



Privacy statement Alfam

This privacy statement was published on 21 October 2022

Who is responsible for your data?

Alfam Holding N.V. is responsible for your data, as the Controller. (Alfam). Alfam is a wholly-owned subsidiary of ABN AMRO Bank N.V. (ABN AMRO Bank). Alfam offers loans through its brands: Alpha Credit Nederland B.V., Defam B.V., Credivance N.V., ABN AMRO Kredieten B.V. and GreenLoans, a trade name of Defam B.V. This privacy statement applies to the aforementioned lending brands of Alfam Holding N.V.

Do you have any questions about this privacy statement? If so, please email Alfam's Privacy Officer: privacyoffice@alfam.nl. ABN AMRO Bank has a data protection officer. An email to this officer can be sent to privacy.office@nl.abnamro.com.

Alfam Holding N.V. and your personal data

This privacy statement tells you how we handle your personal data. You may rest assured that we do so carefully. For some apps or websites, the use of personal data may differ from what we describe in this privacy statement. In those cases, you will find a different privacy statement in the app or be given additional information with the specific online service. We think it is important that you are aware of this and are not faced with surprises.

For whom is this privacy statement intended?

Are you a customer of ours or have you expressed interest in a particular product by making an enquiry or application, for example? If so, we use your personal data and this privacy statement applies to you. You may be visiting our website or using one of our apps. In that case too, we use your personal data and this privacy statement applies.

In addition, we may process personal data of individuals who do not have an agreement with us. For example, when we capture and use personal data of contact persons at companies to which we provide our services, of shareholders of these companies, or of Ultimate Beneficial Owners (UBOs) of these companies. We may also process data of persons who, for example, act as guarantors for our customers.

Are you one of these people? If so, this privacy statement is also for you.

Keep to read later?

You can save our privacy statement on your computer or send it to your email address.

Amendments to the privacy statement

Changes in the law or in our services and products may affect how we use your personal data. We will then adjust the privacy statement and inform you of this, for example through a notice on our website and in the My Environment.

Do you have a complaint or is something unclear?

Please contact us if you have any questions about this privacy statement. We're happy to help. You can send an email to privacyoffice@alfam.nl. Do you disagree with how we handle your data? Then send a letter to Alfam, customer service department, PO Box 178, 3980 CD, Bunnik. Or you can email info@alfam.nl.

What are personal data?

Personal data say something about a natural person. The best-known personal data are name, (email) address, age and date of birth. Your bank account, phone number, IP address and your Citizen Service Number (BSN) are also personal data. Then there are the 'special personal data'. This includes data about your health, for example. It also includes biometric personal data. This refers to a collection of techniques to measure and determine body characteristics of an individual. We may use biometric applications for identification purposes, among others. Examples are facial recognition or your fingerprint when you log into a mobile app. We may use these special personal data only if the law says so or if you give your consent. Otherwise, we are not allowed to use them.

Your data obtained from others

Suppose your partner also applies for a loan on your behalf. In that case, we may use the personal data we request about you. Sometimes we are even obliged to do so. This may also include data from other sources. Consider, for example:

- (public) registers containing your details, such as the Bureau Krediet Registratie (BKR) credit bureau;
- public sources, such as newspapers, the internet and sections of social media that are not private;
- files of other parties who have collected data about you, such as external marketing agencies or trade information agencies.

On what basis do we process your personal data?

Of course, we may not request or use your personal data without reason. The law states that this is only allowed if there is 'a basis for the processing'. This means that we may 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 perform an agreement, for example, if you want to take out a loan with us. Are you the representative of your company and does your company have or want an agreement with us? Or are you the contact person, shareholder, director or UBO of this company or one of our corporate customers? In such cases, we use your personal data and this privacy statement applies.

