Privacy Policy

KoronaPay Europe Limited

KoronaPay Europe Limited (“we”) has adopted this privacy policy (the “policy”) to inform you about how we process your personal data in the course of providing online money transfer services.

This policy is layered. If you wish to learn about how we process personal data for a particular purpose, you can select and read the respective section of the policy.

1 Who we are

We offer money transfer services via the koronapay.eu website (the “website”) and KoronaPay mobile app (the “mobile app”).

Unless otherwise stated, we are the controller of the personal data we process. We may process your personal data when you:

1) become a registered user of our services and perform money transfers;
2) receive a money transfer;
3) visit our website;
4) contact us via email, phone or the feedback forms on the website and mobile app.

Our head office is located in Cyprus. Our address and contact details are listed below:

- Address: Georgiou A Street 89, MAIROZA YIATROS COURT, 3rd Floor, CY–4048 Limassol, Cyprus.
- Phone and email: +357 25 328 288, info@koronapay.eu.

You can contact the DPO via email at dpo@koronapay.eu or at the contact details above.

2 Who we work with

We are an independent organisation established in Cyprus and hold an electronic money institution licence from the Central Bank of Cyprus.

When we provide money transfer services as part of our relationship with you as the client, we engage a group of Russian entities that form the Centre of Financial Technologies (CFT) Group. CFT is among the Top 5 Software Developers in the Russian market and leads in terms of business scale among national companies developing software for the finance sector.

We may also use third-party data processors to provide elements of services for us.

We have contracts with the third parties in place. This means we are aware of all operations they perform with your personal data on behalf of us and instruct them on how to keep your personal data secure and on how long to store your data.

We have implemented measures to safeguard transfers of personal data to and from Russia. To learn more, please go to the “Third country processing” section.

Below is an overview of the roles of the third parties we engage in personal data processing. Please refer to the “Purposes for personal data processing” section to find out under which circumstances we may share your personal data with third parties for specific purposes.

1. Credit Union Payment Center (Ltd.) (CFT Group).

Credit Union Payment Center (Ltd.) acts as a joint controller in the processing of your personal data. The main area in which we operate jointly is clearing of funds. We also utilise Agents’ network operated by Credit Union Payment Center (Ltd.) for the purposes of money transfers withdrawal by cash.

We have distributed our personal data duties for the above processes in a joint controller agreement in line with Article 26(2) of the GDPR. This agreement also covers how you can exercise your personal data rights by contacting us or Credit Union Payment Center. You can learn more details about this agreement in the “Fulfilment of your data protection rights in the context of joint controller relations” section.

2. CJSC Zolotaya Korona (CFT Group)

CJSC Zolotaya Korona (“Zolotaya Korona”) acts as a processor in the course of activities related to your personal data. Under our instructions, Zolotaya Korona provides us with technical and operational facilities to perform money transfers, including fraud detection and information security aspects, customer support services and maintenance of our website and mobile app under our real-time control. Zolotaya Korona also takes part in sending mandatory notifications on the status of money transfers.

3. CJSC CardStandard (CFT Group)

CJSC CardStandard (“CardStandard”) acts as a processor in the course of activities related to your personal data. Under our instructions, CardStandard provides us with technical and operational facilities to perform payment card transactions, including compliance with the rules imposed by international payment systems such as Visa and Mastercard and resolving disputes.

4. Other processors

We engage third-party processors to host our IT infrastructure and process your requests via the contact centre.

3 Purposes for personal data processing

This section will tell you in detail:

- Why we process your data;
- What data we process;
- How long we store your data;
- Whether any third parties are involved in processing your data;
- Whether we intend to transfer your data to third countries;
- Whether we do automated decision making or profiling;
- What you can do in relation to your data and how to communicate your requests to us.

Descriptions of the processing activities are arranged by processing purpose. Please use the section subheadings to navigate and search for the information you need.

We receive most of your personal data from you directly and process your data to:

- Register you for online money transfer services;
- Perform mandatory identification checks;
- Process your money transfer;
- Inform you of the transfer details and services issues;
- Detect and prevent fraudulent transactions;
- Communicate with the public authorities in Cyprus;
- Process your customer support requests or information requests;
- Process your feedback on our services;
- Optimise our mobile app;
-
- Inform you about our products and services;
- Perform online marketing activities.

