Privacy Policy

1. Introduction

Capital Com (UK) Limited (hereinafter the "**Company**", "**we**", "**Capital.com**") is an investment firm authorised and regulated by the Financial Conduct Authority ("the FCA") for the provision of investment and ancillary services under the FRN number 793714 and registered in England and Wales under the registration number 10506220. Our business address is 2nd floor, 4 Orchard Place, London SW1H 0BF.

This privacy policy (the "**Policy**" or "**Privacy Policy"**) explains how Capital.com collects, processes and discloses personal information through its websites, mobile applications, and other online products and services that fall under this Policy (collectively, the "**Services**") or when you otherwise interact with us.

The Services include providing: (i) the Capital.com trading platform for investing in stocks and for CFD trading and Spread Betting which users can sign up for an account with Capital.com; (ii) any other site, web platform, mobile application or other service facilitated by Capital.com.

Capital.com is responsible for the protection of the privacy and the safeguarding of the personal data of our Clients including (i) Retail Clients and/or (ii) Professional Clients, acting as the counterparty of the Company having agreed to the Terms and Conditions of the Company, as well as website visitors (hereinafter "**you**").

If you visit our website without creating an account, we may still collect certain technical data about your visit automatically, including your IP address, browser type and version, pages visited, time and date of your visit, and information about how you navigate our website. We collect this data through cookies and similar technologies on the basis of our legitimate interests in operating and improving our website, and where we rely on your consent for non-essential cookies. For full details of how we use cookies, please see Section 4 of this Policy.

Your privacy is important to us. This Privacy Policy outlines how we collect, process, manage the personal data we collect from your use of our services, applications or our website capital.com, through your interaction with us on social media or your other dealings with us. When doing that we act as data controller in accordance with the principles contained in the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA"), and the Data (Use and Access) Act 2025 ("DUAA").

We have appointed a Senior Responsible Individual ("SRI") as required under the DUAA. The SRI role was introduced by section 96 of the DUAA and came into force on 5 February 2026. The SRI is a member of our senior management team with designated responsibility for our compliance with UK data protection law under the UK GDPR and the Data Protection Act 2018. The SRI role is distinct from the Data Protection Officer ("DPO") role: our DPO is responsible for advising on and monitoring compliance with data protection law across all applicable jurisdictions, while the SRI holds specific senior accountability for our UK data protection compliance programme.

To contact our SRI, please write to us at: gdpr.uk@capital.com, marking your correspondence "For the attention of the Senior Responsible Individual."

Data Protection Officer

We have appointed a DPO who is responsible for overseeing our compliance with data protection law and for advising us on our data protection obligations across all applicable jurisdictions.

To contact our DPO, please email: dpo@capital.com, or write to us at: Capital Com (UK) Limited, 2nd Floor, 4 Orchard Place, London SW1H 0BF, marking your correspondence "For the attention of the Data Protection Officer."

2. What kind of personal data do we collect?

- **Identity data** includes full name or its parts, username or similar identifier, marital status, title, date and place of birth, nationality, tax number, gender, information from your identity document(s), employment status and related information and your pictures / pictures of your identity (including biometric information such as a visual image of your face) or other document(s) we may request from time to time.
- **Contact data** includes billing address, residential address, email address and telephone number.
- **Screening data** includes close connections, political background and information pertaining to sanctions and adverse media.
- **Risk assessment data** includes client risk score and client risk categorisation.
- **Economic and appropriateness data** includes employment status, annual income, source of income, current value of wealth, annual investment, investment plans, investment objectives, trading experience, level of education.
- **Financial data** includes bank account and payment card details.
- **Trading data** includes information about your trading activity on our platform, such as instruments traded, orders, positions and position sizes, leverage, opening and closing prices and times, stop-loss and take-profit settings, and realised and unrealised profit and loss.
- **Transaction data** includes details about payments to and from you in relation to our Services.
- **Technical data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access the Services.
- **Communication data** includes communication between you and Capital, including chats, call recordings and emails.
- **Profile data** includes your username and password, your interests, preferences, feedback and survey responses.
- **Usage data** includes information about how you access our Services and use our Services, including user sessions (screen) recordings in some cases.