Legal obligation

There are many legal rules that we, as financial service providers, have to follow. These rules state that we must record your personal data and sometimes pass it on to others. These are a few examples of legal obligations we have to comply with:

- According to the Financial Supervision Act (Wft), we have a statutory duty of care. One example is that, as a financial services provider, we have to take measures to prevent excessive lending. This means we need to use your personal data to have a clear picture of your financial situation.
- We must take measures to prevent and combat fraud, tax evasion, terrorist financing and money laundering. How does this affect you? We ask you to identify yourself so that we know who you are. We will keep a copy of your identity document.
- Several laws require us to keep your personal data. For example, the Civil Code, the Prevention of Money Laundering and Financing of Terrorism Act (Wwft) and the Bankruptcy Act.

Other organisations may sometimes request data from financial service providers. Examples are the tax authorities, the Ministry of Justice (financial fraud) and intelligence agencies (e.g. terrorism). Furthermore, we sometimes have to share personal data with regulators, such as the Authority for the Financial Markets (AFM), the Dutch DPA (Data Protection Authority), De Nederlandsche Bank (DNB, the Dutch Central Bank) and the European Central Bank (ECB).

For example, if they conduct research on business processes or on certain (groups of) customers. As part of the Banking Disciplinary Act, we sometimes have to pass on 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 that case, it does not matter whether you are a customer with us or not. For instance, every financial institution must check whether customers or representatives of (business) customers are really who they say they are. Legitimate interest of the financial services provider or others. We may use your personal data if we have a 'legitimate interest' in doing so ourselves. We must then be able to demonstrate that our interest in using your personal data outweighs your right to privacy. In other words, we weigh all interests. We explain this with a few examples:

- We protect property and personal data belonging to you, to us and to others.
- We protect our own financial position (e.g. by estimating whether you can repay a loan), your interest and the interest of other customers.
- We perform fraud detection to help prevent losses due to fraud for you and for us.
- We will keep you informed of product changes.
- We want to run our administration efficiently. We centralise our systems, use other service providers, and conduct statistical and scientific research.

The use of personal data with or without your consent

In some situations, the law allows us to use your personal data without asking permission. These cases are as follows:

- if we need that data to comply with the law;
- if there is a legitimate interest of the financial services provider or a third party or;
- if the data are necessary for the agreement we enter into or wish to enter into with you.

Sometimes we do need to ask for your permission. If we do so in the future, we will provide you with information on why and for what we use your personal data. We will also indicate how you can withdraw your consent. We advise you to read that information carefully before giving consent.

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

- If we use biometric technology such as facial recognition for identity verification, for example.
- We use cookies and similar techniques on our websites and/or apps to provide you with personalised offers. You can read more about this in our Cookie Statement.
- If we need to access your location data in certain apps.
- If we use automated decision-making or profiling and the law states that we need your consent to do so.

What do we use your personal data for?

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

1. Agreement. To enter into and perform agreements with you.
2. Research. We investigate possible trends, problems or causes of errors and of risks. For example, to check whether new rules are properly enforced. This way, we can prevent complaints and damage. It also allows us to intervene or warn you in time if, for example, you can no longer repay your debts.
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.
4. Marketing. When you receive offers and news releases from us, they suit you. As a result, you will receive as little advertising as possible on products you already have or are unlikely to want. In doing so, we use personal data obtained from you. For example, because you once requested information or because you are already a customer with us. We may also use personal data obtained from others.
5. Our safety and integrity as a financial services provider and of our industry. We are obliged to safeguard the security and integrity of the financial sector. We may therefore 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 ensure our security and integrity as well as that of the financial sector, our employees and you, the customer. We may also use your data for alert systems.
6. Social responsibility and legal obligations. We help combat terrorist financing, money laundering and fraud. For example, by reporting unusual transactions or recognising, stopping, and, if necessary, verifying possible fraudulent transactions with you. Government agencies also request data from us when they want to investigate problems or criminal offences. We do check if there is a good reason for this. We also have to comply with many regulations as financial service providers. These are sometimes not EU or Dutch rules, but laws from other countries. This therefore requires us to record, store and sometimes give personal data to authorised bodies.

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 allowed.

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 match the purpose for which you had initially given us the personal data. This is called 'compatible use of data' in the law. The law does not say exactly when this is the case, but it does give indications:

- Is there a clear connection to the purpose for which you previously gave the personal data? Does the new purpose fit with that?
- How did we originally receive the personal data? From yourself or in some other way?
- What kind of personal data are involved exactly? Are they sensitive or less sensitive?

