AMRO Group can, for example, share personal data in order to respond adequately and within a certain timeframe to requests from regulators.
- ABN AMRO Group strives to offer added value in its services. This means that you, as an ICS customer, may receive a tip or offer about another ABN AMRO Group product. If the law stipulates that this can only be done on the basis of consent, we will ask for your consent first.

Co-branders

Do you have a credit card issued together with another organisation (co-brander)? We and the co-brander may then share your personal data with each other if necessary to comply with the agreement or if required by law. Sometimes we can also share your personal data within the ABN AMRO Group, for example, if this is required by law.

Authorised (public) authorities

Banks are among the most regulated sectors of the economy. This means that we have to comply with many rules. These are not only European or Dutch regulations, but sometimes also regulations from other countries. To comply with these, we sometimes need to store, retain and share your personal data with authorities that have a legal right to it.

A range of authorities may request your data from us. These include, for example, our own regulators, the Tax Administration, the Public Prosecutor's Office or other (government) bodies. The law states when we must provide this information. For example:

- The Tax Administration for information reporting purposes, a reporting obligation intended to prevent tax evasion, the Central Electronic System of Payment (CESOP) or DAC 6.
- Law enforcement agencies or the Dutch Public Prosecution Service may request data for criminal investigations, such as fraud, money laundering or terrorism financing.
- Banks and, therefore, also us, sometimes have to share data with regulators, such as the Dutch Authority for the Financial Markets (AFM), De Nederlandsche Bank (DNB) and the European Central Bank (ECB). This happens, for example, if they carry out research into our company or certain (groups of) customers.
- We also sometimes have to provide personal data to the Foundation for Banking Ethics Enforcement (FBEE) if the disciplinary law so requests.

If the law or the supervisory authority states that we must record or use your data, we shall do so. It does not matter if you are a customer with us.

Providers of financial services

Do you want us to provide your data to financial services providers? This is possible if you first give your consent. We are then obliged to provide your personal data to these third parties. When you share your personal data with others, we are not responsible for the use of your personal data by the recipients. Then the third party's privacy statement applies.

Mutual insurance societies

Insurance is linked to your credit card. For the execution of the insurance contracts, we may transfer your personal data to the mutual insurance society/societies. These mutual insurance societies are responsible for the use of your personal data.

National Credit Register (BKR)

Before entering into an agreement with us, we consult the BKR-register and/or the registers of credit agencies. We can also do this during the term of your agreement, for example if you want to adjust your spending limit, if you are in arrears or if we want to check whether your spending limit still suits your situation. Are you taking out a loan with us? Then we will report this to the BKR-register. Even if you are in arrears, we must pass this on.

Visa and Mastercard

Do you use your credit card to make a transaction? Then your personal data will also end up with payment network providers. We may transfer your personal data to Visa if you have a Visa Card or to Mastercard if you have a Mastercard.

With Business Card and Corporate Card: your employer

If you have a Business Card or Corporate Card from your employer, your employer will receive statements stating which transactions you have made with the Business Card or Corporate Card.

Business partners and service providers

When necessary, we work together with other companies. We will always check first whether it is permitted to share your data with these companies. Sometimes we, together with such a company, are responsible for your data. If a company processes your data on our behalf, we call that company a processor.

We always make agreements with these parties about who fulfils which role and how we jointly guarantee your privacy rights.

We sometimes also work with firms, such as law firms, accountants or bailiffs. These companies are always responsible for how they handle your data.

11 How long do we keep your personal data for?

We retain your personal data for as long as necessary for the purpose for which we have collected it.

The General Data Protection Regulation (GDPR) and the GDPR Implementation Act (GDPRIA) do not have specific retention periods for personal data. However, other laws may set minimum retention periods that we must adhere to. Then we have to retain that data for as long as required. For example, under tax regulations, the Dutch Civil Code (BW), the Dutch Bankruptcy Act (Faillissementswet) or special laws for financial companies, such as the Dutch Financial Supervision Act (Wft) and the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft).

How long we retain personal data for depends on the situation. Sometimes it is only for a few months, sometimes a few years. For example, we store customer files for 7 years after you are no longer a customer. We store prospect data for 3 months.

After these periods, the personal data is deleted or anonymised. Sometimes we do retain certain data for a longer period. We do so, for example, for risk management, for security purposes or if there is a claim, investigation or lawsuit. This applies to customers, but also to prospects.

12 Transfer of personal data outside Europe

Your personal data may also be processed outside Europe. Additional rules apply to this. This is because not all countries have the same strict privacy laws as in Europe.

Sharing personal data within the ABN AMRO Group

We may share your personal data outside Europe with other group companies of the ABN AMRO Group. We do so on the basis of the ABN AMRO Group's global internal policy, the Binding Corporate Rules (BCRs). These have been published on the ABN AMRO website and are sometimes amended as required by legislation and regulations.

International payments

You can use our international financial services, for example if you use your credit card abroad. The details of your payment can then be stored on servers outside of Europe. Foreign organisations, such as banks, governments or the police can also request your personal data from us. They do this, for example, to carry out an investigation.

