Privacy policy

Version 1
Last updated 25/09/2025

Table of contents

Privacy policy

1. Introduction

1.1. The Deriv group of companies is committed to protecting your personal data and respecting your privacy. This Privacy Policy explains how we collect, use, store, disclose, and protect personal data across all Deriv entities and in connection with our products, services, applications, and websites. When we say "**we**", "**us**", or "**our**" in this Privacy Policy, we mean the specific entity within the Deriv group that is responsible for processing your personal data, typically the Deriv group entity with whom you have a business relationship or that provides you with services (as described in the "Data controller and contact information" section below).

1.2. This Privacy Policy applies to current and prospective clients, website visitors, business partners, service providers (and their employees), event participants, visitors to our offices, and anyone interacting with our products, services, mobile apps, platforms, or digital channels, regardless of their country of residence. This Privacy Policy does not apply to job applicants or employees of the Deriv group.

1.3. We process your personal data as a controller, in accordance with applicable laws, which may include the European Union General Data Protection Regulation (GDPR), the United Kingdom General Data Protection Regulation (UK GDPR), and other applicable privacy laws ("**Privacy Laws**").

2. Categories of personal data

2.1. Depending on your relationship with us, we may collect and process one or more of the following types of personal data, such as:

2.1.1. Identity data: First name, surname, gender, nationality, date of birth, and/or government-issued identification documents (including passports, driving licences, national IDs, and/or resident permits).

2.1.2. Contact data: Postal address, email address, and/or telephone number.

2.1.3. Professional data: Job title, employer name, occupation, areas of responsibility, and/or remuneration.

2.1.4. Residential information, including rental/tenancy agreements, title deeds, and utility bills.

2.1.5. Communication data: Content of communications (emails, live chat, call logs, feedback, and/or market research responses).

2.1.6. Services data: Account or application information, trade or transaction history, contracts, preferences, and/or usage records.

2.1.7. Provider data: Information exchanged as a service provider or partner (contract details and/or meeting notes).

2.1.8. Visitor data: Office visit details (entry logs, date/time and purpose of visit, and/or special needs communicated).

2.1.9. Consent data: Given/withdrawn consents, cookies, and/or marketing authorisations and preferences.

2.1.10. Payment data: Billing address, payment details, bank account, payment method, and/or payment history.

2.1.11. Usage data: The transactions you make on your account, how you use our various platforms and products, or how you interact with our websites, applications, marketing, and communications.

2.1.12. Digital data: For example, IP address, location information (including GPS and geolocation), device and browser data, and/or security information (such as how you log in or authenticate yourself to access your account).

2.1.13. Verification data: Proof of address, source of wealth, and/or source of funds.

2.1.14. Biometric data: Data processed for unique identification, such as facial recognition or voiceprints. Some photographs, images, audio, or video recordings may qualify as biometric data if processed for identification purposes.

2.1.15. Event participation data: Information for event registration, attendance, and/or participation.

2.1.16. Other: Any additional information you supply, or we are required to collect by law, or that relates to our professional activities.

3. Sensitive personal data

3.1. Unless expressly requested by us or required by law, please do not provide or disclose any sensitive personal data to us, including via our websites, applications, or other channels. Depending on your jurisdiction, "sensitive personal data" may include, but is not limited to, data relating to your racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, health, genetic or biometric data, sexual orientation, criminal background, or administrative or legal proceedings and sanctions.

3.2. If we need to collect or process sensitive personal data, we will do so only in accordance with applicable Privacy Laws and only where we have a valid legal basis, such as your explicit consent, compliance with a legal obligation, or as necessary for the establishment, exercise, or defence of legal claims.

4. Sources of personal data

4.1. We may collect your personal data in the following situations from:

4.1.1. You directly: When you interact with us, register, correspond with our teams, attend events, or visit our offices;

4.1.2. Our websites/applications: When you use our products and services, engage with our websites, applications or communicate with us, for example, through forms, cookies, or usage logs;

4.1.3. Third parties: Including business partners, service providers, public authorities, or verification databases;

4.1.4. Public sources: Such as regulatory registers or publicly available databases;

4.1.5. Self-generated by Deriv: In the provision of our services (e.g. meeting records, call logs) or by creating insights or other information about you when analysing information we already hold; and/or

4.1.6. Ongoing requests for information: As part of our ongoing compliance, due diligence, and to ensure the security and integrity of our services, we may require you to provide further personal data or supporting documents at any time during your relationship with us.