- What are the implications for you? Is the new purpose to your advantage, your disadvantage or is it neutral?
- What can we do to best protect your personal data? (Such as making it anonymous or encrypting it).

Our group and your personal data

We may share your personal data within the ABN AMRO Group (including its direct and indirect subsidiaries and branches and other entities) for certain purposes. Such as:

- for internal administrative purposes;
- to improve the service we provide to you;
- when the law says we must;
- to fulfil our duty of care.

Mandatory data

To conclude an agreement with you, we need personal data from you. Do you not want to give them, even though the law says you must if you wish to conclude the agreement? Or because they are necessary for the agreement? Then, unfortunately, we cannot enter into an agreement with you. Would you like us to remove your personal data from our systems? Unfortunately, this is not possible for all personal data. For example, there are data we have to keep by law. We may also need personal data to perform the agreement you have with us. Another possible reason is that, as a financial services provider, we have a legitimate interest in retaining certain personal data.

Camera images, phone calls and (video) chats

If you visit our office, we may make camera recordings of you. We do this for safety reasons. In some cases, we will have telephone contact with you. Perhaps in the future it will be possible to contact us via (video) chat. We may record phone calls, and any (video) chats. We do this to:

- improve our services (e.g. by coaching or assessing our employees);
- comply with a legal obligation;
- be able to provide evidence;
- prevent fraud.

We handle such image and sound recordings with care. They fall under the same rules as other personal data. In this regard you have certain rights, such as the right to inspect.

Other parties using your personal data

There are situations where your personal data is processed by individuals and bodies involved in our services. You can read below who they are.

Our service providers

We cooperate with other companies that help us with our services. This is called outsourcing. Your personal data may not be processed by them just like that. There are rules we have to follow as financial service providers. We choose these companies carefully and clearly agree how they will handle your personal data. We remain responsible for your personal data ourselves. Sometimes we engage other parties who also provide services,



such as lawyers, accountants, collection agencies or bailiffs. These parties are themselves responsible for the use of personal data.

Intermediaries

We work with intermediaries. So you may have taken out a loan with us through an intermediary. This intermediary 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 Office, the Public Prosecution Service, and other (government) agencies may request personal data about you. The law says when we have to pass it on. Employees in the financial sector are bound by Banking Disciplinary Law. In the event of a disciplinary case, we may have to disclose your personal data to the Banking Disciplinary Foundation.

Other financial service providers

Do you want us to disclose your personal data to other financial service providers? Then it is necessary for you to give your consent first. We are then obliged to pass on your personal data to these providers. If you yourself share your data with other parties, we are not responsible for the recipients' use of your personal data. The other party's privacy statement will then apply.

Potential buyers of-or investors in-a portfolio

We may disclose personal data to other parties if we are considering transferring our legal position vis-à-vis you to a potential buyer or investor. We do this, for example, if we want to sell your loan. This allows the other parties to make decisions on and for the transfer. This is a legitimate interest of Alfam and enables the acquiring party to fulfil its legal obligations, for example.

Use of your data for direct marketing

If you have previously purchased a product or service from a financial services provider, we may consider offering you our own similar products and services that best suit you. This also applies if you are a visitor to our website. To make the best possible offers, we can use different sources. You can read below which ones these might be:

- The personal data we have received from you for the agreement.
- When you visit our website, we may examine how you use it. We do this through your IP address. We can then make you personalised offers that are right for you. You must, however, have consented to the use of cookies and similar techniques, such as JavaScripts. You can read more about cookies in our Cookie Statement.
- Data via social media.
- Our ability to do so depends on your own privacy settings of your accounts on these social media.
- Other (public) sources of information.
- We always check beforehand whether the use of a (public) source of information is reliable. If necessary, we will check whether you as a customer have consented to the use of personal data we have obtained from another party.