Sharing personal data with other service providers

Sometimes we share your personal data with companies or organisations outside of Europe. For example, if we outsource tasks. We then make clear agreements with these parties in accordance with European rules, such as the EU Standard Contractual Clauses. We also assess whether additional security is needed, such as data encryption, so that your data is well protected.

13 ICS and the use of new technologies

We are always looking for ways to make our products and services easier to use, safer and more reliable. We also look at how we can comply better with the law and what regulators ask of us. If we want to use a new technology, such as artificial intelligence, we first consider whether this is necessary and whether it is permitted by law. We also check whether its use is fair, secure and responsible.

14 Security of your data

We do our best to properly protect your personal data:

- We invest in our systems, procedures and employees.
- We adapt the way we work to the sensitivity of your data.
- We teach our employees how to handle your data securely.

For your security, we do not tell you exactly what security measures we are taking. However, here are a few examples of things that you may know:

- Our online services are well secured.
- We check in two steps whether you really are who you say you are (two-step verification).
- We ask additional verification questions when you call us.
- We have rules on how to send confidential documents.

Security is something we want to continue working on together with you. For example, have you been affected by security leaks? You can report this to us in confidence via our website. You can do this via the page: Reporting weaknesses in our IT systems.

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

If your personal data is processed, you have a range of rights under the GDPR. We will explain the rights that you have below.

- **Right of access**
  You have the right to request from us which personal data we process about you and how we use this data. You can see much of this data when you log in to your ICS environment. We can help you best if you are specific in your request.

  If you request access, we do not provide the following information: personal data for other people, confidential information about KYC files or fraud investigations and (email) messages that you already have. Sometimes we will also not provide other information.

- **Right to rectification**
  You may ask us to correct your personal data if it is incomplete or incorrect.

- **Right to deletion of data**
  You may ask us to delete your personal data. Sometimes we are not permitted or not able to do so. For example, if the law states that we need to retain your data for longer, or if we still need your data.

- **Right to restriction of processing**
  You may ask us to temporarily restrict the processing of your personal data. This is possible in the following situations:
  - You think that the data we have about you is incorrect.
  - We are using your personal data although that is actually not permitted.
  - We want to delete your data because we no longer require it, but you still need it for bringing, pursuing or substantiating a legal claim.
  - You have objected to the use of your personal data.

- **Right to data portability (transferring your personal data)**
  Do you want to have the personal data that you have provided to us and that we store automatically for the execution of an agreement? This is possible, but only if we process your personal data because you have given your consent or on the basis of the agreement that we have concluded with you. That is called 'data portability'. Pay close attention to the security of your data.
  - First of all, check carefully what the other party intends to use your data for. For example, read the privacy statement on their website.
  - Would you like to receive your data? Make sure that your own computer or phone is secure and cannot be hacked easily. Your (financial) data is of interest to criminals.

- **Right to object**
  When 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 purposes. However, we do so sometimes, even if you object. For example, to combat fraud, manage risks or investigate unusual transactions.

  However, you can always object to the creation of a personalised customer profile for direct marketing purposes. You do so via your cookie settings.

- **Right to object to marketing**
  What if you no longer want to receive advertisements or offers for our products and services? Then you can always unsubscribe. You can do so via the unsubscribe link at the bottom of each marketing message. Are you no longer a customer of ICS and do you no longer want to receive advertising? Please send a request to ICS' Complaints Management.

How can you exercise your rights?

You can exercise your rights by completing the form Application to change the processing of personal data and sending it to us. We will ask you for a copy of your ID, so that we can be sure that it is you. This is to prevent someone else from exercising your rights. You can black out your passport photo and Citizen Service Number (BSN) on the copy. You may also add a watermark.

We will try to respond to your request within a month. This is permitted under the GDPR regulations. What if we need more time? Then we will let you know quickly.

We may reject your request. We will then always tell you the reason for doing so.

16 Contact, questions or complaints about privacy

Do you have a question about this Privacy Statement or about how we use your personal data? Please contact us. We are happy to help. You can also contact the Data Protection Officer at privacy.office@nl.abnamro.com.

Do you have a complaint about how we handle your personal data? If so, please follow the ICS complaints procedure. We will gladly assist you. ICS follows the escalation ladder from the Dutch Data Protection Authority (AP) to handle complaints as an organisation.

You can find more information on the ICS complaints procedure here.

Are you unable to resolve the issue and has your complaint already been dealt with via ICS' Complaints Management? You can contact the Data Protection Officer at privacy.office@nl.abnamro.com.

You also have the right to file a complaint with the Dutch Data Protection Authority.

Do you want to read it at a different time?

On icsbusiness.nl/EN/privacy-statement/ you can read an earlier version of our Privacy Statement and save it as a PDF.

17 Amendment

This Privacy Statement can sometimes change. For example, if the law changes or if we deal with your data differently. If this happens, we will amend the Privacy Statement. The latest version is always on our website.