5. Lawful basis and purposes

5.1. We only use your personal data where we have your consent or a lawful reason for using it. These reasons may include:

5.1.1. Processing your personal data to comply with a legal obligation, including licensing requirements, anti-fraud requirements, and anti-money laundering laws;

5.1.2. Processing your personal data to enter into or carry out an agreement we have with you;

5.1.3. Pursuing our legitimate business interests; and/or

5.1.4. Establishing, exercising, or defending our legal rights.

5.2. We may use your information for the following purposes:

5.2.1. Customer management and account administration;

5.2.2. Providing services, performing trades, and managing transactions;

5.2.3. Customer service support to facilitate communications and handle complaints or disputes;

5.2.4. Partner management;

5.2.5. Client due diligence, Know Your Customer (KYC) procedures, anti-fraud measures, anti-money laundering (AML) activities, and sanctions screening;

5.2.6. Security and access control, site security, and to address actual or suspected fraud, unlawful activity, or misconduct;

5.2.7. Marketing and analytics purposes, which may include conducting surveys, measuring customer satisfaction, and collecting feedback;

5.2.8. Improving our products and services, conducting research and development activities, performing user experience research, and gathering business intelligence;

5.2.9. Events, webinars, training sessions, and learning programmes;

5.2.10. Finance, treasury, accounting, and payment processing;

5.2.11. Supplier and third-party management;

5.2.12. Risk management, crime prevention and detection, internal audits, corporate governance, and remediation activities;

5.2.13. Operating our website, applications, and platforms, as well as for IT and security infrastructure and system testing or development;

5.2.14. Legal compliance, managing litigation or defence of legal claims, record-keeping, and protecting our legitimate interests or legal rights, including taking and responding to legal action or making insurance claims;

5.2.15. Merger, acquisition, sale, asset transfer, restructuring, or bankruptcy of all or part of our business, including the relevant due diligence;

5.2.16. Processing your requests or to help you exercise your rights;

5.2.17. Producing and distributing audio, video, or other media content;

5.2.18. Any other purpose required or authorised by law, regulations, codes of practice, or court order; and/or

5.2.19. Machine learning and automated processing, including using personal data to train, develop, and improve algorithms, models, or artificial intelligence systems, for the purposes of enhancing our services, fraud prevention, risk management, and business operations.

5.3. You agree that when you use the live chat feature on our website and applications, all personal data that you enter in the chat channel, including but not limited to your first name and email address, is processed by us and stored in our databases.

5.4. You will be clearly informed if we rely on your consent, and you may withdraw your consent at any time.

6. Disclosure of personal data

6.1. We may share your personal data with the following categories of recipients, where necessary and appropriate to achieve the purposes outlined in this Privacy Policy, and based on a corresponding legal basis:

6.1.1. Other companies within the Deriv group;

6.1.2. Agents, contractors, suppliers or service partners, including IT, cloud, web-hosting, analytics, fulfilment, content providers, customer support, communication platforms and logistics service providers;

6.1.3. Payment processors, banks, and financial institutions to process transactions;

6.1.4. Regulators, courts, law enforcement, tax, or other public authorities as required by law or to protect our rights;

6.1.5. Professional advisers, including insurers, lawyers, auditors, and accountants, for business continuity, risk management, or in the course of legal matters or claims;

6.1.6. Business partners;

6.1.7. Event or marketing partners, advertising networks, analytics providers, and social networks, as relevant for marketing, advertising, product development, or event participation;

6.1.8. With your explicit consent, to other third parties whom you direct us to share your data with; and/or

6.1.9. Other parties Deriv is authorised or required by law, regulations, codes of practice or court order to disclose information to.

6.2. We require all third parties who process your personal data on our behalf to offer appropriate security, comply with applicable law, and provide protection at least equivalent to what is described here.

7. International data transfers

7.1. The Deriv group is a global business with offices, partners, and service providers located around the world, including in the European Economic Area (EEA), the United Kingdom, Asia, Africa, Latin America, and other regions. As a result, your personal data may be processed in or transferred to countries outside your country of residence—including countries outside the EEA or UK—that may not provide the same level of data protection as in your home jurisdiction.