Social media

We engage with customers, app users and website visitors about our organisation, products and/or services through (our own) social media channels. We do this to provide useful information and/or answer questions that come in via social media. We use the internet and social media channels, such as Facebook and Twitter, for this purpose. We also participate in discussions on these channels and/or answer individual, useful questions and comments from other participants. We may in those instances record personal data. We process these according to this privacy statement.

Profiling

As a financial services company, we use profiling. Below you can read regarding what and at what times we do this.

Anti-fraud

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

Unusual payments

As a financial services provider, we must comply with the Money Laundering and Terrorist Financing Prevention Act (Wwft). We therefore pay particular attention to unusual transactions and those that by their 'nature' carry a higher risk of money laundering. This requires establishing and maintaining a risk profile of the customer, including you. If we suspect that a transaction is related to money laundering or terrorist financing, we report it to the authorities.

Duty of care and risk management

Regulators expect us to do as much as we can to prevent excessive lending. And they expect us to intervene more quickly if a customer is at risk of financial difficulties. We can also use profiling for this purpose. In doing so, we first make a list of the most common characteristics of customers who have run into financial difficulties. These characteristics make up the profile. We then look if there are any customers who fit this profile. Finally, we determine what we can do to help these customers.

Customer acceptance and product acceptance

How do we use profiling when you want to buy a product? We explain this with an example. Suppose you apply (online) for a loan from us. We then take the following steps:

- Upon request, we will inform you about how we draw up a profile and the things you can take into account.
- We make a risk analysis. We do this if you are a new customer, but also if, as an existing customer, you want to buy other products from us. We know from experience that certain characteristics are an indication of whether or not you will be able to repay a loan properly later on. For example, whether you have a job or debts. We assess these characteristics.
- Customers who can normally repay a loan share a number of characteristics. And so do customers who can't. Based on your characteristics, we draw up a profile.

- We compare your profile with our existing profiles. Then we estimate the risk of whether you can repay the loan.

Direct marketing

We also use profiling to make you appropriate offers. Suppose you have a loan. If so, you will not receive offers from us for this. Based on a number of characteristics, we try to find out where your interests do lie. For example, we will look at an age range and whether you already have other products with us. Only if you fit a certain profile will you be selected for a relevant marketing campaign. Of course, we test the use of personal data against privacy rules. You can always object to the creation of a personalised customer profile for direct marketing purposes. Please email privacyoffice@alfam.nl.

If you do not have an agreement with us, we will check whether direct marketing is allowed in certain situations.

Automated decision-making

We may use 'automated decision-making' when we enter into an agreement with you, for example for a loan. This means that our software automatically makes a decision based on personal data, without the intervention of a real person. If we make a decision that has legal consequences for you, or that 'significantly affects' you, this is always done with the intervention of one or more authorised employees. This is also the case if the process leading to the decision is automated or if profiling may have been used. One example is reporting unusual transactions to the authorities.

If in the future we also want to use automated decision-making that has legal consequences for you or 'significantly affects' you, we will clearly indicate this in advance. We will then let you know your rights. For example, the right to get an explanation of the automated decision, the right to let us know your point of view, the right to challenge this decision and the right to human intervention.

Security of your personal data

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

- We 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 give details of exactly what measures we take. Here are a few examples of security measures you may have encountered:

- Securing our online services.
- Establishing who you are (authentication) in two steps.
- Security questions when you call us.
- Requirements on how to send confidential documents.

Safety is something we also want to continue working on together with you. For example, to counter phishing. Phishing is a form of fraud where a consumer is lured to a particular (fake) website to fill in personal details. Have you encountered phishing (or suspected it)? If so, please report this to us as soon as possible by sending an email to compliance@alfam.nl.

The alert system of banks and financial service providers

To protect the safety of the financial sector, financial institutions in the Netherlands have developed an alert system. This allows them to check whether someone:

- ever committed fraud;
- ever tried to defraud;
- otherwise poses a threat to industry security.

You can read more about this alert system and how it works on the site of the Dutch Banking Association (NVB).

Your personal data outside Europe

Your personal data is also processed outside Europe. Additional rules apply for this, as not all countries have the same strict privacy rules as the European Union.

