

Dukascopy Europe IBS AS

Privacy Policy

Version	Approval date
v.5	05.09.2025
v.4	01.11.2022
v.3	01.10.2021
v.2	01.04.2020
v.1	25.05.2018

Effective: 12 September 2025

Owner: Legal and Compliance Department

Applies to: All Divisions

Classification: External

Next review: 4 Sep 2026

Approved by: Supervisory Board

1. TERMS AND ABBREVIATIONS

Client (Data subject) – a natural person who uses, has used or has expressed willingness to use the Services provided by the Company (including Potential clients).

Company (Controller) – Dukascopy Europe IBS AS, registered in the Commercial Register of the Republic of Latvia under No. 40003344762, registered office: Marijas iela 2A, Riga, Latvia.

Controller – a body (the Company) that determines the purposes and means of Processing Personal data.

Data subject – an identified or identifiable natural person (e.g., Client, Client's representative, employee).

DPO – Data Protection Officer.

Dukascopy Group – Dukascopy Bank SA incorporated in the Swiss Confederation (including its Latvian representative office) and Dukascopy Europe IBS AS incorporated in the Republic of Latvia.

EEA – European Economic Area.

EU – European Union.

GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).

Personal data – any information relating to an identified or identifiable natural person (Data subject).

Policy – this Privacy Policy of Dukascopy Europe IBS AS.

Processing – any operations performed on Personal data (collection, recording, storage, use, transfer, erasure etc.).

Profiling – any form of automated Processing of Personal data to evaluate certain personal aspects, in particular to analyse or predict aspects concerning a natural person's economic situation, reliability, behaviour, location or movements, and to support Client due diligence.

Services – any services offered to Clients and other natural persons or legal entities by the Company.

AMLTPF – Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing of the Republic of Latvia.

2. SCOPE

2.1. The goal of this Policy is to inform Data subjects who use or are willing to use the Services about the Processing carried out by the Controller (the Company) and, where relevant, Dukascopy Group, and to ensure necessary data-protection rules and mechanisms.

2.2. This Policy applies to interactions via websites, web or mobile applications, electronic communications (including recorded telephone lines), video identification, at Company premises and by post.

3. PERSONAL DATA CATEGORIES PROCESSED BY THE COMPANY

3.1. The Company may collect and process the following categories of Personal data for the purposes specified under Section 4:

3.1.1. General identification data – name, surname, date of birth, personal identity number, gender, copies and details of identity documents (passport/ID card/driver's licence), photographs and other related data.

3.1.2. Contact details – residence and correspondence address, phone number, e-mail address and related data (where necessary).

3.1.3. Financial and transactional data – bank account information, origin of funds and assets, income and its stability, transactional data, investment goals, risk tolerance, tax identification number (TIN), country of taxation and other related data.

3.1.4. Education and economic activity information – education level, place and area of employment, previous employment, economic/commercial activity, experience in investing and other related data.

3.1.5. Related-persons data – authorised persons/representatives, relatives and whether persons closely related to Clients may be classified as politically exposed persons (PEPs) in accordance with AMLTPF, and other related data.

3.1.6. Service-use and technical data – information on Services used, personal settings, IP address, device identifiers, preferred language, and participation in surveys/contests/campaigns.

3.1.7. Data related to criminal convictions and offences – data on criminal offences of Clients, Potential clients, beneficial owners and representatives thereof, only where permitted by law and with appropriate safeguards.

3.1.8. Audio/Video data – CCTV footage, phone conversation recordings, and video/audio generated during video identification (including liveness checks).

3.2. The list above is not exhaustive. Upon necessity the Company may request, collect and process other Personal data required in accordance with applicable legal enactments.

4. LEGAL BASIS AND PURPOSES FOR PERSONAL DATA PROCESSING

4.1. The Company processes Personal data if at least one of the following legal bases applies:

4.1.1. Contract – Processing is necessary to enter into and perform a Distance agreement or another agreement with the Data subject.

4.1.2. Legal obligation – Processing is necessary for the Company to comply with legal obligations to which it is subject as a Controller (e.g., AMLTPF, MiFID II/MiFIR, tax and accounting laws).

4.1.3. Legitimate interests – Processing is necessary for the purposes of the Company's or a third party's legitimate interests (e.g., IT and payment security, fraud

prevention, service improvement, internal administration and group reporting, and direct marketing of similar Services to existing Clients).

4.1.4. Consent – the Data subject has given clear consent for Processing for one or more specific purposes and may withdraw consent at any time without affecting prior Processing.

4.1.5. Article 10 GDPR – Processing of data relating to criminal convictions and offences only where authorised by EU or Latvian law (e.g., AMLTPF) and subject to appropriate safeguards.

4.2. The Company processes Personal data for the following purposes:

4.2.1. to provide and administer Services;

4.2.2. to send administrative information, including updates to policies and changes to agreement terms;

4.2.3. to send information about Services, products, educational materials, upcoming events and other information that may be useful to the Client in relation to the Services (you may object at any time to direct marketing);

4.2.4. to assess and mitigate risks related to money laundering, terrorism and proliferation financing, as well as transaction-related risks;

4.2.5. to comply with legal obligations and/or government authorities' requests;

4.2.6. in relation to establishment, exercise or defence of legal claims and the Company's legitimate interests;

4.2.7. to provide additional or supportive services.

5. AUTOMATED DECISION-MAKING AND PROFILING

5.1. Automated decision-making and profiling are used by the Company during Client Personal data Processing to create Client risk profiles, perform Client due diligence and monitor transactions to counter money laundering and terrorism and proliferation financing. Based on the results of the aforementioned processes, Company staff may make individual decisions for each Client.

