

Privacy Policy

We are committed to protecting and respecting your privacy.

We:

- will always keep your personal data safe and confidential;
- will never sell your personal data;
- allow you to manage your communication preferences at any time.

About Deblock

Deblock SAS ("Deblock"), with an address at Talent Garden - 100, Av. Willy Brandt, 59777 Lille, France, is an electronic money institution authorised approved by the "Autorité de Contrôle Prudentiel et de Résolution" ("ACPR", 4 place de Budapest CS 92459 75436 Paris Cedex 09, 01.49.95.40.00) registered under CIB 17748.

Deblock is also registered as a Digital Asset Service Provider ("PSAN") with the "Autorité des Marchés Financiers" ("AMF") for the purchase/sale of digital assets against legal tender and the exchange of digital assets for other digital assets under number E2023-081.

Scope

Deblock, as a data controller, is required to collect, process and store your personal data when you use our deblock.com website or our mobile application. This concerns our customers but also prospects.

When we mention "personal data", we mean information:

- about you and of which we are aware of;
- that can be used to personally identify you (for example, a combination of your name and postal address).

This policy sets out what information we collect, how we use it and your rights if you wish to change the way we use your personal data.

If you have any questions about how we use your personal data, you can contact us at the following address: dpo@deblock.com.

Which personal data do we collect?

Deblock may collect and process the following categories of personal data:

- identification data: title, surname, first name(s), gender, date and place of birth, nationality, two-sided video of one or more identity documents, proof of identity, and authentication pictures (which may undergo biometric processing);
- contact data: postal address, e-mail address, telephone number;
- data related to your professional situation: type of job;
- economic and financial information: income (amount, sources and supporting documents), tax residence, consumption habits and uses;
- financial and transactional data: in particular the nature of the operations, date, card payments, transfers, direct debits, amounts, descriptions, justifications for the operations, bank details;
- connection data related to the use of our services: identification and authentication data, logs;
- data from correspondence and communications between you and us, carried out remotely: instant messaging, communications on social networks, complaints or any other type of communication;
- data of the device used to connect to the application and data associated with the use of the Deblock application: in particular dates and times of access to the Deblock service, data on the telephone, data associated with the use of the device, unique identifiers, crash data;
- geolocation data: GPS data of the device used;
- data and information intended to be communicated to the public and shared with other customers within the Deblock application: profile and wallpaper photos, images, photos related to the operations carried out (which may be subject to processing biometrics), comments and other messages;
- data provided within the framework of additional services such as the numbers as well as the e-mail addresses present in the Customer's address book (only if the Customer chooses to link his contact directories to the Deblock application in order to know which of his contacts use the Deblock app;
- any other information or document necessary to find the origin and destination of funds for transactions carried out with your account.

These personal data are collected either directly from you by Deblock, or indirectly from:

- the General Directorate of Public Finances;
- from any judicial or financial authorities, State agencies or public bodies, in accordance with the regulations;
- from all public sources relevant to the purposes pursued.

Finally, when relevant, some of the data or types of data mentioned above may be reconciled in order to better meet the purposes described below.

These reconciliations are always made taking care to use only the data strictly necessary for the achievement of the objective pursued by the processing (in application of the so-called principle of "minimisation" provided for by the applicable regulations).

How do we access, process and store your data?

The personal data referred to in the previous paragraph are processed, depending on the situation, to meet different purposes. Each of these purposes is associated with a type of personal data and a retention period beyond which these data are anonymised and/or deleted, except for some of them which may be subject to archiving with restricted access for a fixed term.

The different purposes that lead us to process your personal data are as follows:

- management of the business relationship, the account and/or the products and services subscribed to, in particular for the purposes of proof. Your personal data may be kept for a period of five (5) years from the end of the business relationship or, where applicable, from the end of any legal or recovery proceedings;
- carrying out opinion and satisfaction surveys and statistical studies. Your personal data may be kept for a period of three (3) years from the completion of the study;
- the fight against fraud (examples: establishment of ratings or scores, detection of atypical transactions). Your personal data may be kept for a maximum period of five (5) years from the closing of the proven fraud file or the issuance of an alert in our systems;
- compliance with legal and regulatory obligations incumbent on Deblock, in particular know-your-customer obligations, operational risk management (including

computer network security, customer protection, internal supervision and control, security of transactions as well as the security of the use of international payment networks), obligations in terms of financial security (fight against money laundering and the financing of terrorism and obligations in terms of sanctions and embargoes), obligations relating to the determination of your tax status and compliance with associated tax regulations, ethics and the fight against corruption, data protection and all other obligations relating to the management and management of compliance risks. For these purposes, your personal data may be shared between entities of the Deblock Group. They will be kept for a period of five (5) to ten (10) years from the triggering event provided for by the regulations in force (example: in terms of activation, loading and use of electronic money, five years from the execution of these operations);