3.1 Registering you for money transfer services

Purpose and legal basis for processing

To become a new user of our money transfer services, you must register on our mobile app and enter into an agreement with us by accepting the “Online Money Transfers Services - Terms and Conditions” (the “T&C”). The registration requires you enter and confirm your mobile phone number after you have read the T&C and current policy.

The legal basis for this is taking steps for entering into a contract, which refers to Article 6(1)(b) of the GDPR.

Personal data we collect

The phone number that you will use for online money transfers.

Why we need your data

We identify you as a client by the phone number you enter and confirm the number by sending a one-time password. Once registered, all transactions under your user account will be associated with this phone number.

We also create a user ID that is uniquely associated with your phone number. We use this ID to organise data interchanges between our internal systems.

How long we store your data

If you do not use our online money transfer service for six months, we will consider you as an inactive user. According to Cyprus anti-money laundering and terrorism legislation, we are required to retain your user account data for five years. At the end of the retention period, we will erase your data, unless we are required to keep your data longer on other legal grounds (e.g. as part of an investigation).

Sharing your data with third parties

We share your personal data with Zolotaya Korona, which is the company responsible for technically enabling user registration.

3.2 Performing mandatory identification checks

Purpose and legal basis for processing

As an electronic money institution, we are subject to European Union and local Cyprus legislation on the prevention of money laundering and terrorist financing activities.

Depending on the amount of funds transferred we collect and verify various data about the senders and receivers of money transfers to the minimum extent that enables us to fulfil these legal requirements.

The legal basis for these actions is compliance with a legal obligation to which we (as a controller) are subject, which refers to Article 6(1)(c) of the GDPR.

Personal data we collect

We collect your full name, date of birth, permanent address and phone number.

Why we need your data

We use your personal data to verify whether the money transfer is legal before allowing it to be processed.

How long we store your data

If you do not use our online money transfer service for six months, we will consider you as an inactive user. According to Cyprus anti-money laundering and terrorism legislation, we are required to retain your user account data for five years. At the end of the retention period, we will erase your data, unless we are required to keep your data longer on other legal grounds (e.g. as part of an investigation).

Sharing your data with third parties

We do not share your personal data for performing mandatory identification checks.

3.3 Processing your money transfer

Purpose and legal basis for processing

Our purpose is to process the online money transfer you initiate. You will provide us with information about yourself and about the receiver of the money transfer.

The legal basis for processing your data is the performance of a contract (“Online Money Transfers Services - Terms and Conditions”) to which you are a party (as the client). This legal basis refers to Article 6(1)(b) of the GDPR.

The legal basis for processing data of the receiver of payment provided by you is Article 6(1)(f) of the GDPR, which allows us to process the personal data of the receiver of the payment when it is necessary for the purposes of our legitimate interests.

Personal data we collect

To process the money transfer, we need information about the sender, receiver and payment details.

About the sender:

- Identification data. The amount of data varies depending on the transaction, in line with mandatory anti-money laundering procedures. You can learn more in the “Performing mandatory identification checks and anti-money laundering procedures” section of this policy.
- Payment card data: card holders’ name, card number (PAN), card expiration date, security code (CVC/CVV).

About the receiver:

- Full name, destination country, phone number;
- If you are making a money transfer to the receivers’ payment card, we process the card number (PAN).

Why we need your data

Your payment card data is processed by CardStandard Processing Center that is certified under the Payment Card Industry Data Security Standards (“PCI DSS”). In line with this standard and Rules of international payment systems (such as Visa International or MasterCard Worldwide), we never keep card security codes and do not store the payment card details in plain text.

We need this information to process your payment order. When you initiate a money transfer, we create a Money Transfer Control Number (MTCN). This is a unique transaction number that the receiver uses to collect the funds.

How long we store your data

Under Article 72 of the Payment Services Directive (EU) 2015/2366, we are obliged to keep the evidence to prove that payments were duly authorised by you and executed correctly. Besides, Cyprus anti-money laundering and terrorism legislation requires us to retain your user activity history for five years after the end of business relationship with you.