Sharing of personal data within our group

We may share your personal data outside Europe within the ABN AMRO Group (including its direct and indirect subsidiaries and branches and other entities). We do this according to our global internal policy, the Binding Corporate Rules (BCRs). This policy has been approved by the Dutch DPA.

Sharing personal data with other service providers

Sometimes other companies or agencies outside Europe process your personal data. For example, under an outsourcing agreement. We then ensure that we have entered into a separate agreement with those parties that meets European standards, such as the 'EU model clauses'.

How do we determine how long we keep your personal data?

We keep personal data as long as necessary to achieve the purpose. The General Data Protection Regulation (GDPR) does not specify retention periods for personal data. Other laws may well contain minimum retention periods that we must adhere to. Examples include the general administration obligation for companies (Civil Code), tax legislation or legislation for financial companies (Financial Supervision Act).

After the expiry of the retention period, we anonymise the personal data which means that the data can no longer be traced back to a person and are therefore no longer personal data.

In addition, there are reasons to keep customer data longer. For example, for our risk management, for security reasons or to properly deal with claims, investigations or lawsuits. Where possible, we then keep this customer data in an archive and not in our day-to-day systems.

What rights do I have?

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 we may sometimes do so even if you object. For example, to fight fraud, manage risks or investigate unusual

transactions. Of course, we abide by the law in doing so. However, you can always object to the creation of a personalised customer profile for direct marketing purposes via your cookie settings.

Right of objection for direct marketing

If we send you offers for our products and services and you no longer wish to receive them, you can unsubscribe at any time. You can do this with every marketing message.

Inspection, rectification, erasure, 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, there are some cases in which we cannot do this, and others in which we are not obliged 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:
 - if you believe your personal data are incorrect;
 - if you believe we make wrongful use of your personal data;
 - if we no longer need your personal data, but you still need them (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 transfer 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 to whom you want to give your personal data wants to use it for. For example, read the privacy statement on that party's website.
- Would you like to receive your personal data? Then make sure that your own equipment is secure enough and, for example, has not been hacked (or cannot be hacked). Your financial data could be of great interest to criminals.

Exercising customer rights

To exercise your customer right, please send a letter to Alfam, customer service department, PO Box 178, 3980 CD, Bunnik. Or send an email to info@alfam.nl. In connection with the verification of your identity, we will ask you to answer some verification questions when exercising a customer right.

The data protection officer oversees the application of and compliance with the AVG within ABN AMRO Bank's organisation. Biometrics: a collection of techniques to measure and determine an individual's body characteristics, e.g. Face ID or voice recognition. We may use biometric applications for identification purposes, among others.

Special personal data: data so sensitive that its use could seriously affect an individual's privacy. The law lists special personal data as follows: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a person, or data concerning health, or data relating to a person's sexual behaviour or sexual orientation.

Profiling: The Privacy Act defines 'profiling' as follows: 'Any form of automated processing of personal data which uses personal data to evaluate certain personal aspects of a natural person, in particular with the aim of analysing or predicting job performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or travel.' The law therefore allows profiling. This is a general definition that also applies to other responsible parties within the meaning of the Privacy Act. So it is not the case that the bank will use your personal data to evaluate your professional performance or health.

EU Model Clauses: A set of standard contracts drawn up by the European Commission. ABN AMRO Group also uses these standard contracts when personal data needs to be transferred to a country that does not have the same level of protection as within the European Union.

Autoriteit Persoonsgegevens (the Dutch DPA (Data Processing Authority)): the privacy regulator in the Netherlands. ABN AMRO Group: ABN AMRO Group N.V. and its direct and indirect subsidiaries and branches and other entities in which ABN AMRO Bank N.V. has a controlling interest. In this privacy statement, a controlling interest means that ABN AMRO Bank N.V. owns more than 50% of the shares in these entities.

Ultimate Beneficial Owner: The UBO is the person who ultimately owns or controls a company or institution. *Processing:* Processing personal data is a broad concept. It is everything that can be done with personal data. 'Use', 'destroy' or 'provide' are forms of processing. In the privacy statement, you will read about both 'processing' and 'using' personal data.