- the prevention and detection of criminal offences and/or taking legal action (example: for the identification of seriously reprehensible behaviour or acts such as violence against Deblock personnel). Your personal data may be kept for a period of five (5) to twenty (20) years, depending on the nature of the infringement, from the day of its discovery. When legal proceedings are initiated, the data is kept until the end of this procedure and the expiry of the applicable limitation periods;
- the management of dormant accounts and data related to the search for data subjects. Your data may be kept for a maximum period of thirty (30) years depending on the cases provided for by the Eckert law;
- the recording of your conversations and communications with Deblock, whatever their medium (e-mails, letters, chat, etc.). According to the applicable regulations, your personal data may be kept for variable periods which may not however exceed a period of five (5) years from their registration. The recording media or their reproduction will be kept for periods proportionate to the purpose of the recording in question (6 months for staff training purposes);
- accounting processing: accounting data may be kept for a period of ten (10) years in accordance with the legal provisions in force;
- research or analysis activity for the purposes of process improvement and model development. Your data may be used to improve our internal control procedures or contribute to risk and compliance management. These data are kept for a determined period for each of these sub-purposes;
- commercial prospecting, the proposal of commercial offers adapted to your situation and your consumption profile, the realisation of promotional offers and games, commercial animations and advertising campaigns. The data may be kept for a maximum of three (3) years from the end of the commercial relationship or for prospects, from the last contact. This data may be anonymised and aggregated in order to establish statistical reports;
- access the users' GDrive/iCloud for the sole purpose of extracting their AES-key which is used to encrypt their RSA-key.

Your data collected and processed in accordance with the aforementioned purposes may be kept for an additional period if the defence of a right or interest so requires, or in order to meet the requirements of the French or European authorities. In this case, your data will not be used for other purposes, they will be kept in intermediate archiving and will only be accessible to authorised persons with a need to know (examples: legal department, compliance department, audit body and inspection).

Certain specific processing operations, due to the personal data they involve or their purpose, require the application of additional provisions.

Remote identity verification and recovery

In order to verify your identity remotely and to comply with its legal and regulatory obligations relating to identification, identity verification and knowledge of its customers, Deblock is required to collect the following data directly from you:

- a double-sided colour video of your official identity document (national identity card or European passport or valid residence permit); and
- a selfie video of your face taken in colour with the front camera of your mobile phone, of sufficient quality and brightness and not showing any digital alteration. This video is processed to attest to the liveness of the subject but only pictures are saved and kept by Deblock.

To do this, you must allow Deblock to access your mobile phone's cameras and then take the required videos. Once recorded those videos and/or pictures may, if necessary, be viewed by one of our specially authorised employees in order to authenticate you.

Once we have verified your identity, this data will be subject to intermediate archiving: it will only be consulted on an ad hoc and motivated basis (in the event of a request to recover your account) by specifically authorised persons.

A specific technical processing of biometric data (within the meaning of Article 4.14 of the GDPR) is carried out by Deblock for the purpose of verifying your identity remotely. This specific technical processing of facial images makes it possible to confirm the unique identification of a client based on their physical, physiological or behavioural characteristics. It also allows the detection of the "liveness" character of the customer's face to verify that it has not been subject to physical or digital alteration. These biometric data are considered sensitive within the meaning of the GDPR. In order to use this processing in accordance with Article 9 of the GDPR, we justify a specific need to identify our customers to allow access to our services.

Profiling

Deblock implements profiling processing, i.e. processing consisting in evaluating certain aspects of its customers concerning their economic situation, their personal preferences or centres of interest, the analysis of their behaviour, or even their location and their movements.

This profiling processing has different purposes, mainly to secure your operations, fight against fraud, personalise the relationship, commercial prospecting or to better meet our obligations relating to the management of compliance risks.

For each of these profiling processing, an in-depth analysis is carried out in order to determine whether the processing must be based on your consent, the legitimate interest of Deblock, or on another legal basis (the execution of a contract, an obligation legal).

If the profiling is based on your consent, we ensure that your consent is collected, after having informed you explicitly and transparently about the use of your personal data. We also allow you to withdraw your consent at any time.