We will store your personal data for five years after we find that you do not use our online money transfer service for six months and consider you as an inactive user. At the end of the retention period, we will erase your data, unless we are required to keep your data longer on other legal grounds (e.g. as part of an investigation).

Sharing your data with third parties

We share your personal data with:

- Zolotaya Korona, which processes money transfers under our real-time control;
- Credit Union Payment Center (Ltd.), which performs clearing of funds;

- CardStandard, which performs payment card transactions;
- our cloud provider in Cyprus, which hosts the database with our client's transactions.

3.4 Informing you about your transfer details and service issues

Purpose and legal basis for processing

Informing you about your transfer details

Our purpose is to send your transfer details to you and the receiver, including the transaction status and payment receipt.

Under Articles 46, 48 and 49 of the Payment Services Directive (EU) 2015/2366, we are obliged to make payment information available to you after the money transfer is initiated and executed. Article 6(1)(c) of the GDPR provides the legal basis for the processing of your personal data.

If you wish, you can additionally receive your transfer details over email by submitting your email address in the dedicated form in the mobile app. The legal basis for processing of your email address is your consent under article 6(1)(a) of the GDPR.

Informing you about service issues

Our purpose is to notify clients of maintenance activities in our services that may affect their money transfers. We may also contact our clients directly to troubleshoot an invalid transaction.

Article 6(1)(b) of the GDPR provides us with the legal grounds for processing your data as part of performing a contract (T&C) to which you are a party (as the client).

Personal data we collect

- Mobile phone numbers of the sender and receiver of the money transfer;
- Email address, if you wish to receive notifications about the status of your money transfer via email.

Why we need your data

We need to keep you informed about your current money transfers and any operating issues that may affect your work with our services. The information services are used only for notifications concerning money transfers.

How long we store your data

If you do not use our online money transfer service for six months, we will consider you as an inactive user. According to Cyprus anti-money laundering and terrorism legislation, we are required to retain your user account data for five years. At the end of the retention period, we will erase your data, unless we are required to keep your data longer on other legal grounds (e.g. as part of an investigation).

Sharing your data with third parties

We share your personal data with Zolotaya Korona, which issues notifications on the status of money transfers.

3.5 Detecting and preventing fraudulent transactions

Purpose and legal basis for processing

Our purpose is to detect and prevent payment fraud by monitoring transactions on an ongoing basis.

Under the Payment Services Directive (EU) 2015/2366 (Article 94) and our internal guidelines, we may process your personal data to safeguard the funds you send or receive, i.e. to prevent, detect and investigate payment fraud. Article 6(1)(c) of the GPRD allows us to process personal data if it is necessary for compliance with a legal obligation which we are subjected to.

Personal data we collect and use

We use the following categories of personal data:

- Transaction details, such as amount, time of operation, type of operation, purpose of operation;
- History of your operations;
- History and parameters of logins to your accounts;
- Changes of critical data (confirmation channel, information receiving channel, payment card details and so on);
- Geolocation data and IPs;
- Contact information (to contact you if we identify a suspicious operation);
- Information about your device, such as type and ID, operating system, connection settings, accesses you granted for our mobile app, etc.

Why we need your data

We divide all transactions into different risk levels. We define these levels using statistics on fraudulent transactions and the potential for withdrawals.

Our monitoring systems use algorithms and sets of rules to identify unusual behaviour, considering how you typically have used the money transfer service and the transactions you executed previously.

Fraud monitoring is performed online automatically. When monitoring is triggered, the money transfer is temporally blocked, the system alerts us, and we manually investigate and assess the cause of the trigger.

If we detect that something is wrong with the transaction, we may call you to ensure that the transaction is valid.

How long we store your data

If you do not use our online money transfer service for six months, we will consider you as an inactive user. According to Cyprus anti-money laundering and terrorism legislation, we are required to retain your

user account data for five years. At the end of the retention period, we will erase your data, unless we are required to keep your data longer on other legal grounds (e.g. as part of an investigation).

