# Privacy Statement

## This Privacy Statement was amended on 21 July 2023

### ICS and your personal data

This Privacy Statement sets out how we handle your personal data. You can be confident that we handle your personal data with due care. For some of ICS' apps or websites, the use of your personal data may differ from that described in this general Privacy Statement. In such cases, a different Privacy Statement is provided in the app or additional information is given in the specific (online) service.

### Who is this Privacy Statement intended for?

If you are our client or you have shown interest by applying for a certain product. You may have applied for a credit card directly with us or via a partner. Or if you visit one of our websites or use one of our apps? In that case, we use your personal data and this Privacy Statement applies to you.

It is possible that we process personal data relating to individuals who do not have a contract with us, for example when we record and use personal data relating to contact persons at companies to which we provide services, shareholders of these companies, or ultimate beneficial owners (UBOs) of these companies. We may also process personal data relating to individuals who, for example, act as guarantors for clients of ICS. If you run a company that is a client of ours, and your company has shareholders, contact persons who have correspondence regarding your company with other parties your company with other parties, or UBOs, please provide them with this privacy statement so that they can easily find out how we handle their personal data.

If you are one of these people, then this Privacy Statement is intended for you too.

### Our contact person for your questions about data protection

We have a designated Data Protection Officer. Information on how to contact us can be found in the section headed 'Do you have a complaint, question or is something unclear?'

### Who is responsible for your personal data?

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

### What is personal data?

Personal data is information that says something about you. The best-known forms of personal data are your name, address, email address, age and date of birth. Personal data also includes your bank account number, your phone number, your IP address, and your citizen service number (BSN). There are several special categories of personal data. These include data concerning your health as well as biometric data, such as fingerprints or data used for facial recognition. We may only use this personal data if this is permitted by law or if you give your explicit consent for this. In all other situations, we are prohibited from using this personal data.

### Personal data relating to you that we obtained from others

Imagine that your partner applies for a loan in both your names. In that case, we are allowed to use the data we collected about you. Occasionally, we are even required to do so. We may also decide to use personal data obtained from other sources, such as:

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

### When do we use your personal data?

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

### Contract

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

Are you the representative of your company and has your company concluded, or does it want to conclude, a contract

with us? Or are you the contact person, shareholder, managing director or Ultimate Beneficial Owner (UBO) of that company or one of our corporate clients? If so, we use your personal data for other reasons than the conclusion or performance of the contract. We also do this if you are merely the payee of a payment made by one of our clients.

### Legal obligation

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

- Under the Dutch Financial Supervision Act (Wet op het financieel toezicht - Wft), we must, for example, take measures to ensure borrowers do not overextend themselves. This means that we have to use your personal data to obtain a good picture of your financial situation. For example, we use your transaction data for this purpose when we first enter into our contractual relationship with you.
- We have to take steps to prevent and combat fraud, tax evasion, terrorist financing and money laundering. These include asking you to prove your identity so that we know who you are. This is why we keep a photocopy of your identity document. We may also ask you questions about certain transactions or the source of your income or ask for an explanation of the source of your assets. More information about this can be found on the website of the Dutch Central Bank (DNB).
- There are a number of laws that require us to keep your personal data. These laws include the Dutch Civil Code, the Dutch Financial Supervision Act (Wet op het financieel toezicht - Wft), the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme - Wwft) and the Dutch Bankruptcy Act (Faillissementswet).

Other organisations may occasionally ask banks to provide personal data, or we may be required to provide data to them. Examples include the Dutch Tax and Customs Administration as well as investigative services that request data as part of investigations into crimes such as financial fraud, money laundering or terrorist financing.

In addition, banks - and therefore we - are sometimes required to share personal data with supervisory authorities, such as the Netherlands Authority for the Financial Markets (AFM), the Dutch Central Bank (DNB) and the European Central Bank (ECB), for instance when they carry out research into business processes or specific clients or groups of clients. In the context of disciplinary law for banks in the Netherlands, we are sometimes required to provide personal data to Stichting Tuchtrecht Banken.

