



PRIVACY POLICY



Update Date: June 2025

PRIVACY POLICY

TABLE OF CONTENT

PURPOSE AND SCOPE	3
COLLECTION OF PERSONAL DATA	4
PURPOSE OF COLLECTING AND PROCESSING OF PERSONAL DATA	5
WHO CONTROLS AND PROCESSES YOUR PERSONAL DATA	6
PERIOD OF KEEPING YOUR PERSONAL INFORMATION	7
YOUR RIGHTS	8
AUTOMATED DECISION-MAKING	11
GEOGRAPHICAL AREA OF PROCESSING	11
OTHER RELATED INFORMATION	11
RAISING A CONCERN	12
CHANGES TO THIS PRIVACY STATEMENT	12
COOKIES	13
MONITORING AND REVIEW	13

PURPOSE AND SCOPE

The Policy is meant for use by **Royal Financial Trading (CY) LTD** (hereinafter "the Company" and/or "us" and/or "we"), Clients and relevant authorities.

Royal Financial Trading (CY) LTD is authorized by the Cyprus and Securities and Exchange Commission (CySEC) under license number 312/16 to provide Investment and Ancillary services, and is obliged to strictly observe relevant laws, directives and applicable legislations. The company is compliant with the requirements of the Markets in Financial Instruments Directive II (MiFID II) and Regulation (EU) No 600/2014 of the European Parliament and the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (the "MiFIR"), Investments Services Law 87(I) 2017, the laws for the Prevention of Money Laundering and Terrorist Financing, Market Abuse and Insider Dealing, the General Data Processing Regulation as well as other legislations applicable in the Republic of Cyprus.

The company has established this Privacy Policy in accordance with General Data Processing Regulation (GDPR) and laws, regulations and/or directives issued pursuant to this Law.

This policy applies to former, existing and potential Clients as well as to any visitors of the Company's website.

Client means any natural or legal person who has entered into a client relationship with the company and is actively using, or has used, the services of our company until the termination of the client relationship. A prospective Client is a natural or legal person who intends to use our services and has made the initial registration for such use of services without concluding the client relationship.

This policy aims to provide you with information on what type of information we collect, how it is used and the circumstances of which such information could be shared with third parties.

The present privacy statement and/or policy:

- provides an overview of how the Company collects, processes and uses your personal data and informs you about your rights under the local data protection law and the EU General Data Protection Regulation ("GDPR");
- Is directed to natural persons who are either current or potential customers of the Company, or are authorized representatives/agents or beneficial owners of legal entities or of natural persons which/who are current or potential customers of the Company;
- is directed to natural persons who had such a business relationship with the Company in the past;
- contains information about when we share your personal data with other third parties (for example, our service providers or suppliers).

Through this privacy statement, your data may be called either "personal data" or "personal information". We may also, sometimes, collectively refer to handling, collecting, protecting and storing your personal data or any such action as "processing".

For the purposes of this statement, personal data shall mean any information relating to you which identifies or may identify you, including, for example, your name, address and identification number.

The present Privacy Statement aims to help you better understand the most recent changes to the Privacy Policy and Cookie Policy and Disclosure and how they may impact you. To fully understand the changes and terms that will govern your use of our "Services," you will need to fully read the Privacy Policy and **Cookie Policy and Disclosure**.

COLLECTION OF PERSONAL DATA

The Company shall collect information necessary to fulfil their legal and regulatory obligations for the provision of services and to improve our service to you.

We will gather information and documentation to personally identify, contact or locate you and may gather information from third parties and/or other sources which will help us offer our services effectively.

As a Client, you are responsible for the true and accurate information and to keep us informed of any changes to your personal information or circumstance by emailing us at **dpo@oneroyal.com.cy**

We are required to evaluate the appropriateness of the financial instruments and their suitability based on three basic parameters;

- a. The sources of your income and wealth as well as your financial obligations
- b. Your investment knowledge, experience and objectives, including your knowledge and experience of the financial markets along with your understanding of the risks involved.
- c. Your experience in dealing with complex and non-complex financial instruments, especially your investment and risk attitude related such financial instruments.