Sharing your data with third parties

We share your personal data with Zolotaya Korona, which performs anti-fraud activities under our real-time control.

3.6 Communicating with public authorities in Cyprus

Purpose and legal basis for processing

Our purpose is to notify the Unit for Combating Money Laundering ("MOKAS") in Cyprus of anything that is or could be related to money laundering or terrorist financing activities.

We are obliged to do so under the European Union legislation and local Cyprus AML legislation.

Article 6(1)(c) of the GPRD allows us to process personal data if it is necessary for compliance with a legal obligation which we are subjected to.

Personal data we collect

If required, we may collect your personal data to file reports issued by MOKAS directives. The reports may include:

- Name, residential and business address;
- Occupation and employer data;
- Date and place of birth;
- Citizenship and passport data;
- Details of suspicious activities and reasons for considering it;
- Documents related to the suspicious transaction.

Why we need your data

Notifying the public authorities in Cyprus is our legal duty.

How long we store your data

If you do not use our online money transfer service for six months, we will consider you as an inactive user. According to Cyprus anti-money laundering and terrorism legislation, we are required to retain your user account data for five years. At the end of the retention period, we will erase your data, unless we are required to keep your data longer on other legal grounds (e.g. as part of an investigation).

Sharing your data with third parties

We share your personal data with Zolotaya Korona, which processes money transfers and provides us the money transfer data at our request.

We transmit reports containing your personal data only to those public authorities (e.g. MOKAS and other public authorities, if any) for which they are intended.

3.7 Processing your customer support requests or information requests

Purpose and legal basis for processing

Our purpose is to process requests sent to our customer support service via email, Customer Care form on our website or communicated to our contact centre.

In general, we may receive the following types of requests:

- Notification on the misuse of payment or user account information;
- Service requests concerning online money transfers;
- Other information requests.

Informing us about the loss, theft, copy or the misuse of data

Under the Payment Services Directive (EU) 2015/2366 (Article 69) and our T&C (article 11.4, 11.5), you are obliged to notify us if you suspect the loss, theft, copy or the misuse of payment or user account information. Upon your request, we must take all reasonable steps to keep your data secure and prevent its further unauthorised use.

For this reason, we may need to contact you and specify your transaction details. Article 6(1)(c) provides us with the legal grounds to process personal data if it is necessary for compliance with a legal obligation which we are subjected to.

Providing technical support

If you would like to receive support from us concerning money transfers you have executed, our purpose will be to fulfil your request.

To help you with technical support issues, we may need your contact data, identification details and additional information about the case. Article 6(1)(b) of the GDPR provides us with the legal grounds for processing your data as part of performing a contract (T&C) to which you are a party (as the client).

Requests concerning personal data

If you are making a request about your personal data, or acting on behalf of someone making such a request, then we will ask for information to confirm your identity or your authority to act on behalf of someone else, as per Article 12(6) of the GDPR.

Article 6(1)(c) of the GDPR provides us with the legal grounds to process personal data if it is necessary for compliance with a legal obligation which we are subjected to.

Personal data we collect

The information we will need from you may vary depending on the nature of the request.

When you send a customer service request via the Customer Care form on the website, we collect your name, email or phone number, money transfer number (optional field), and your message.

When you request us by calling our contact centre, we may:

- Ask for your name and verify the phone number you are calling from to specify the user who executed the money transfer;
- Ask for your MTCN (unique transaction number) to find the transaction in our systems;
- Ask for other information depending on your request, e.g. location data, if you want to receive information about tariffs.

When your exercise the rights related to personal data, we will collect information that confirms your identity (at a minimum, your full name and identity document data).

Why we need your data

We need the personal data to identify the case you are having troubles with and help you to resolve it.

How long we store your data

We will process the data from the information request until the technical issue you notified us about is resolved or we have fulfilled your information request. We then store the data for five years for our business needs and erase the data at the end of the retention period.

Sharing your data with third parties

We share your personal data with:

- Zolotaya Korona, which maintains the technical infrastructure for receiving your requests, including the website, mobile app and contact centre (for requests in the Russian language);
- one of the entities in the CFT Group or our processor (whichever your request concerns, if any).