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

### Legitimate interest of ICS or others

We also have the right to use your personal data if we have a legitimate interest in doing so. In that case, we must be able to demonstrate that our interest in using your personal data outweighs your right to data protection. We therefore balance all the interests. We explain the situations in which this happens using a few examples:

- We protect property and personal data belonging to you, to us and to others.
- We protect our own financial position (for example, so that we can assess whether you are able to repay your loan), your interests and the interests of other clients (in the event of a bankruptcy, for instance).
- We carry out fraud detection activities so that clients and ICS do not suffer losses as a result of fraud.
- We keep you up-to-date on product changes and send you tips, offers and other relevant news from ICS.
- We aim to keep efficient records and improve our data quality in order to provide you with the best possible service. We also need to ensure our banking systems are organised optimally and efficiently in order to meet our legal obligations.
- We conduct research to find out how we can improve our existing processes, develop products and services, and fulfil our legal obligations more effectively. We may use new technologies for this. We will consider which data we can use for developing, training and testing new technologies on a case-by-case basis
- We constantly search for appropriate ways to ensure the highest possible level of protection for your data and for ours.
- We carry out statistical research.

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

Even if you do not have a contract with us, we may still use your personal data either because this is necessary to ensure

compliance with the law or on the basis of a legitimate interest. We will of course first check whether this is the case, for instance if your personal data is used for security purposes.

**Using personal data with or without your consent**

In most cases, ICS uses your personal data without obtaining your consent for this. This is permitted by law. In those cases, we use your personal data because:

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

Sometimes, however, we are required to ask you for your consent before we may use your personal data. Before you give consent, we recommend that you carefully read the information we provide concerning the use of your personal data.

If you have given consent and you want to withdraw this consent, you can do that very simply. Read more about withdrawing your consent.

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

1 We always ask for your consent before we process special categories of your personal data. We do not use special categories of personal data without your consent unless the law states we are required or permitted to do this.
2 When another party requests access to your payment details so that you can make use of external applications such as a financial journal.
3 When we place cookies and similar technology on our websites and/or in apps in order to make you personalised offers. For more details, see our Cookie Statement.
4 When we want to send you commercial offers of third parties.
5 When we make use of automated decision-making and profiling and the law states that we require your consent for this. 6. When we use biometric technologies, such as facial recognition for identity verification.

**Good to know:** when we use your personal data on the basis of the law or a legitimate interest, we do not require your consent to use your personal data. In such cases, however, you may raise an objection.

**What does ICS use your personal data for?**

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

1 **Contract.** To be able to enter into contracts with you and perform these contracts. If we do not have your personal data, we cannot offer you a credit card for example.
2 **Research.** Within ICS, we study possible trends, problems, root causes of errors and risks, for instance to check whether new and existing rules are properly complied with. This helps us prevent complaints and losses. In this way, we can intervene or issue a warning in time, for example if you are no longer able to repay your debts. We also need to test whether systems (that enable us to provide our services to you or that we have to use so that we can comply with the law) are working properly and investigate whether new technologies are helping us to comply more effectively with the law or provide a better service to you. We also carry out research into economic trends. This helps us to gain a better understanding of the impact of our services. We do not share research or reports from which your personal data can be extracted.
3 **Better or new products and services.** Do our products still meet your wishes and expectations? We carry out research in this area, using your personal data. We study trends and use personal data with the aim of analysing and continuing to develop our products and services. We may use new technologies as part of this.
4 **Marketing.** You receive offers and news that is appropriate for you. That is why you receive as little advertising as possible for products you are probably not interested in or already have. In this context, we use personal data that we received from you, for instance because you requested information in the past or because you are already a client of ours. We may also make use of personal data that we obtained from other parties. We only do this if it is permitted by law.
5 **Security**. We are required to guarantee the security and integrity of the financial sector. We may therefore use your personal data to prevent or combat attempted or actual criminal or objectionable acts, such as fraud or terrorism. We do this so that we can guarantee the security and integrity of the financial sector, ICS, our employees and you, as the client. We may also use your personal data for warning systems.
6 **Legal obligations.** As a bank, we play a key role in society. Within the limits of the law, we participate in alliances with public parties and with financial and other institutions. Through these alliances, we want to use our special position within society to make a positive contribution in tackling certain social problems. We help to prevent terrorist financing, money laundering and fraud, for instance by reporting unusual transactions or by identifying and stopping potentially fraudulent transactions and verifying transactions with you if necessary. Public authorities also ask us to provide personal data when they want to investigate problems or criminal offences. In this context, we check whether they have good reason to do so.