Data we collect (or receive) about you

The personal data we collect (or receive) about you may include your:

- Name and address;
- E-mail address;
- Username, password;
- IP address;
- Phone numbers (which could be your home, work or mobile numbers);
- Credit card details;
- Source of wealth information;
- Occupation;
- Bank account details, including institution name, branch, account name, bank identifier;
- Bank account number or IBAN; or
- Trading experience information.

We're required to identify you if you're opening a new account or adding a new signatory to an existing account under anti-money laundering laws. We'll ask you to submit identity documents, which we'll then keep in our system in compliance with our anti-money laundering obligations. The types of identity documents that we'll ask you for can include:

- Passport;
- Driver's licence;
- National identity card (if applicable);
- Utility bills;
- Trust deed;

- Credit check; or
- Other information we consider necessary to our functions and activities.

PURPOSE OF COLLECTING AND PROCESSING OF PERSONAL DATA

Your personal data is used for specific, explicit and legitimate purposes and only as required to provide quality service to you and to comply with applicable legislations as referred to above.

A. For the performance of a contract

The personal data collected from you is used to verify your identity, to construct your economic and investment profile in order to ensure that we provide you with products and services suitable to your requirements, knowledge and risk appetite, to manage your account with us, to process your transactions, to provide you with post-transaction information, to inform you of additional products and/or services relevant to your economic profile, to produce analysis and statistical data which will help us improve our products and services, and for website improvement purposes. These are necessary for the entry into or performance of our contract once signed. We will carry out regular checks to ensure that our systems are working as intended.

B. For Identity Verification purposes

The Company needs to perform its due diligence measures and apply the principles of KYC (Know-Your-Client), before entering a client relationship, in order to prevent actions such as money laundering or terrorist financing, and also to perform other duties imposed by law. Therefore, we collect identity verification information from our Clients (such as images of your government-issued national ID card or International Passport, driving license or some other governmental proof of identification, as permitted by applicable laws) or some other authentication information. We are also requesting our Clients to provide us with a recent Utility Bill in order to verify their address. Further to this, the Company can use third parties which carry out identity checks on its behalf.

C. For compliance with a legal obligation

There is a number of legal obligations emanating from the relevant laws, of which we are subject to, as well as statutory requirements. There are also various supervisory authorities whose laws and regulations we are subject to. Such obligations and requirements impose on us necessary personal data processing activities for credit checks, identity verification, compliance with court orders, tax law or other reporting obligations and anti-money laundering controls.

These include, among others, transaction reporting requirements, assessment of Clients' knowledge and experience, FATCA and CRS reporting.

D. For the purposes of safeguarding legitimate interests

We process personal data so as to safeguard the legitimate interests pursued by us or a third party. A legitimate interest is when we have a business or commercial reason to use your information. But even then, it must not unfairly go against what is right and best for you. Examples of such processing activities include:

- Initiating court proceedings and preparing our defense in litigation procedures,
- Means and processes we undertake to provide for the Company's IT and system security, preventing potential crime, asset security, admittance controls and anti-trespassing measures,
- Measures to manage the Company's business and further develop products and services,
- The transfer, assignment (whether outright or as security for obligations) and/or sale to one or more persons and/or

charge and/or encumbrance over, any or all of the Company's benefits, rights, title or interest under any agreement between the Client and the Company.

E. For Marketing Purposes

The Company may use client data, such as location or trading history, to deliver any news, analysis, research, reports, campaigns and training opportunities, that may interest the Client, to their registered email address. You always have the right to change your option if you no longer wish to receive such communications.

F. Transaction Reporting

We are also obligated to regularly report to the respective authorities of the market, share products and the services held by client groups, as well as other financial figures.

WHO CONTROLS AND PROCESSES YOUR PERSONAL DATA

The Company, and any undertakings being a member of our group, agents which we engage with for the purpose of collecting, storing and processing personal data and any third parties acting on our or their behalf, may collect, process and store personal data provided by you.