3. Purposes for which we use personal data

Capital.com, as a data controller, may only use your personal data if there is a lawful basis for such use. The most common lawful bases used by Capital.com are:

- **consent:** in some cases, we may process your personal data only if we obtain your prior consent;
- **performance of a contract:** we will require your personal data to be able to offer you the Services in accordance with the contract terms between you and us;
- **compliance with a legal obligation:** due to the nature of the Services we provide, the laws applicable to our activities require us to collect and store certain data about you; and
- **legitimate interests:** sometimes we rely on our legitimate interests to process your data (e.g. to improve our Services) and we will do so except where such interests are overridden by your interests or fundamental rights and freedoms.
- **recognised legitimate interests:** in certain specific circumstances defined by law, we may process or disclose your personal data on the basis of a recognised legitimate interest without carrying out a balancing test. This lawful basis came into force on 5 February 2026 under the DUAA. There are currently five recognised legitimate interests set out in Annex 1 of the UK GDPR: (i) disclosure to a public body on request to carry out its public task; (ii) national security, public security or defence; (iii) emergencies under the Civil Contingencies Act 2004; (iv) crime prevention, detection, investigation or prosecution; and (v) safeguarding of individuals at risk. A necessity test still applies. This basis does not cover direct marketing or intra-group data sharing — those activities rely on the standard legitimate interests basis under Article 6(1)(f), subject to a legitimate interests assessment. Where we rely on recognised legitimate interests, we will identify it clearly in the table below.

Below you will find a table describing how we may use your personal data and which of the legal bases are used by Capital to ensure lawful data processing:

Purpose/Activity	Type of data	Lawful basis for processing
To create your account	● Identity data ● Contact data ● Technical data	● Performance of a contract when we provide our Services to you
To verify your identity, carry out checks that we are required to conduct by applicable laws and regulations, including: “know your customer” (KYC), anti-money laundering, fraud, sanctions, politically exposed person (PEP) and liveness checks and perform client risk categorisation	● Identity data ● Contact data ● Screening data ● Transaction data ● Risk assessment data ● Technical data ● Communication data ● Financial data ● Usage data	● Compliance with our legal obligations under applicable AML/CFT obligations, namely the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
To obtain and assess economic profile and appropriateness information and categorise the client	● Economic and Appropriateness data	● Compliance with our legal obligations under applicable laws including obligations under the Rules of the Financial Conduct Authority (FCA) and AML/CFT obligations under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
To provide our Services and process transactions including, payments, fees and charges.	● Identity data ● Contact data ● Financial data ● Transaction data ● Technical data ● Profile data	● Performance of a contract when we provide our Services to you
To monitor your transactions for the purposes of detection, storage and reporting of fraudulent activities	● Identity data ● Contact data ● Screening data ● Risk assessment data ● Financial data ● Transaction data ● Technical data ● Usage data	● Compliance with our legal obligations under applicable AML/CFT obligations, namely the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; or our recognised legitimate interests in the detection, investigation and prevention of fraud and financial crime, where processing goes beyond what is strictly required by those obligations

To provide customer support	• Identity data • Contact data • Financial data • Transaction data • Technical data	• Performance of a contract when we provide our Services to you
To send you service notifications related to your use of the Services	• Contact data • Communication data	• Performance of a contract when we provide our Services to you
To record and store communication with you	• Identity data • Contact data • Communication data	• Compliance with our legal obligations under applicable laws, including obligations under the Rules of the Financial Conduct Authority (FCA)
To send you updates and marketing communication as well as to deliver relevant content to you, including ads, suggestions, personalised offers and recommendations	• Identity data • Contact data • Financial data • Transaction data • Technical data • Profile data • Usage data	• Consent, or • our legitimate interests in promoting our Services. Direct marketing is confirmed by the DUAA as capable of constituting a legitimate interest, but a legitimate interests assessment is still required and the processing remains subject to your right to object. You may object to marketing processing at any time.
To measure and improve the effectiveness of our advertising campaigns	• Contact data • Technical data	• Consent
To perform data analytics with respect to our Services for improvement purposes	• Technical data • Usage data	• Our legitimate interests to improve our Services and, where data is shared within the Capital.com group for internal administration, our legitimate interests in the efficient operation of the Group
To manage and protect our business and website including system maintenance	• Identity data • Technical data • Usage data	• Our legitimate interests to improve our Services and protect personal data and the Services; • Performance of a contract when we provide our Services to you
To help us improve our Services by completing a survey, feedback, or review	• Identity data • Profile data	• Consent
To carry out automated appropriateness assessment (determining whether you have sufficient knowledge and experience to trade our products)	• Economic and Appropriateness data • Identity data	• Compliance with our legal obligations under FCA Rules (appropriateness assessment obligation). Where the outcome significantly affects your access to our Services, you have the right to request human review, express your point of view, and contest the