3.8 Processing feedback you have left about our services

Purpose and legal basis for processing

Our purpose is to process the feedback you may leave on our website.

The legal basis for the processing of your personal data is your consent under article 6(1)(a) of the GDPR.

Personal data we collect

Information about your user experience you want to let us know and your contact data (email address or phone number). If necessary, you may also leave additional information such as MTCN.

Why we need your data

We use the information you provide to improve our services, resolve issues as they occur and give positive feedback to our team when you inform us about the high quality of our service.

How long we store your data

We will process your feedback until we perform all actions you expect from us related to your feedback. We then store the data for five years for our business needs and erase the data at the end of the retention period.

Sharing your data with third parties

We share your personal data with:

- Zolotaya Korona, that maintains the technical infrastructure for processing your feedback;
- one of the entities in the CFT Group or our processor (whichever your feedback concerns, if any).

3.9 Optimising the mobile app

Purpose and legal basis for processing

Using your phone services

In the course of using the mobile app, it will request access to your phone, contact list, location, camera and messenger service. Granting access is optional. This means you will still be able to send the money transfer even if you do not grant access rights.

Our purpose is to make your work with the mobile app easier and faster. Specifically, we need your data for the following purposes:

- Phone number: to automatically fill in your phone number when you enter the mobile app;
- Contact list: to help you search for the receiver’s phone number directly from your contact list and avoid errors in entering the details;
- Messenger service: to automatically insert a confirmation code into the field;
- Camera: to scan your card and automatically fill in your card details;
- Location data: to automatically fill in your country.

The legal basis for the processing of personal data we rely on is your consent under article 6(1)(a) of the GDPR.

Using analytical tools

We operate fully online and use in-house and third-party analytical tools that are integrated into our mobile app. Our purpose is to improve the mobile app by using information gathered through such tools.

Analytical tools set metrics that provide us with:

- Anonymous usage statistics, e.g. counters that cannot be associated with a specific user;
- Personalised metrics that allow us to learn more about how our clients use the mobile app.

The legal basis for the processing of personalised metrics we rely on is your consent under article 6(1)(a) of the GDPR.

You can see more detailed information about the use of metrics in the metrics usage notice that is available on the mobile app.

Personal data we collect

While you use the mobile app, we may request and use access to your phone, contact list, location, camera and messages.

For analytical purposes, we may collect visiting statistics, user interaction history, geolocation data, information about your mobile device, etc. (See the metrics usage notice for details.)

We do not match this analytical data with your transaction history or the identification data of our existing clients and do not have the technical capacity to do so. To distinguish between users, we use numeric IDs that are randomly generated by analytical platforms.

Why we need your data

We need to conduct these processing activities to improve the mobile app and your user experience. The analytics data is collected by tools embedded into the mobile app. We do not install any additional software and other technology on your device.

Typical scenarios for our use of the analytics include:

- Analysing visiting statistics (such as the number of active users); behaviour patterns and user errors (such as the sequence of filling in forms or common mistakes users make); deletions and installations;
- Evaluating KPIs for specific services or categories of services;
- Logging events, such as registering in the mobile app; calculating the tariff; sending the money transfer; selecting the specific transfer destination; adding the incoming money transfer to the account or card;
- Analysing characteristics of mobile devices to develop and improve our mobile app, such as type, operating system and screen resolution.

We collect this analytical information only if you allow us to do so. When registering in our mobile app, you can adjust your settings to allow the use of personalised metrics or disable them. You can also change these settings while using the mobile app.

How long we store your data

We will use your information for three months after the date of collecting and delete the information at the end of this period.

Sharing your data with third parties

We share your personal data with:

- Zolotaya Korona, which maintains the mobile app and performs analytical tasks at our request;
- Third-party processors that provide us with analytical platforms.

3.10 Informing you about our products and services

Purpose and legal basis for processing

Marketing communications to existing clients

Our purpose is to notify you about new system features, promotions and offers that as we consider may be of your interest. To make the offer specific and commercially reasonable and to reduce the number of messages as well, we use your personal data to define what message will be most relevant for you.