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

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

### Other purposes

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

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

### 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 specific purposes. We may do this for internal administrative purposes (such as optimising data quality), to improve our services to you, to fulfil a legal obligation, to enable us to comply more effectively and efficiently with the law, or to fulfil our duty of care. To give another example, we may also share your personal data to enable us to better comply, as a group, with the rules aimed at combatting money laundering and terrorist financing. It may also be necessary for us to share personal data within our group in connection with a fraud investigation. In every case, we first check whether sharing your personal data is permitted within the legal parameters.

### Required personal data

If we need personal data from you in order to conclude a contract with you or to comply with a legal obligation and you refuse to provide this data, we cannot enter into a contract with you, or, if a contract already exists, we must terminate our contract with you. The required personal data is specified in the online forms and other forms we occasionally need you to complete.

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

### Telephone calls

We may record your telephone calls with our staff. We may do this for the purpose of:

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

We handle audio recordings with due care. They are subject to the same rules as other personal data. You may exercise your rights, such as your right of access. Information about all your rights can be found here.

## Who do we share your personal data with?

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

### Our service providers

We work with other companies that help us provide services to you. We carefully select these companies and reach clear agreements with them on how they are to handle your personal data.

### Co-branders

If you have a credit card that is issued in collaboration with a co-brander, we may exchange your personal data with the co-brander if that is required to comply with the contract you have with us or with the co-brander.

### Competent public authorities

Our supervisory authorities, the Dutch Tax and Customs Administration, the Netherlands Public Prosecution Service and other public authorities may ask us to provide personal data relating to you. The law specifies when we are required to provide this data. Bank officials are bound by the disciplinary law for banks in the Netherlands. In this context, banks may need to provide personal data to the disciplinary commission (Stichting Tuchtrecht Banken).

### Financial Services Providers

Do you want us to give your personal data to providers of financial services? This is possible if you give your consent first. We will then be required to provide your personal data to these third parties. If you share your personal data with other parties yourself, we are not responsible for how they use your personal data. In that case, the Privacy Statements of those third parties apply instead.

### Insurances

Your credit card is linked to a number of insurance contracts. For the performance of these insurance contracts we are authorised to pass on your personal data to the relevant insurance company, which is the responsible party with respect to the insurance contract.

### National Credit Register (Bureau Krediet Registratie - BKR) When

you apply for a credit card, we will carry out a credit check, within which context we will consult the National Credit Register (BKRregister). We will also consult this register and/or registers of credit agencies during the term of the credit card agreement. We do this if we have a reasonable interest in doing so, for example if you apply for a change in your spending limit or if you are in arrears with payments. If you sign up for a credit with us, we will register it in the BKR register. We also need to record late payments in the BKR register, for example.

### Business partners

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

### Visa and Mastercard

We may pass on your personal data to Visa if you have a Visa Card, or to Mastercard if you have a Mastercard.

### In the case of a Business Card or Corporate Card: Your employer

If you have a Business Card or Corporate Card of your employer, your employer will receive account statements which list the payments you made with the Business Card or Corporate Card.

### What messages do we send you?

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

### Tips and offers

If you have previously purchased a product or service from ICS, we would like to offer you ICS products and services that best suit you. This also applies when you visit our website. In order to send you tips and offers, we may use information obtained from various sources:

1. The personal data that we received from you in the context of the contract and what products you have with us.
2. When you visit our website, we examine how you use the website. We do this using your IP address. We can then make you offers that are relevant to you personally. In that case, you must have agreed to the use of cookies and similar technology such as JavaScript. For more information about cookies, please see our Cookie Statement. The use of social media depends on the privacy settings you use on social media sites.
3. Your individual transaction details so that we can send you personalised tips and offers. We only do this if you have given your explicit consent.
4. Other sources of information, including public sources. We will always check first whether a public or other source of information can be used reliably.

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

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

### Social media

We use (our own) social media channels to discuss our organisation, products and services with clients, users of apps and visitors to the website. We do this so that we can offer useful, relevant information and/or answer questions we receive through social media. We use the internet and social media channels, such as Facebook and Twitter, for this purpose. In addition, we reply to individual, relevant questions and comments from other participants. We also use social media channels for marketing purposes. For more information about the use of

cookies, similar technologies and your settings, please see our Cookie Statement.