		decision — see Section 6.
To detect and prevent fraud and suspicious activity on your account through automated transaction monitoring	• Identity data • Contact data • Screening data • Risk assessment data • Financial data • Transaction data • Technical data • Usage data	• Compliance with AML/CFT legal obligations (MLR 2017); and/or • our recognised legitimate interests in the detection, investigation and prevention of fraud and financial crime ("crime condition", in force 5 February 2026). You have the right to request human review of significant automated decisions — see Section 6.
To automatically assign a client risk score and determine the appropriate level of customer due diligence to apply to your account	• Identity data • Contact data • Screening data • Risk assessment data • Transaction data • Financial data	• Compliance with AML/CFT legal obligations (MLR 2017 and FCA Rules). You have the right to request human review of significant automated decisions — see Section 6.
To carry out research, testing and analysis to improve our Services and client outcomes, including research into how clients make trading decisions, which we may carry out with academic research partners	• Trading data; • Usage data; • Technical data	• Our legitimate interests in improving our Services and client outcomes and in supporting scientific research.

If you fail or refuse to provide your personal data we need to provide the Services to you or if the processing of personal data is necessary for compliance with our legal obligations (e.g. compliance with anti money laundering rules), you will not be able to access the Services.

4. Cookies

We use cookies and similar technologies when you access or use our Services. Some cookies are essential to the operation of our Services and do not require your consent. Others, including certain analytics cookies that help us understand how our Services are used, functional cookies that improve your experience, and cookies used to detect or prevent fraud, may be placed without your prior consent under UK law, but you can opt out of these at any time using the cookie settings available on our website. Where we rely on your consent to place cookies, we will ask for it before doing so, and you may withdraw that consent at any time. For full details of the cookies we use, their purpose, and how to manage your preferences, please review our Cookie Policy.

5. Sources of personal data

Most of the personal data we process about you is received directly from you. For example, when you register to use the Services or communicate with us, we may receive your identity and contact data from you.

In other cases, we may receive personal data about you from various third parties and publicly accessible sources, including but not limited to social media, search engines, company registers, banks, payment service providers, KYC service providers, advertising networks, analytics providers and screening data vendors.

If you choose to sign in to our Services using a third-party service, such as Google, Facebook, and Apple, you direct the service to send us certain social account information such as your email address.

When you use the Services we may also automatically collect technical data through the use of cookies and similar technologies.

6. Automated decision-making with respect to your personal data

As part of delivering our Services and meeting our obligations under applicable law, Capital.com uses systems that make automated decisions about you, that is, decisions reached without meaningful human involvement at the point of determination. This section explains where we do this, why, and what rights you have.

Where we use automated decision-making

Appropriateness assessment. When you submit your economic and appropriateness questionnaire, our system automatically assesses whether you have sufficient knowledge and experience to trade the products we offer. Where the outcome of this assessment is a decision that significantly affects your access to our Services, you have the rights described below.

Anti-fraud and transaction monitoring. Our anti-fraud systems automatically detect patterns that may indicate fraudulent or suspicious activity on your account. Where a significant decision about your account is made on this basis, we will notify you where we are legally permitted to do so.

Client risk scoring. Our systems automatically assign a risk profile to your account based on a number of factors we are required to consider under applicable AML/CFT legislation. This risk score determines the level of customer due diligence we apply to your account.

Special category data in automated decisions

Where any automated decision relies on special category personal data, such as biometric data used for identity verification, we will only make that decision where we have your explicit consent or where the processing is otherwise permitted under applicable law.

Your rights in relation to automated decisions

Where we make a significant decision about you based solely on automated processing, you have the right to:

- request that a member of our team reviews the decision manually;
- express your point of view in relation to the decision; and
- contest the decision and ask us to reconsider.

To exercise any of these rights, contact us at gdpr.uk@capital.com, quoting your account number and the decision you wish to challenge. We will acknowledge your request within 30 calendar days.

Exercising these rights does not guarantee a different outcome. Where a decision is required by law, for example, a regulatory obligation to refuse access to a product, we will explain the basis for that decision and the options available to you.

7. How do we protect your personal data?

We take all reasonable and appropriate technical and organisational measures to protect all personal data collected by us from loss, theft, misuse and unauthorised access, disclosure, alteration and destruction.

8. How long do we keep your personal data?

Generally, we will retain your personal data for a minimum period of five (5) years after the end of the business relationship with Capital.com to fulfil the specific purpose we collected it for, including the purpose of satisfying any legal, accounting, reporting requirements and our legitimate interests. For example, your personal data will

be generally stored for the period required by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 or the Rules of the Financial Conduct Authority (FCA), namely not less than 5 years after the end of the business relationship with Capital.com. We may store certain personal data for not less than 6 years to meet our book keeping obligations under the tax legislation of the UK.

