Privacy Policy

(version effective as from 31.05.2021)

Protecting your personal data is very important to us. This Privacy Policy informs how Aion SA (“us”, “we” or “our”) collects and processes your personal data, notably through your use of the ROI Mobile App (“App”) or the website www.roi-app.com (“Website”); jointly called “Services” and their functionalities, including any data you may provide through this Website when you sign up to a product or service.

For the purpose of the relevant data protection legislation, the data controller responsible for your personal data is Aion SA whose registered office is located at avenue de la Toison d’Or 26/28, 1050 Brussels.

We have appointed a data protection officer (“DPO”) who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise any of your legal rights, please contact the DPO using the details set out below:

a. App: Customer Support (logged Users),
b. Email address: dpo@aion.be
c. Postal address: Aion SA, avenue de la Toison d’Or 26/28, 1050 Brussels.

It is important that the personal data we hold about you is accurate and up to date. Please inform us about any relevant changes during your relationship with us using the contact details as set out in the previous paragraph.

Terms not otherwise defined in this Privacy Policy have the meaning given to them in our Terms and Conditions which are available on our Website.

Our App or Website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third-parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our Services, we encourage you to read the privacy notice of every third-party website you visit.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

WHAT DATA WE COLLECT ABOUT YOU

Personal data, or personal information means any information about an individual from which the person can be identified. It does not include data from which the identity of the natural person cannot be derived (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

a. Identity Data like your first and last name, date of birth, National Registration number, copies of identification documents and any other information we need to verify your identity or prove your eligibility to use our Services.
b. Contact Data includes billing address, delivery address, e-mail address and telephone number.
c. Financial Data is data collected and processed in order to provide you with financial products and services. This may include your identification number and bank account numbers, credit or debit card numbers, information on your savings and investments, loans and credits, information necessary to assess your creditworthiness (information about your employment and salary, credit history, marital status and family composition, education).
d. Transaction Data includes details about payments to and from you like account and card numbers, date, time, amount, currencies used, exchange rate, beneficiary details, details on the location of the merchant or CDM/ATM, IP address of sender and receiver, sender's and receiver's name, registration information, device information used to facilitate the payment and other details of services you have selected and the mandate you have given us.
e. Marketing and Communications Data includes your preferences in receiving marketing from us and your communication preferences.

We also collect, use and share Aggregated Data such as statistical or demographic data. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

FAILURE TO PROVIDE PERSONAL DATA

Where we need to collect personal data by law, or under the Investment Terms we entered with you and you fail to provide that data when requested, we may not be able to perform the obligations we have. In this case, we may have to terminate your Account but we will notify you if this is the case at the relevant time.

HOW WE COLLECT PERSONAL DATA

Direct interactions. This is information you give us by filling in forms on the App or the Website. You give us the information when you create an account or do a transaction. The information may include Identity Data, Contact Data, Financial Data, Transaction Data.

Third parties or publicly available sources. We may receive personal data about you from third-party and public sources as set out below:

a. Banks you use to transfer money to the account(s) you hold with us;
b. Business partners such as those who offer complementary services (such as investment advisory),
c. Credit reference agencies, fraud prevention agencies or data brokers, including bodies charged with tasks in the public interest (e.g. the Official Belgian Gazette, the Central Individual Credit Register (CICR) and the file of non-governed registrations (ENR) of the National Bank of Belgium (NBB),
d. Advertising networks, analytics providers and search information providers based inside and outside the EU,
e. Providers of technical, payment and delivery services.

Specific cases of personal data collection. In some cases we can collect information about you whereas you do not have a direct relationship with us in the capacity of one of our clients as such. This may happen if you are for example the beneficiary of a payment made by one of our clients or if you are a client's

a. family member or heir
b. co-borrower / guarantor,
c. legal representative or contact person;
d. ultimate beneficial owner (UBO)
e. debtor (in case of bankruptcy),
f. creditor (in case of seizure requests);
g. shareholder, director or partner,
h. staff member.

LEGAL GROUNDS AND PURPOSES FOR WHICH WE PROCESS YOUR PERSONAL DATA

We will only process your personal data in accordance with the applicable laws, for the following legitimate purposes and based on the following legal grounds.

Contract. We need your personal data to conclude a contract with you and to carry out our obligations relating to your contract with us or in order to take steps at your request prior to entering into a contract.

If you have not concluded a contract with us, we do not process your personal data on the basis of a contract. We may, however, use your personal data for other purposes, such as fraud detection. We always check first whether using your personal data for those other purposes is permitted.