### Profiling and the use of advanced technologies

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

#### Profiling

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

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

#### Fraud prevention

We have a great deal of knowledge and experience in the area of fraud prevention. Unfortunately, we are faced with increasingly sophisticated forms of fraud. We may take measures, including profiling, to prevent fraud. For the sake of security, we cannot go into detail about the measures to be taken.

#### Fraud detection and payments

We carry out fraud detection activities in an effort to prevent clients and ICS from suffering potential losses as a result of fraud. We do this by creating a profile of you with the data you generate by logging on to our website and apps, and by making payments. One of the purposes for which these profiles are used is to enable decisions to be taken quickly by automated means. This is necessary to prevent the immediate execution of potentially fraudulent transactions. It also gives us an opportunity to assess the transaction and, if necessary, contact you. Please note that these systems do not guarantee all fraud will be prevented. You remain responsible for the use of your credit card, as detailed in the General Card Conditions.

#### Unusual transactions

As a bank, we have to comply with the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme - Wwft). We therefore pay particular attention to unusual transactions and to transactions that - by their nature - result in a relatively high risk of money laundering. To do this, we need to create and maintain a risk profile of you. If we suspect that a transaction is connected with money laundering or terrorist financing, we will report this to the authorities.

#### Duty of care, Client Centricity and risk management

The supervisory authorities expect us to do everything possible to reduce excessive lending, and to take faster action when clients are likely to get into financial difficulties. We may make use of profiling for this purpose too. In that case, we first make a list of the most common characteristics of clients who have found themselves in financial difficulties. These characteristics are combined to create the profile. We then check whether there are any clients who meet this profile. Finally, we determine what we can do to help these clients. The supervisory authority with responsibilities relating to the duty of care and client centricity expects banks to monitor the financial situations of their clients actively and continuously in order to prevent clients from overextending themselves. We always check the use of your data against the criteria laid down in the data protection legislation.

#### Client and product acceptance

How do we make use of profiling when you want to purchase a product? The following example explains how we do this. Imagine that you apply for a loan from us.

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

#### Direct Marketing

We use profiling to send you offers that are appropriate for you. For example, you have a specific product. You will not receive any offers from ICS for this specific product. We attempt to identify your areas of interest, based on a number of characteristics. We then look at specific aspects, such as your age category and whether you already have any other products from us. You will only be selected for a relevant marketing campaign if you meet a specific profile. Obviously, we check the data protection rules

to determine whether personal data may be used for that purpose. You may object to the creation of a personalised client profile for direct marketing purposes at any time.

If you do not have a contract with us, we determine whether direct marketing is permitted in specific situations.

### Automated decision-making

We may use automated decision-making if we enter into a contract with you.

If ICS makes a decision that has legal consequences for you or affects you to a significant degree, this will be done with the intervention of one or more competent employees. This also applies if the process that led to the decision is automated or if profiling was used. Examples include client acceptance or the reporting of unusual transactions to the authorities.

There are situations in which we use automated decision-making without any human intervention. This is permitted by law. These situations may concern decisions not to execute payments made using your credit card because they might be fraudulent. Such decisions may be made on the basis of an entirely automated process, without any human intervention.

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

### Personal data protection

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

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

For security reasons, we are unable to provide details of the precise measures we take. But you may have come across some of the following procedures we use to protect your personal data:

- Security of our online services
- We follow a two-step process to establish your identity (authentication)
- Security questions when you call us
- Requirements for sending confidential documents

Security is our shared priority. If, for example, you encounter breaches in our security, you can **report them** to us confidentially through the website.

### Warning system used by banks

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

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

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

### The internal reference register (IVR)

An internal reference register (Dutch acronym: IVR) is linked to the event records. Consequently, if we believe a client’s involvement in an event is sufficiently serious, we can warn the appropriate departments and group companies. This warning does not have any effect outside our organisation. We check the GDPR rules to determine whether it is permissible to share a specific event through the internal reference register within our organisation. When a client is included in this register, we provide specific information about the reasons for the inclusion in the internal reference register, the consequences of inclusion for the client and also the client’s relationship with us and our group companies, as well as the duration of the inclusion and the client’s rights, such as the right to object.