We originate all marketing communications (not third parties) related to money transfer services. We have an interest in developing our services and continue serving our existing clients. Article 6(1)(f) of the GDPR provides us with the legal grounds to process personal data when it is necessary for the purposes of our legitimate interests.

Marketing communications to receivers of money transfers

Our purpose is to inform the person to whom you sent money to about our services, after we receive their consent.

Article 6(1)(a) of the GDPR provides us with the legal grounds to process the receiver's personal data, with their consent.

Personal data we may collect

About the sender:

- Communication channel that you choose to get information on (e.g. messengers, email);
- Your transaction history, such as frequency of money transfers, destinations and money transfer amounts;
- Actions you make on the website or mobile app, e.g. direction of money transfers you are interested in;
- Geolocation data and IPs to inform you on territory-specific offers;
- Whether you are a new or existing user.

About the receiver:

- Phone number and country from the transactional data.

Why we need your data

We conduct these processing activities to notify you and the receiver about relevant news, services and offers.

We may use several different communication channels, including SMS, messengers like WhatsApp and Viber, or email.

You can subscribe to our marketing communications and choose the preferable communication channel by ticking the check box in the mobile app. You can also unsubscribe from our marketing communications

by disabling the check box in the settings in the mobile app and we will stop sending you relevant news or offers.

How long we store your data

If you do not use our online money transfer service for six months, we will consider you as an inactive user. We will use your personal data to inform you about our products and services for three years after your inactivity. Then we will store your data for one year for our business needs. At the end of the retention period, we will erase your data.

The option to unsubscribe is available to you in all our messages. If you unsubscribe, we will immediately stop sending to you any marketing information.

Sharing your data with third parties

We share your personal data with:

- Zolotaya Korona, which maintains the mobile app and performs marketing communications at our request.
-

3.11 Online marketing activities

Purpose and legal basis for processing

We use in-house and third-party analytical tools that are integrated into our mobile app. Our purpose is to launch and evaluate our online marketing activity.

Analytical tools set metrics (in the mobile app) and gather personalised information that enables us to specify the audience for our marketing activities, including the development of new services.

The legal basis for the processing of personal data we rely on is the receiver's consent under article 6(1)(a) of the GDPR.

You can see more detailed information about the use of metrics in the metrics usage notice that is available on the mobile app.

Personal data we collect

For online marketing activities, we may collect visiting statistics, including the source of your visit, user interaction history, information about your device, information on marketing campaigns or promo pages you visited, social networks you are registered in to launch marketing campaigns on these platforms, etc. (See the metrics usage notice for details.)

We do not match this analytical data with transaction history or identification data of our existing clients and do not have the technical capacity to do so. To distinguish between users, we use numeric IDs that are randomly generated by analytical platforms.

Why we need your data

We conduct these processing activities to promote our money transfer services and make information about our services available for visitors of our website or promo-pages on different platforms.

Typical scenarios for our use of the analytics include:

- Planning, launching and evaluating the performance of marketing campaigns;
- Estimating the market's feedback to new services by launching experimental services;
- Assessing the efficiency of the marketing communication channels we use;
- Evaluating KPIs for specific services or categories of services;
- Establishing sources of your visit, such as partner websites, specific ads or promo pages.

We collect this analytical information only if you allow us to do so. When visiting our mobile app, you can adjust the settings to allow the use of personalised metrics or disable them. You can also change these settings while using the mobile app.

How long we store your data

We will use your information for three months after the date of collecting and delete the information at the end of this period.

Sharing your data with third parties

We share your personal data with:

- Zolotaya Korona, which maintains the mobile app and performs analytical tasks at our request;
- Third-party processors that provide us with analytical platforms.

4 Third-country processing

To provide you online money transfer services, we engage CFT Group companies located in Russia in the processing of your personal data. The entities are named in the section "Who do we work with" of the Policy.

We have safeguards in place with CFT Group companies. To maintain your privacy during the money transfers, together with CFT Group companies we have adopted the standard data protection clauses approved by the European Commission in accordance with Article 46(2)(c) of the GDPR.

Standard data protection clauses form an agreement containing the description of our mutual data protection obligations in relation to personal data processing.