7.2. Where personal data subject to the GDPR, UK GDPR, or other applicable Privacy Laws is transferred to a country that has not been found to offer an adequate level of data protection, we will implement appropriate safeguards in accordance with the relevant legal requirements. These safeguards may include Standard Contractual Clauses approved by the European Commission or UK government, adequacy decisions, further transfer impact assessments, and supplementary technical and organisational measures, as needed, to ensure that your personal data remains protected.

8. Data retention

8.1. We retain your personal data only for as long as it is necessary to fulfil the purposes for which it was collected, including to comply with legal, regulatory, accounting, or reporting requirements, and in accordance with our internal retention policies. After the applicable retention period has ended, we will securely delete or anonymise your data, unless a longer retention period is required or permitted by law, such as for the establishment, exercise, or defence of legal claims, or for archiving, scientific, or historical purposes.

9. Your rights

9.1. Depending on the jurisdiction in which you reside and the Privacy Laws applicable to your personal data, you may have the following rights:

9.1.1. Information and access: You may request to access your personal data, receive supplemental information about how we process it, and obtain details of public and private entities with whom your data has been shared. You may also request a copy of your personal data.

9.1.2. Rectification: You may request to rectify or update inaccurate or incomplete personal data.

9.1.3. Erasure: You may have the right to request deletion of your personal data, subject to applicable legal requirements.

9.1.4. Restriction of processing: You may have the right to request that we restrict the processing of your personal data under certain circumstances.

9.1.5. Objection to processing: You may have the right to object to certain types of processing, including direct marketing and profiling.

9.1.6. Data portability: You may have the right to request a portable copy of your personal data in a structured, commonly used, and machine-readable format, subject to legal limitations and provided this does not adversely affect the rights of others or compromise confidential information.

9.1.7. Automated decision-making: You may have the right not to be subject to decisions based solely on automated processing (including profiling), where such decisions produce legal or similarly significant effects.

9.1.8. Withdrawal of consent: Where we process your data based on consent, you have the right to withdraw your consent at any time. Withdrawal will not affect the lawfulness of processing carried out prior to withdrawal.

9.1.9. Complaint to a supervisory authority: You may have the right to lodge a complaint with a data protection supervisory authority in the country where you reside, where your data is processed, where your data controller is established, or where a potential data breach has occurred.

9.2. Please note that we may request additional information from you to verify your identity before processing your request. In some cases, if a request is manifestly unfounded, repetitive, or excessive, we may charge a reasonable fee or decline to act on the request, as permitted by applicable law.

9.3. You can request to update your personal data in your account settings. It is your responsibility to ensure that your personal data remains accurate and up to date, as we rely on this data to provide our services. Please note that if you provide inaccurate information or do not update your details when they change, it may affect the quality or availability of our products and services to you.

9.4. If you wish to exercise any of these rights or have questions regarding your rights under this Privacy Policy, please contact our Data Protection Officer at dpo@deriv.com.

9.5. This Privacy Policy does not create, extend, or modify any rights or obligations except as granted by applicable law (such as the relevant Privacy Laws).

10. Marketing

10.1. You have the right to opt out of receiving marketing materials from us. This can be done by revoking your consent at any point during the period that you hold an account with us.

10.2. You can opt out of receiving marketing communications in your account settings or unsubscribe from marketing emails by clicking the “Unsubscribe” link included in all our marketing communications.

10.2.1. If you choose to opt out or unsubscribe from our marketing communications, please note that you may still receive transactional or service-related emails. We will make every effort to minimise the frequency of these messages and ensure that they are necessary for the proper functioning of our products and services.

10.2.2. Please note that due to processing times, you may receive some marketing communications for a short period of time, even after you've requested to opt out or unsubscribe. Additionally, if a marketing communication is already in transit or being sent, you may still receive it. If you are still receiving marketing communications from us after a reasonable time has passed, contact us via live chat.

11. Security of your personal data

11.1. We take the security of your personal data and financial transactions seriously and employ a risk-based approach to safeguards, including:

11.1.1. Your password is uniquely assigned to your account and securely stored using strong cryptographic hashing. Neither we, nor our staff, can access your password. Please contact us if you have any issues with your password.

11.1.2. All credit card data is processed securely and directly with our payment partners, using current SSL/TLS encryption and in compliance with the Payment Card Industry Data Security Standard (PCI DSS) or equivalent standards.