In certain cases the authorities may require us to store the personal data longer if they deem necessary (e.g. in case of an ongoing investigation). If you have not been actively making use of our financial services for 5 - 6 years (depending on the data), we will remove any details that will identify you or we will securely destroy the records, unless we substantiate why we need the data for a longer period of time.

9. Your rights

With regards to our collection and processing of your personal data you have the right to (subject to applicable exceptions):

1. Obtain confirmation from us as to whether we process your personal data.

2. Access your personal data processed by Capital.com.

3. Correct your personal data.

4. Withdraw your consent to processing at any time, where we rely on consent as our lawful basis. Withdrawal of consent does not affect the lawfulness of any processing carried out before you withdrew it. To withdraw consent, contact us at gdpr.uk@capital.com. Note that withdrawal of consent may mean we are unable to continue providing some or all of our Services to you

5. Obtain restriction of processing, for instance, where you contest the accuracy of your personal data for a period enabling us to verify the accuracy of the personal data,

6. Have your personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others.

7. Erasure of your personal data under certain circumstances. Capital.com is obligated by the UK authorities to keep records of client details and trades for a minimum period of five to six (5-6) years from the end of business relationship with you according to the relevant regulations. See more information about our data retention obligations in section “How long do we keep your personal data” above. Withdraw your consent to processing at any time, where we rely on consent as our lawful basis. Withdrawal of consent does not affect the lawfulness of any processing carried out before you withdrew it. To withdraw consent, contact us at gdpr.uk@capital.com. Note that withdrawal of consent may mean we are unable to continue providing some or all of our Services to you

8. Object to the processing of your personal data where we rely on legitimate interests (Article 6(1)(f) UK GDPR) or recognised legitimate interests as our lawful basis, unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is necessary for the establishment, exercise or defence of legal claims. You have an absolute right to object to processing of your personal data for direct marketing purposes at any time, including profiling related to direct marketing. To object, contact us at gdpr.uk@capital.com stating the processing you wish to object to and the grounds for your objection

9. Rights in relation to profiling. We carry out profiling in connection with our Services — for example, to assess your appropriateness to trade, to assign a client risk score, and to deliver personalised marketing content. You have the right to obtain information about the existence of profiling, the logic involved, and the significance and likely consequences of such processing for you. This information is set out in Section 6 of this Policy. Where profiling is used for direct marketing purposes, you have an absolute right to object to it at any time.

10. Lodge a complaint with the Information Commission (formerly the Information Commissioner’s Office). If you believe we have not complied with your data protection rights, you have the right to lodge a complaint with the UK supervisory authority. The Information Commission’s contact details are set out in

Section 12 of this Policy. You also have the right to make a formal data protection complaint directly to Capital.com — see “Your right to complain to us” below.

To exercise any of the rights listed above, contact our Data Protection team at gdpr.uk@capital.com, quoting your account number and the right you wish to exercise.

How we handle your subject access request

When you submit a subject access request, we will search for your personal data in a way that is reasonable and proportionate to the nature and scope of your request. This means we will conduct a thorough search of the systems and records where your data is reasonably likely to be held, but we are not required to search every system we operate if doing so would be disproportionate given what you have asked for.

If your request is unclear or covers a very broad range of data, we may contact you to ask for clarification before we begin our search. The one-month response period will be paused from the date we send that request until the date we receive your reply.

We will respond to your subject access request within one month of receiving it, or within one month of receiving any clarification we have asked for. Where your request is complex or we are handling a large number of requests at the same time, we may extend this period by up to two further months. We will always tell you within the first month if an extension applies and explain the reason for it.

Your right to complain to us

With effect from 19 June 2026, you have the right to make a formal data protection complaint directly to Capital.com about how we process your personal data. This is a separate right from your other data subject rights listed above.

To submit a complaint, contact us at gdpr.uk@capital.com with the subject line "Data Protection Complaint" and include your account number and a description of your concern. You can also write to us at: Capital Com (UK) Limited, 2nd Floor, 4 Orchard Place, London SW1H 0BF.

We will acknowledge receipt of your complaint within 30 calendar days. We will then investigate and notify you of the outcome and any action taken without undue delay. We keep a record of all complaints received and the steps taken to resolve them.

If you are not satisfied with our response, you have the right to escalate your complaint to the Information Commissioner's Office (ICO). Details of how to contact the ICO are set out in Section 12 of this Policy.

10. How do we share your personal data?

We do not share your personal information with third parties, except as described in this Privacy Policy.