5.2. Where a decision producing legal or similarly significant effects on a Client is based solely on automated Processing, the Company ensures such Processing is necessary for entering into or performing a contract or is authorised by law, and the Client has the right to obtain human intervention, to express their point of view and to contest the decision.

6. DISCLOSURE OF PERSONAL DATA

6.1. The Company discloses Clients' Personal data only insofar as necessary for the performance of delegated functions and where there is an adequate legal basis.

6.2. The Company may disclose Personal data to:

6.2.1. selected and designated third parties, including Dukascopy Group providers that perform services on behalf of Dukascopy Group under a written agreement ensuring

appropriate safeguards and Processing limitations (including providers of IT/cloud, audit, identity verification, marketing, translation and/or due-diligence services, data analysis);

6.2.2. Dukascopy Group entities for internal administration, risk control and consolidated reporting;

6.2.3. payment, trading, settlement, correspondent banking and market-infrastructure partners;

6.2.4. professional advisers (e.g., auditors, lawyers, insurers);

6.2.5. government, regulatory or other law-enforcement agencies/authorities in cases specified by law;

6.2.6. third parties upon the Client's instruction or where necessary to establish, exercise or defend legal claims.

7. TRANSFER OF PERSONAL DATA OUTSIDE THE EU/EEA

7.1. Personal data may be transferred by the Company outside the EU, the EEA and/or the Swiss Confederation only where appropriate safeguards are in place and at least one of the following applies:

7.1.1. the European Commission has adopted an adequacy decision for the destination country or framework (e.g., Switzerland; the EU-U.S. Data Privacy Framework for certified U.S. recipients);

7.1.2. the transfer is subject to Standard Contractual Clauses (SCCs) adopted by the European Commission (including transfer-impact assessment and, where appropriate, supplementary measures);

7.1.3. the transfer is necessary for entering into or performing an agreement with Clients for the provision of Services;

7.1.4. the transfer is required under EU or Latvian legal acts;

7.1.5. the Client has given explicit consent to the transfer.

8. CLIENT'S RIGHTS

8.1. Each Client has the following rights:

8.1.1. the right to access their Personal data processed by the Company upon written request; if a request is excessive and/or repetitive, the Company may charge a reasonable fee based on administrative costs of preparing a copy, subject to legal limitations;

8.1.2. the right to obtain rectification of inaccurate or incomplete Personal data without undue delay;

8.1.3. the right to request erasure (the "right to be forgotten") of Personal data undergoing Processing in the Company, except where Processing is necessary for performance of a Distance agreement or compliance with a legal obligation under EU or Latvian law (e.g., AMLTPF);

8.1.4. the right to request restriction of Processing, subject to evaluation of any conflicting legal grounds;

8.1.5. the right to data portability where Processing is based on consent or a Distance agreement and carried out by automated means, provided this does not adversely affect the rights and freedoms of others;

8.1.6. the right to object at any time to Processing based on the Company's legitimate interests, including objecting at any time to direct marketing;

8.1.7. the right to be informed about automated individual decision-making, including profiling, and to request human intervention where applicable;

8.1.8. the right to lodge a complaint with the personal data protection supervisory authority of the Republic of Latvia (Data State Inspectorate) if a complaint cannot be resolved with the Company/DPO (see Section 12).

8.2. All rights shall be exercised in good faith and on a written-request basis. The Company will respond within one month, extendable as permitted by law.

9. LEGAL WAIVER

The Client agrees not to hold the Company, Dukascopy Group and their employees and affiliates liable for losses of any kind, including financial, suffered by the Client due to disclosure or use of the Client's Personal data (e.g., login details) by a third party where such disclosure results from the Client's actions or negligence or from abusive/fraudulent acquisition from the Client by third parties. The Client is responsible for safeguarding credentials and any disclosure to unauthorised third parties.

10. PERSONAL DATA RETENTION PERIOD

10.1. The period of Personal data retention depends on the purpose of Processing specified by the Company and shall not exceed what is necessary for such purposes.

10.2. In determining retention periods, the Company takes into account agreements with Clients and contractual obligations, the Company's legitimate interests and relevant legal enactments. In determining retention periods, the Company takes into account agreements with Clients and contractual obligations, the Company's legitimate interests and relevant legal enactments.

10.3. The Company generally stores the Client's Personal data for five (5) years after termination of the business relationship with the Client, unless otherwise provided by applicable laws and regulations.

10.4. MiFID II recorded communications on recorded lines are retained for at least five (5) years (and up to seven (7) years upon request of a competent authority). AML/CTF records are retained for at least five (5) years from the end of the business relationship or the date of an occasional transaction, with extensions where permitted by law.

11.COOKIES

Cookies (small text files placed on the device) are used on the Company's website to make it work more efficiently, store information about Clients' preferences and provide statistical information to the Company. Cookies are not used to identify Clients personally. For detailed information on cookie types and purposes, please see the Company's Cookie Policy.

12.CONTACT DETAILS

12.1. Client support (24/7): phone +371 67 399 000; +371 67 399 039; e-mail: support@dukascopy.eu.

12.2. DPO: e-mail dpo@dukascopy.eu; post: Data Protection Officer, Dukascopy Europe IBS AS, Marijas iela 2A, Riga, Latvia.

13.FINAL PROVISIONS

The Company reserves the right to amend the Policy unilaterally at any time. Material changes will be posted on the Company's website together with the updated text of the Policy. The Client undertakes to review the Company's website regularly to check for updates to the Policy.