For the purpose of processing and the storage of personal data provided by you in any jurisdiction within the European Union or outside of the European Union, the company can confirm this will be done in accordance with applicable laws.

Authorized Processor

The company may also use authorized external processors for client data processing, based on concluded service agreements, which are governed by instructions from the Company for the protection of client-related data. The contract is important so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the contract, which the Company has adhered to; the below is not an exhaustive list of the obligations of all relevant parties;

- Such third parties must only act on the written instructions of the Company (unless required by law to act without such instructions);
- Ensure that people processing the data are subject to a duty of confidence;
- Take appropriate measures to ensure the security of processing;
- The rights of Clients will not be impaired, in accordance with GDPR requirements;
- The security of processing, the notification of personal data breaches and data protection impact assessments will not be impaired;
- Deletion or return of all personal data as requested at the end of the contract; Such providers will provide various services as agreed with us.

Third parties will not promote our services, products or provide information to Clients or potential Clients regarding the investment and/or ancillary services and financial instruments that we offer.

We have a regulatory obligation to supervise and effectively oversee the outsourced functions and its obligation to take appropriate measures when it determines that the service provider is not performing the said functions effectively and in accordance with the applicable legislation.

We may use or disclose personal information without your consent only in certain circumstances:

- if required by law or by order of a court, administrative agency or other government entities;

- if there are reasonable grounds showing disclosure is necessary to protect the rights, privacy, property or safety of users or others;
- if we believe the information is related to a breach of an agreement or violation of the law that has been, is being, or is about to be committed;
- if it is necessary for fraud protection, risk reduction, or the establishment or collection of funds owed to us;
- if it is necessary to enforce or apply the Terms and Conditions and other agreements, to pursue remedies or to limit damages to our company;
- for other reasons allowed or required by law.
- if the information is public;

When we are required or permitted to disclose information without consent, we will not disclose more information than necessary to fulfil the disclosure purpose.

We inform all Clients to maintain confidentially and not share, with others, their usernames and private passwords or other such information provided by us. The Company bears no responsibility for any unlawful or unauthorized use of Clients' personal information due to the misuse or misplacement of Clients' access codes (i.e. passwords /credentials), negligent or malicious, however conducted.

Marketing Activities and Profiling

The Company may process your personal data to inform you about products, services and offers that may be of interest to you. The personal data that we process for this purpose consists of information you provide to us and data we collect and/or infer when you use our services, such as information on your transactions. We study all such information to hypothesize what we think you may need or what may interest you. In some cases, profiling is used, i.e. we process your data automatically with the aim of evaluating certain personal aspects in order to provide you with targeted marketing information on products.

We can only use your personal data, to promote our products and services to you if we have your explicit consent to do so – by clicking on the tick box on the account opening form – or in certain cases, if we consider that it is in our legitimate interest to do so.

Furthermore, you have the option to choose whether you wish to receive marketing-related emails (company news, information about campaigns, the company's newsletter, the company's strategic report, etc.) to your provided email address by clicking the relevant tick box on the account opening form.

You have the right to object, at any time, to the processing of your personal data for marketing purposes or unsubscribe to the provision of marketing-related emails by the Company by contacting, at any time, our customer support department via the following methods:

- a. By Email: **dpo@oneroyal.com.cy**
- b. By post or in person at the Company's Headquarters: Franklin Roosevelt Avenue, Limassol, 3045, Cyprus

PERIOD OF KEEPING YOUR PERSONAL INFORMATION

The Company will keep your personal data for as long as a business relationship exists, either as an individual or in respect of our dealings with a legal entity you are authorized to represent or are beneficial owner. Once the business relationship with you has ended, we are required to keep your data for a maximum period of five (5) years to meet our regulatory and legal requirements.

If reasonably necessary or required to meet other legal, contractual or regulatory requirements, resolve disputes, prevent fraud and abuse, or enforce our terms and conditions, we may also keep some of your information for an additional five (5) years as required, even after the previously-mentioned period.