Capital.com is part of the Capital.com Group of companies that all have a role in offering a complete service to our clients. For this reason, the Company may share information with its subsidiaries or affiliated companies, including those located outside the UK or European Economic Area (EEA), in the event such information is reasonably required by the subsidiary to provide the Services to you.

Capital.com may also engage service providers and partners to assist with delivery of the Services:

Category	Purpose
Identity verification service providers	- Document validation and verification - Liveness checks - PEP (politically exposed persons) and sanctions screening - Risk assessment and scoring
Anti-fraud system providers	- Detection and prevention of fraudulent transactions/activities
Payment service providers	- Payment processing - Anti-fraud/risk check system - Application logs for payment system
Banks	- Facilitation of money transfers
Marketing	- Marketing analytics and reporting - Marketing attribution automation
Business intelligence providers	- Product analytics
Project management and customer support providers	- Automation of customer support processes
Cloud service providers	- Hosting of personal data - Storage/Backup
Communication providers	- Email and voice communication - Sending transactional emails and SMS - Call recording, monitoring and transcription

Category	Purpose
Performance monitoring providers	- User sessions (screen) recording and monitoring
Social network platforms	- Managing our relationships with clients - Promoting the Services
Professional Consultants	- Receiving professional services
Advertising analytics	- Receiving advertising analytics and reporting

Where your personal data is transferred to subsidiaries or service providers outside the UK, we take steps to make sure it remains protected. We do this by putting in place appropriate transfer safeguards, which may include a UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses. Before making any such transfer, we carry out a transfer risk assessment to satisfy ourselves that the standard of data protection in the receiving country is not materially lower than that provided under UK data protection law. That assessment takes into account the nature, volume and sensitivity of the data being transferred and the risks associated with the specific transfer.

Capital.com requires all service providers who receive your personal data to put in place appropriate security measures to protect it in accordance with applicable data protection legislation. If you would like further information about the specific safeguards we use for a particular transfer, contact us at gdpr.uk@capital.com.

The countries to which we currently transfer your personal data outside the UK, and the basis on which we do so, are set out in the table below:

Country	UK Adequacy decision?	Transfer mechanism where no adequacy decision
Bulgaria	Yes — EU member state (UK–EU adequacy)	Not applicable
Cyprus	Yes — EU member state (UK–EU adequacy)	Not applicable
Poland	Yes — EU member state (UK–EU adequacy)	Not applicable
Australia	No	UK International Data Transfer Agreement (IDTA) or UK Addendum to EU Standard Contractual Clauses, supported by a transfer risk assessment

Dubai (UAE)	No	UK International Data Transfer Agreement (IDTA) or UK Addendum to EU Standard Contractual Clauses, supported by a transfer risk assessment

When required by the applicable laws, we may disclose your personal data to the relevant government agencies and regulatory authorities, including but not limited to the UK Financial Intelligence Unit (UK FIU) and the FCA.

Some of our service providers require us to include information about their privacy practices in our Privacy Policy:

- Sum & Substance Ltd. We may use Sum & Substance Ltd for customer screening and monitoring. Please refer to Sum & Substance's Privacy Notice to learn more about how Sum & Substance Ltd handles your personal data.
- LexisNexis. We may use LexisNexis to verify information you give to us during the onboarding process. We do so to prevent fraud and comply with our AML obligations. Please refer to LexisNexis Privacy Policy to learn more about how LexisNexis handles your personal data.
- If you opt-in to targeted advertising, we may share your email address with The UK Trade Desk Ltd ("TTD") which transforms such data into a string of text and numbers known as an advertising identifier ("EUID") so that it is no longer recognisable as such. The EUID allows Capital to measure and improve its digital marketing campaigns while complying with data protection laws. TTD is a joint controller for EUID and you can get more information about how they process your data by accessing TTD's privacy notice. You may withdraw your consent for targeted advertising based on EUID by opting out using this link.

11. Privacy Policy updates

Capital.com may update this Privacy Policy from time to time. In the event we materially change this Policy including how it collects, processes or uses your personal information, active clients will be notified as in accordance with the Capital.com's Terms & Conditions. Potential clients are notified by means of the publication of the updated Privacy Policy on our website capital.com.

12. Contact information

If you have questions about this Privacy Policy or our privacy practices, or if you are seeking to exercise any of your rights you can contact us. You may contact us at gdpr.uk@capital.com. Contact details for our DPO and SRI are set out in Section 1 of this Policy.

You have the right to lodge a complaint at the UK Information Commissioner's Office, the details of which are set out below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510
Website: https://ico.org.uk