11.1.3. Access to your personal data is limited to authorised personnel who strictly require it to fulfil their responsibilities. All access is managed according to role-based access controls and is subject to regular review and audit.

11.1.4. We implement industry-standard technical and organisational measures, including data encryption in transit and at rest, network security protections (such as firewalls and intrusion detection), regular security testing, and business continuity planning, to safeguard your information.

11.1.5. Our systems monitor for suspicious activity and potential fraud. We verify identity where appropriate and, in cases of suspected fraud, may engage law enforcement and relevant agencies.

11.1.6. You are responsible for keeping your login details, associated email account, and devices secure. We strongly recommend choosing strong, unique passwords, regularly updating them, never disclosing them, and not using public or shared devices or networks to access your account.

11.2. While we strive to protect your data, please note that no online platform can be guaranteed to be completely secure. In the unlikely event of a data breach, we shall follow applicable notification requirements in accordance with the relevant Privacy Laws.

12. Automated decision-making and profiling

12.1. We reserve the right to use the data that we collect and assess to profile you in relation to our products. We do this manually with the assistance of automated processing. In this way, we shall be able to provide you with the most appropriate products and services.

12.2. We may also use automated systems to help us make risk assessment decisions, such as when we conduct fraud and money laundering checks. While we may use technology to assist us in identifying levels of risk, all decisions that may adversely impact you will always include manual intervention to ensure that decision-making is not based solely on automated processing.

13. Cookies and website analytics

13.1. Cookies are small text files placed on your device to store data that can be recalled by a web server. They are widely used to make websites work, improve user experience, and deliver relevant content and advertisements.

13.2. We use cookies and similar technologies (such as web beacons and pixels) to:

13.2.1. Enable website functionality and secure areas;

13.2.2. Remember your preferences and settings;

13.2.3. Understand how you use our services and improve them;

13.2.4. Deliver tailored content and advertising; and

13.2.5. Help secure your account by recording accesses and login attempts.

13.3. We may use the following types of cookies:

13.3.1. Strictly necessary cookies: Essential for you to browse the website and use its features, such as logging in;

13.3.2. Functionality cookies: Remember your preferences and choices to enhance your experience;

13.3.3. Performance/Analytics cookies: Help us understand how visitors interact with our website by collecting and reporting information anonymously; and/or

13.3.4. Targeting/Advertising cookies: Used by us and our third-party partners to deliver relevant advertising and measure its effectiveness.

13.4. Strictly necessary cookies will be set automatically. Other cookies (such as functionality, analytics, and advertising cookies) may only be set if you provide your consent in accordance with applicable law.

13.5. You have many choices with regards to the management of cookies on your computer. Most web browsers allow you to control or disable cookies through your browser settings. Please note that disabling certain cookies may affect the functionality of our products and services.

13.6. Cookies are stored only for as long as needed to fulfil their intended purpose. The retention period depends on the type of cookie. Session cookies are deleted when you close your browser, while persistent cookies may remain longer unless you delete them sooner.

13.7. We use third-party services, such as Google Analytics, Meta Pixel, LinkedIn Insight Tag, and Snap Pixel, which may set their own cookies on your device. You can email us at dpo@deriv.com for information about these cookies and how to manage your preferences.

14. Links to other websites

14.1. Our website contains links to other websites and may contain banner or icon advertisements related to third-party websites. These websites and their advertisements may submit cookies to your web browser, which is beyond our control. We are not responsible for the privacy practices or the content of such websites. We encourage you to read the privacy policies of these websites because their practices may differ from ours.

15. Data controller and contact information

15.1. For the purposes of applicable data protection laws, the data controller responsible for your personal data depends on your country of residence and the Deriv services you use. For information on the Deriv companies which offer services, including registered addresses and regulatory information, please visit: https://deriv.com/regulatory.

15.2. If you are located in the European Union (EU), your data controller will be Deriv Investments (Europe) Limited, incorporated in Malta (Company No. C 70156), with its registered address at Level 3, W Business Centre, Triq Dun Karm, Birkirkara BKR9033, Malta. Deriv Investments (Europe) Limited is regulated by the Malta Financial Services Authority under the Investments Services Act.

15.3. If you would like more information about your data controller, have questions or comments about this Privacy Policy or our data protection practices, or wish to make a complaint regarding our compliance with applicable Privacy Laws, please contact our Data Protection Officer at dpo@deriv.com.


deriv