5 Your data protection rights

Right to access

You have the right to ask us whether we are processing your personal data and if so, to receive or get access to a copy of your data.

This right is set by Article 15 of the GDPR.

Right to rectification

You have the right to correct any errors in your personal data and make the data complete if you believe that your data is incomplete. You can correct all your data in the mobile app or on the website.

This right is set by Article 16 of the GDPR.

Right to erasure of personal data (‘right to be forgotten’)

You have the right to request that we delete or remove your personal data. This right is set by Article 17 of the GDPR.

Under the GDPR, we can fulfil this right if there is no compelling reason for its continued processing, in particular:

- We no longer need the data for the purposes for which they were initially collected or processed;
- You have withdrawn consent that you provided for processing your personal data, and we do not have any other legal grounds to process your personal data;
- You have exercised your right to object the processing of your data (according to Article 21(1) of the GDPR) and we are unable to demonstrate a compelling legitimate interest that would override you interests, rights or freedoms;
- You object to the processing of your personal data for direct marketing purposes;
- You believe we have processed your data unlawfully;
- Your data must be erased in order to comply with EU or Member State law.

Right to restriction of processing

You have the right to ask us to restrict or suppress the processing your personal data. This right is set by Article 18 of the GDPR.

Under the GDPR, we can fulfil this right when:

- You challenge the accuracy of your personal data for a period, enabling us to verify the accuracy of the personal data;
- You have objected to the processing of your personal data (according to Article 21(1) of the GDPR) and you are waiting for verification of whether our legitimate grounds override your interests, rights or freedoms.
- You believe the processing is unlawful and want to restrict the use of your data instead of deleting your data;
- You believe we no longer need to process your personal data for our intended purposes, but you need this data to establish, exercise or defend legal claims.

Right to data portability

In some cases, you have the right to ask us to provide your personal data in a structured, commonly used and machine-readable format, and, if we can perform it technically, to send your data to other organisations.

This right is set by Article 20 of the GDPR.

Under the GDPR, we can fulfil this right when:

- We rely on the following legal grounds to process your personal data: your consent, performance of a contract to which you are subject or taking steps to enter it at your request;
- We process data with automated tools.

Right to object

You have the right to object to the processing of your personal data if:

- We rely on our legitimate interests to process your personal data; and
- We cannot demonstrate a compelling legitimate interest that would override you interests, rights or freedoms.

This right is set by Article 21 of the GDPR.

Right to withdraw consent

If we ask for your consent to process your personal data, you can withdraw it anytime. This right is set by Article 7(3) of the GDPR.

Right to lodge a complaint

You have the right to complain about the way we process your data to the data protection authority. This right is set by Article 77(1) of the GDPR.

In Cyprus, the data protection authority is the Office of the Commissioner for Personal Data Protection.

If you believe that we have no opportunity to resolve an issue concerning your personal data, you may address the data protection authority by following the link www.dataprotection.gov.cy.

6 How you can exercise your rights

- Make a request using the form on the website.
- Write to dpo@koronapay.eu.
- Send a letter to Georgiou A Street 89, MAIROZA YIATROS COURT, 3rd Floor, CY–4048 Limassol, Cyprus.

7 Fulfilment of your data protection rights in the context of joint controller relations

Together with Credit Union Payment Center (Ltd.), we act as joint controllers in the processing of your personal data during the following activities:

- clearing of funds;
- money transfers withdrawal by cash.

Under Article 26(2) of GDPR, we have entered into a joint controller agreement, which, among other things, sets our duties in relation to personal data processing.

Below is information that may help you exercise your personal data rights.

How you can exercise your rights

You can send any concerns you have about your data protection rights, as described in the “Your data protection rights” section, to us or Credit Union Payment Center (Ltd.) anytime.

Together with Credit Union Payment Center (Ltd.), we have established our DPO as the single point of contact to whom you can address your requests. Please find the contacts for DPO on the beginning of this policy.

You may also contact Credit Union Payment Center (Ltd.) directly using the contact details below.

- Address: Shaturskaya Str., 2, Novosibirsk, 630055, Russia.
- Phone and email: +7 (383) 336-49-49, 335-80-88, mail@rnko.ru.