If the profiling is based on our legitimate interest, we will have carried out a prior analysis allowing us to ensure, for each processing operation envisaged, that your interests and fundamental rights are respected and that you can reasonably expect that your data will be used in this frame. We allow you at any time to oppose this processing, under the conditions provided for by the regulations and according to the methods described in this policy.

Fully automated decisions

In cases where Deblock implements data processing involving fully automated decision-making, including profiling, and producing legal effects concerning you or significantly affecting you, such processing is based on one of the following legal bases: your consent, the execution of a contract, our legitimate interest or a legal obligation. This processing is carried out in accordance with the applicable regulations, and accompanied by appropriate guarantees.

In the event that this profiling has legal consequences for you, you can request the intervention of a human person, in particular in order to obtain a re-examination of your situation, to express your own point of view, to obtain an explanation of the decision taken or to challenge the decision.

Legal bases for data processing

The processing carried out by Deblock is based on one of the following legal bases:

- the execution of any contract concluded with you (example: our Terms and Conditions);
- compliance with the legal and regulatory obligations applicable to Deblock (example: fight against money laundering and the financing of terrorism);

- the pursuit of the legitimate interests of Deblock (example: fight against fraud, research and development activities, commercial prospecting, including profiling);
- consent (example: use of biometric data for identification purposes);
- safeguarding the vital interests of the person concerned or of another natural person, when a customer has paid by bank card for a product or service presenting a threat to the safety of persons (recall of defective products, health crisis, etc.).

Can we share your data?

Your personal data may be communicated according to the purposes pursued:

- to companies of the Deblock group, its partners, subcontractors and service providers. This communication only takes place in the context of processing that pursues one of the purposes described in this Policy;
- in compliance with the applicable regulations, to third parties in France or abroad for the purposes of establishing, safeguarding or defending a legal right, in the context of administrative or criminal investigations by one or more regulators, compliance with commitments made to them or in the context of legal disputes of any kind;
- to certain regulated professions such as auditors, lawyers, in order to provide regulatory reports or to act in defence of our rights;
- to payment processors and account information service providers, only with your consent or at your request.

Transfer of data outside the European Economic Area (EEA)

Due in particular to the international dimension of the Deblock group, the processing described in this Policy is likely to involve transfers of personal data to countries that are not members of the EEA and in particular the United Kingdom where the other companies of the Deblock group are established. However, your personal data remains at all times hosted within the European Union.

Furthermore, your personal data may, within the limits of what is authorised by the applicable regulations, be communicated to the official bodies and to the authorised administrative and judicial authorities of countries that are not members of the EEA, in particular within the framework of the regulations on the fight against money laundering and the financing of terrorism, international sanctions and embargoes, the fight against fraud and the determination of your tax status.

Your rights

You have a right of access to your personal data, a right of rectification, erasure, limitation of processing, as well as a right to the portability of some of your data. You can also withdraw your consent at any time, or object for reasons relating to your particular situation to the processing of your personal data, or define general or specific directives on the fate of your personal data in the event of death.

You can also, at any time and free of charge, without having to justify your request, object to your personal data being used for commercial prospecting purposes. If your opposition request does not concern commercial prospecting, Deblock may refuse to respond to your request if:

- there are legitimate and compelling reasons to process the personal data or that the latter is necessary for the establishment, exercise or defence of legal rights;
- you have consented to the processing of your data, in which case you must then withdraw this consent and not object;
- the processing in question is necessary for the execution of a contract between you and us;
- there is a legal obligation to process your personal data;
- the processing is necessary to protect the vital interests of the data subject or of another natural person.

You can exercise your rights and contact the data protection officer as follows:

- at the following mailing address: Deblock DPO - Talent Garden, 100 Av. Willy Brandt 59777 Lille;
- by e-mail to the following address: dpo@deblock.com

Finally, you have the right to lodge a complaint with the "Commission Nationale de l'Informatique et des Libertés" ("CNIL"), the supervisory authority in charge in France of compliance with obligations in terms of personal data.

Security

Deblock takes all physical, technical and organisational measures to guarantee the confidentiality, integrity and availability of your personal data, in particular in order to protect them against loss, accidental destruction, alteration and unauthorised access.

In the event of a breach of personal data involving you, implying a risk to your rights and freedoms, Deblock will notify the breach to the CNIL within the regulatory deadline.

In the event that this breach would present a high risk to your rights and freedoms, Deblock will inform you as soon as possible of the nature of this breach and the measures implemented to remedy it.