# Privacy statement - glossary of key terms

**Personal data:** The General Data Protection Regulation (GDPR) defines personal data as any information concerning an identified or identifiable natural person. This means that the information is either related directly to someone (such as a name and an identification number) or traceable back to that person (for example using an IP address). Information relating to deceased persons or organisations is not considered personal data under the GDPR.

ABN AMRO's **Data Protection Officer** monitors the application of, and compliance with, the General Data Protection Regulation (GDPR) at the bank.

**Biometrics**: a collection of techniques used to measure and identify an individual's body features, such as facial recognition or voice recognition. We cannot use biometric applications for identification and other purposes unless we have obtained your prior explicit consent.

**Special categories of personal data**: personal data that is so sensitive that its use may seriously affect an individual's privacy. The GDPR contains the following list of special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**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 is a general definition that also applies to other controllers within the meaning of the GDPR. The bank will not use your personal data to evaluate your performance at work or your health.

**EU Model Contract Clauses:** The Model Contract Clauses, which are also referred to as *standard contractual clauses,* or SCCs, are standardised contractual clauses that were drafted by the European Commission. ABN AMRO Group also uses these standardised contractual clauses if it is required to transfer personal data to a country that does not offer the same level of protection as EU countries.

**Dutch Data Protection Authority:** the data protection authority in the Netherlands.

**ABN AMRO Group**: ABN AMRO Bank N.V. and its direct and indirect subsidiaries, branches and other entities in which ABN AMRO Bank N.V. has a majority stake. For the purpose of this privacy statement, a majority stake means that ABN AMRO Bank N.V. holds more than 50% of the shares in the relevant entity.

**Guarantor:** A guarantor is required to fulfil a client's financial obligations towards the bank if the client fails to fulfil them. The guarantor gives this undertaking in a contract that the guarantor concludes with the bank.

**UBO**: The UBO is the person who is the ultimate beneficial owner of a business or institution or who controls a business or institution.

**Processing:** Personal data processing is a broad concept that encompasses everything that can be done with personal data. “Using”, “destroying” and “providing” are all forms of processing. The privacy statement refers to both the processing and use of personal data.

**Warning system used by banks:** ABN AMRO - like other banks - has its own incident register. For example, if a client attempts to commit fraud, ABN AMRO can enter a certain amount of data relating to this client in its own internal reference register (Dutch acronym: IVR). If the incident is considered serious, information might be shared with other banks, in which case the data will also be entered in the external reference register (Dutch acronym: EVR). We are not permitted to do this without good reason, and strict conditions must be fulfilled when sharing information.

Warning other banks is permitted, because ensuring an ethical financial system is of great importance to society. The conditions set out the Financial Institutions Incident Warning System Protocol (Dutch acronym: PiFi) must always be met. The aim of this protocol is to ensure the security of the financial system. If you would like to know more, you can find further information about the warning system used by banks on the website of the Dutch Banking Association (NVB).

**CAAML list:** This list, like the IVR, is an internal list kept by the bank, although it serves a different purpose. We also make an entry in this list 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.