When we no longer need such personal data, we securely delete or destroy it.

YOUR RIGHTS

1. Your Rights to Access

You have the right to request copies of your personal data.

Information must be provided, without delay and at the latest, within one month of request. The Company will be able to extend the period of compliance by an additional two (2) months when requests are complex or numerous. If that is the case, we will inform the individual within one (1) month of the receipt of the request and explain why the extension is necessary.

Can the Company charge a fee for dealing with a subject access request?

We shall provide a copy of the information free of charge. However, the company can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The fee, if applied, will be based on the administrative cost of providing the information.

If, at any time, we refuse to respond to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and, at the latest, within one month.

When is information provided?

The company will verify the identity of the person making the request, using reasonable means.

2. Your Right for Rectification

When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. You can make a request for rectification either verbally or in writing.

If we have disclosed the personal data in question to others, we shall contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, we shall also inform the individuals about these recipients.

How long does the Company have to comply with a request for rectification?

We shall respond within one month.

This can be extended by two (2) months if the request for rectification is complex.

In cases where the Company is not taking action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

3. Your Right to Erasure

When does the right to erasure apply?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with a request. We have a legal obligation to obtain data on you while meeting relevant regulatory obligations; based on the legal obligations imposed on us, individuals shall have no right to erasure, no right to data portability or right to object on the information gathered meeting with our legal obligation under our license to provide financial services.

When can the Company refuse to comply with a request for erasure?

We can refuse to comply with a request for erasure when the personal data is processed for the following reasons:

- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- the exercise or defense of legal claims.

Does the Company have to tell other organizations about the erasure of personal data?

If we have disclosed the personal data in question to others, we must contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the individuals about these recipients.

4. Your Right to Restrict Processing

When does the right to restrict processing apply?

We will be required to restrict the processing of personal data in the following circumstances:

- When an individual contests the accuracy of the personal data, we should restrict the processing until you have verified the accuracy of the personal data.
- When an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) and we are considering whether our Company organization's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If the Company no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

We may need to review procedures to ensure we are able to determine when we may be required to restrict the processing of personal data.

If the Company has disclosed the personal data in question to others, we must contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the individuals about these recipients.

The Company must inform individuals when we decide to lift a restriction on processing.

5. Your Right to Consent

Initial registration - In order to create a Demo or Live trading account with the Company, a person must make an initial registration via the website's registration form or directly through their Trader's Room and agree with the terms listed in the given Privacy Policy. The Client confirms acceptance of these terms by ticking the corresponding box on the registration form. If such consent is not given, the Company cannot process a persons' data nor provide any services to the person in question.

Cancellation of the initial registration - When a person cancels the registration process and does not complete it, that person's data will not be retrieved by the Company and will, therefore, not be saved for further processing in the future.

Declining the option to be contacted via phone - A person always has the right to request not to be contacted via telephone by the Company's representative. This request will be saved within the Company's internal systems and act as a separate restriction, which we will, of course, respect. The request to not to be contacted via telephone does not affect a Client from using our services. Additionally, this does not restrict said person from contacting the company by their own initiative.

6. Your Right to Data Portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- It enables consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.
- We shall respond such a request without undue delay and within one (1) month. This can be extended by two (2) months if the request is complex or when the company may receive a number of requests. We will inform the individual within one (1) month of the receipt of request and explain why the extension is necessary, if applicable.
- When we are not taking action in response to a request, we shall explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and, at the latest, within one (1) month.

7. Your Right to Object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

- direct marketing (including profiling);
- processing for purposes of scientific/historical research and statistics.

We will stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defense of legal claims.

AUTOMATED DECISION-MAKING

In establishing and carrying out a business relationship, we generally do not use any automated decision-making. We may process some of your data automatically, with the goal of assessing certain personal aspects (profiling), in order to enter into or perform a contract with you for data assessments (including on payment transactions), which are carried out in the context of combating money laundering and fraud. Utilization of your account may be detected as unusual for you or your business. These measures shall also serve to protect you.