Legal obligation. We process your personal data to adhere to statutory requirements. As a bank we are subject to various legal obligations which require us to process your personal data. These include our obligations to combat and prevent fraud, money laundering and terrorist financing (AML-CTF) and our obligation to adhere to the rules of conduct in economic and financial law. In some cases, we are also subject to the obligation to disclose your personal data to judicial authorities, intelligence agencies and regulatory and supervisory authorities such as the Financial Services and Markets Authority (FSMA), the European Central Bank (the ECB), the National Bank of Belgium (NBB) and the Federal Public Services Economy and Finance (FPS Economy & FPS Finance). We must also comply with a number of obligations in application of the Foreign Account Tax Compliance Act (FATCA).

Legitimate interest. We have the right to process your personal data if it is necessary for the purposes of the legitimate interest pursued by the controller (us) or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms. Legitimate interests on the basis of our processing activities are for example the following:

a. Research. We study possible trends, problems, root causes of errors and risks in order to prevent complaints and losses. This way, we are able to intervene and issue a warning in time, if need be. We also study trends and our clients' preferences for the purpose of analysation and continuous development of the products and services we offer.
b. New and improved products and services. We use our clients' personal data for the purpose of deploying and developing our products and services in order to keep up with our clients' evolving wishes and expectations.
c. Marketing relating to our products and services. We process your personal data for the purpose of direct marketing communications through analysing your needs, preferences, habits and situation, and to market and/or communicate our products and services to you.
d. Risk management and protection of our legal rights. We use your personal data for the purpose of improving our risk management and to defend our legal rights, including:
    1. providing evidence of transactions you are involved in or communications between you and us;
    2. fraud prevention, for instance by detecting theft of your identity or credentials (e.g. phishing, theft of your ID document), unauthorised access to your data or device (hacking attempts);
    3. IT management, including infrastructure management, business continuity and IT security;

4. establishing statistical models, (e.g. in order do to assess your credit risk score);
5. performing internal control and audit;
6. enforcement of claims and defence within legal disputes.

Public interest. We have the right to process your personal data if and insofar as it is necessary for reasons of substantial public interest (such as ensuring effective AML-CTF processes).

Further processing. We may use your personal data for other purposes than the purpose for which your personal data was initially collected. In that case, the new purpose must be in line with the purposes for which your personal data was initially collected. In those cases, we will always check first if such further use of personal data is permitted, taking into account your rights and interests.

HOW WE USE YOUR PERSONAL DATA FOR PROFILING AND AUTOMATED DECISION-MAKING

As a credit institution, we make use of profiling. This entails that in certain situations we automatically assemble a profile using a set of your personal data. We do this for purposes of fraud detection when (potentially fraudulent) payment transactions are initiated, unusual transaction detection (based on risk profiles), and direct marketing.

We make use of systems to make automated decisions. This helps us to make sure our decisions are quick and based on what we know. Automated decisions may affect the range of products, services or features offered to you now or in the future, or the price that we charge you for them. They are based on personal information that we have or that we are allowed to collect from others. Here are the types of automated decisions we make:

1. As a credit institution, we make use of profiling. This entails that in certain situations we automatically assemble a profile using a set of your personal data. We do this for purposes of fraud detection when (potentially fraudulent) payment transactions are initiated, unusual transaction detection (based on risk profiles), client and direct marketing.
2. We make use of systems to make automated decisions. This helps us to make sure our decisions are quick and based on what we know. Automated decisions may affect the range of products, services or features offered to you now or in the future, or the price that we charge you for them. They are based on personal information that we have or that we are allowed to collect from others. Here are the types of automated decisions we make:
    1. Detecting fraud. We use your personal information to help decide if your account(s) may be being used for fraud or money-laundering. We may detect that an account is being used in ways that fraudsters work. We may also notice that an account is being used in a way that is unusual for

you or your business. If we think there is a risk of fraud, we may stop activity on the account(s) or refuse access to them.

2. Opening accounts. We check that you or your business meet the conditions needed to open the account. This may include checking age, residency, nationality or financial position
3. You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or otherwise similarly significantly affects you. You can object to such automated decision-making, including profiling, by adjusting the settings in our App. We may perform a manual double check upon your request.
4. You do not have this right if the automated decision-making is authorised by applicable laws we are subject to.

3. You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or otherwise similarly significantly affects you. You can object to such automated decision-making, including profiling, by adjusting the settings in our App or. We may perform a manual double check upon your request. You do not have this right if the decision is authorised by applicable laws we are subject to.

WHO DO WE SHARE YOUR PERSONAL DATA WITH

In order to fulfil the aforementioned purposes, we only disclose your personal data to:

a. Know Your Customer (KYC), analytical and cyber security providers,
b. Other service providers which process personal data on our behalf, we do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.
c. Organisations set up for detection and prevention of terrorism.
d. Financial or judicial authorities, state agencies or public bodies, upon request and to the extent permitted by law,
e. any other third party, but only subject to your prior consent.

INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA

In case of international transfers originating from the EEA to a non-EEA country which the European Commission has recognised as providing an adequate level of data protection, your personal data will be transferred on this basis. For transfers to non-EEA countries of which the level of protection has not been recognised by the European Commission as adequate, we will either rely on a derogation applicable to the specific situation (e.g. if the transfer is necessary to perform our contract with you such as when making an international

payment) or implement one of the following safeguards to ensure the protection of your personal data:

a. Standard contractual clauses approved by the European Commission;
b. Binding Corporate Rules.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third-parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

HOW LONG DO WE KEEP YOUR PERSONAL DATA

We will retain your personal data for the duration required for the purposes of processing as set out above, in order to comply with applicable laws and regulations or as is necessary with regard to our operational requirements, such as account maintenance, facilitating client relationship management, and responding to legal claims or regulatory requests.

The period for which we will retain information about you will vary depending on the type of information and the purposes that we use it for. For instance:

a. data used for AML purposes — for 10 years as of the single transaction or as of the end of the contractual relationship;
b. data kept as a proof of transactions — for 10 years as from processing of the transaction concerned;
c. customer complaints — for 5 years as from the complaint concerned;
d. prospects data used for marketing purposes — for 3 years from the collection of the data concerned;
e. FATCA and CRS documents — for 7 years as from the 1st of January following the year of account closing, the statement or the operation.

WHAT ARE YOUR RIGHTS AND HOW CAN YOU EXERCISE THEM

In accordance with applicable regulations, you have the following rights:

a. To access: you can obtain information relating to the processing of your personal data, and a copy of all your personal data that is processed by us.
b. To rectify: when you consider that your personal data are inaccurate or incomplete, you can require that such personal data be modified or completed accordingly.
c. To erase: you can require the deletion of your personal data. We are not always able to do this, however, and we do not always have to agree to do this, for example if we are required by law to keep your personal data for a longer period of time.
d. To restrict: you can request a restriction of the processing of your personal data if:
    1. you think that your personal data is incorrect;
    2. you think that we are not supposed to process your personal data;
    3. we want to destroy your personal data but you still need it (e.g. after the retention period has ended).
e. To object: you can object to the processing of your personal data, on grounds relating to your particular situation. You have the absolute right to object to the processing of your personal data for direct marketing purposes, which includes profiling related to such direct marketing.
f. To data portability: where legally applicable, you have the right to have the personal data you have provided to be returned to you or, where technically feasible, transferred to a third party.
g. To withdraw your consent: where you have given your consent for the processing of your personal data, you have the right to withdraw your consent at any time. h. To ask that we do not make our decision solely based on automated processes, including profiling. You can object to such an automated decision, and ask that a person review it unless such decision is authorised by applicable law to which we are subject.

You can exercise the rights listed above using the details set in Point 3. Please note that in case you contact us by Email or post you are required to provide at least your first and last name, signature and a copy of your ID document. Otherwise we won't be able to identify you and, consequently, take actions on your request. If you make a request on behalf of someone else, you must provide evidence of your authority to make such a request.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We try to respond to all legitimate requests within one month.

To do so, please contact by emailing us at dpo@aion.be.

COMPLAINTS

If you have any complaints regarding this Privacy Policy or on how we protect or use your data, please contact our DPO using the contact details as set out above in Point 3. Please note that in case you contact us by Email or post you are required to provide at least your first and last name, signature and a copy of your ID document. Otherwise we won't be able to identify you and, consequently, reply to your complaint.

If you have any concerns about our use of your personal data or if you feel like we have not addressed your questions or concerns adequately, you have the right to lodge a complaint at any time with the Belgian Data Protection Authority, which regulates and supervises the processing of personal data in Belgium, by e-mail to contact@apd-gba.be, via their helpline on +32 (0)2 274 48 00 or by writing to Rue de la Presse 35, 1000 Brussels; or We would, however, appreciate the chance to deal with your concerns before you approach the relevant authority so please contact our DPO in the first instance.

FEE

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

GOVERNING LANGUAGE

This Privacy Policy has been drafted in English. If this Policy is translated into another language and there is a conflict or inconsistency between the English language text and the translated text, the English language text prevails.

CHANGES TO THIS POLICY

As changes in the law or in our services and products may affect the way we use your personal data, we reserve the right to amend or modify this Privacy Policy, in accordance with the applicable laws. We will inform you of any material changes through our App or Website or through other usual communication channels. Your continued use of the App or Website after a modification of this Privacy Policy entails your acceptance of the modified Privacy Policy.