### The CAAML list

We also record if we have been forced to terminate our contractual relationship with you in accordance with the provisions of the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act, for example because you failed to provide us with sufficient information about where your money comes from or you are involved in money laundering or terrorist financing. In such cases, we may record your data in the CAAML list. This record is similar to the internal reference register in that it has no effect outside ICS. 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 ful fil our

obligations under the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act. Once again, we have a legitimate interest in this. If you are included in the CAAML list, you will be explicitly informed about this, as well as, among other things, the reasons for inclusion, the consequences for your relationship with the bank and its subsidiaries, and the duration of the inclusion and your rights, such as the right to object.

### The external reference register (ERR)

In addition to this, financial institutions in the Netherlands, including ICS, 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 ICS, 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.

### Your data outside Europe

Your personal data is processed outside Europe too. Additional rules apply in that case, the reason being that not all countries have the same strict data protection legislation as we do in Europe.

### Sharing personal data within the ABN AMRO Group

We may share your personal data outside Europe with other group companies of ABN AMRO Group. Our sharing of personal data is governed by the global internal policy, the Binding Corporate Rules (BCRs). These have been approved by the Dutch Data Protection Authority (Dutch DPA).

### Sharing personal data with other service providers

We may occasionally share your personal data with other companies or organisations outside Europe, for instance in the context of an outsourcing agreement. In that case, we ensure that we have concluded separate agreements with those parties, and that these agreements comply with the European standard, such as the EU's standard contractual clauses, and additional requirements.

### International payment transactions

There are situations in which you make use of our international financial services, for instance if you use your credit card abroad. In such situations, foreign parties, such as local supervisory authorities, banks, government bodies and investigative authorities, may ask us for your personal data, for instance so that they can carry out an investigation.

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

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

The General Data Protection Regulation and the Dutch GDPR Implementation Act (Uitvoeringswet AVG) do not give specific data retention periods for personal data. Other legislation may specify minimum data retention periods, however, which we must comply with. If it does, we are under the obligation to observe these periods. Such legislation includes tax laws or laws governing financial undertakings specifically (such as the Dutch Financial Supervision Act).

The length of time we keep personal data varies from a few months to many years. In many cases it is kept for seven years after your relationship with ICS ends. Personal data is deleted or anonymised once the retention periods have ended. Certain personal data may be kept for longer for various reasons, for instance, as part of our risk management, for security reasons, or in connection with claims, investigations or lawsuits.

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

## What rights do you have?

### Right to object

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

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

### Right to object to processing for direct marketing purposes

If you no longer want to receive offers for our products and services, you can unsubscribe at any time. All marketing messages include this possibility.

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

- You have the right to demand an overview of the data relating to you that we use.
- If your personal data is incorrect, you can ask us to change your personal data.
- You can ask us to erase your personal data at any time. We are not always able to do this, however, and we do not always have to comply with your request, for example if we are required by law to keep your personal data for a longer period of time.
- You can also ask us to temporarily restrict our use of your personal data.

This is possible in the following situations:

- You believe that your personal data is incorrect.
- We use your personal data wrongfully.
- We no longer require your personal data but you still need your personal data (for example following the storage period).
- If you submit an objection.

### Right to data portability

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

### Please keep your personal data secure

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

If you want to receive the personal data we hold on you or arrange for it to be passed on to another party? Please fill out the form below and send it to us:

**Request change of personal data handling**

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

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

You can find more information about ICS' complaints procedure here (only in Dutch).

Has your complaint already been dealt with by ICS' Complaint Management department and are you not satisfied with the solution? Then you can contact the Data Protection Officer at privacy.office@nl.abnamro.com. You also have the right to take your complaint to the Dutch Data Protection Authority.

If you have specific questions about this Privacy Statement, you can also contact the Data Protection Officer.

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

You can open and save our Privacy Statement on your smartphone, tablet or computer. Would you like to read back an earlier version of our Privacy Statement?

### Changes to the Privacy Statement

Changes to the law or our services and products may affect the way in which we use your personal data. If this happens, we will make changes to our Privacy Statement and notify you of these changes. We will post any changes on our website or in the app.