GEOGRAPHICAL AREA OF PROCESSING

As a general rule, the client data is processed within the European Union/European Economic Area (EU/EEA), but in some cases it is transferred to and processed in countries outside the EU/EEA.

The transfer and processing of client data outside the EU/EEA can take place, provided there are appropriate safeguards in place and the actions are made on a legal basis only.

Upon request, the Client may receive further details on client data transfers to countries outside the EU/EEA.

OTHER RELATED INFORMATION

We use appropriate technical, organizational and administrative security measures to protect any information we hold in our records from loss, misuse, and unauthorized access, disclosure, alteration and destruction. Unfortunately, no company or service can guarantee complete security. Unauthorized entry or use, hardware or software failure, and other factors may compromise the security of user information at any time.

Among other practices, your account is protected by a password for your privacy and security. You must prevent unauthorized access to your account and Personal Information by selecting and protecting your password appropriately and limiting access to your computer or device and browser by signing off after you have finished accessing your account.

Transmission of information via regular email exchange is not always completely secure. The Company however exercises all possible actions to protect clients' personal data, yet it cannot guarantee the security of client data that is transmitted via email; any transmission is at the clients' own risk. Once the Company has received the client information it will use procedures and security features in an attempt to prevent unauthorized access.

When you email the Company (via the "Contact Us" page), or using the Live Chat feature, a person may be requested to provide some additional personal data, like their name or email address. Such data will be used to respond to their query and verify their identity. Emails are stored on our standard internal contact systems which are secure and cannot be accessed by unauthorized external parties.

RAISING A CONCERN

You have the right to be confident that we handle your personal information responsibly and in line with good practice. If you have a concern about the way we are handling your information, for example, if you feel we may not be;

- keeping your information secure;
- holding accurate information about you;
- disclosing information about you;
- deleting or archiving information about you beyond the necessary period of time; or
- collecting information for legitimate reasons, in accordance to laws and regulations;

We take all concerns seriously and will work with you to resolve any such concerns.

Any concerns and/or requests can be raised to the appointed Data Protection Officer, whose contact details are below:

Royal Financial Trading (CY) LTD

Level 3 IRIS House, 8 John Kennedy, 3106 Limassol Cyprus

Tel: +357 25 080880

Email: dpo@oneroyal.com.cy

If you are not satisfied with any responses provided by us, you have the right to raise such matters with the Cyprus Data Protection Commissioner;

Office of the Commissioner for Personal Data Protection 1 Iasonos str., 1082 Nicosia

P.O.Box 23378, 1682 Nicosia

Tel +357 22818456

Fax +357 22304565

Email: commissioner@dataprotection.gov.cy

The client has the right to go to court or to escalate their complaint to the data protection regulator in their jurisdiction for the protection of rights, unless the applicable laws prescribe a different procedure for handling such claims.

CHANGES TO THIS PRIVACY STATEMENT

The Company reserves the right to modify or amend this Privacy Statement unilaterally, at any time, in accordance with this provision.

If any changes are made to this privacy statement, we shall notify you accordingly.

The revision date shown at the end of this page will also be amended. We do, however, encourage you to review this privacy statement occasionally in order to stay informed about how we are processing and protecting your personal information.

COOKIES

Our website uses small files known as cookies to enhance its functionality and improve your experience. To find out more about how we use cookies, please refer to our Cookies Policy and Disclosure.

MONITORING AND REVIEW

The Company will monitor, on a regular basis, the effectiveness of this Policy and, in particular, the execution quality of the procedures explained in the Policy; where appropriate, the Company reserves the right to correct any deficiencies.

In addition, the Company will review the Policy at least annually. A review will also be carried out whenever a material change occurs that affects the ability of the Company to maintain the best possible result for the execution of its Client Orders, on a consistent basis, using the venues included in this Policy.

The Company will inform its Clients of any material change to this Policy by posting an updated version of this Policy on its Website(s).