

## GDPR Data Privacy Policy

### **Important Information**

In line with Article 24 GDPR (EU) 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons, BUX has implemented appropriate technical and organisational measures to ensure compliance with, and pursuance to, the General Data Protection Regulation (GDPR). This policy stands as the cornerstone of BUX's compliance with GDPR and is reviewed and updated accordingly.

BUX is a trading name of ayondo markets Limited. ayondo markets Limited is a company registered in England and Wales under register number 03148972. ayondo markets Limited is authorised and regulated by the Financial Conduct Authority, FCA Register number 184333.

**General Data Protection Regulation (GDPR)**

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organisations across the region approach data privacy.

In line with Article 5 of GDPR, BUX must conform to the following principles at all times.

<b>1. Lawfulness, fairness and transparency</b>	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
<b>2. Purpose limitation</b>	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
<b>3. Data minimisation</b>	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
<b>4. Accuracy</b>	Personal data shall be accurate and, where necessary, kept up to date.
<b>5. Storage limitation</b>	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
<b>6. Integrity and confidentiality</b>	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
<b>7. Accountability</b>	The controller shall be responsible for, and be able to demonstrate compliance with GDPR.

BUX is at all times responsible for, and able to demonstrate compliance with the aforementioned principles.

Any reference to 'Us', 'Our', 'We' or 'BUX' is a reference to each group company within the ayondo Group as the context requires unless otherwise stated.

## **Applicability**

This privacy policy applies to the processing activities of ayondo Group. The three main trading entities within ayondo Group are:

- ✓ ayondo markets Limited: a company registered in England and Wales under register number 03148972. The registered address of the company is 1st Floor, 7-10 Chandos Street, London, W1G 9DQ United Kingdom. It is registered with the UK Information Commissioner under registration number is Z1457804.
- ✓ ayondo portfolio management GmbH: a company registered in Germany, commercial register of the District Court of Frankfurt am Main HRB 102933. The registered address of the company is Niddastraße 91, 60329 Frankfurt am Main, Germany.
- ✓ ayondo GmbH: a company registered in Germany, commercial register of the District Court of Frankfurt am Main 84169. The registered address of the company is Niddastraße 91, 60329 Frankfurt am Main, Germany.

ayondo Group provides execution only and social trading services to retail and professional clients for Spread Betting ('SB') and Contract for Difference ('CFD') products via its subsidiaries, ayondo markets Limited, London and ayondo portfolio management GmbH, Frankfurt respectively. ayondo GmbH is a tied agent of ayondo markets Limited. The above group entities are individual data controllers of personal data in respect of the services provided by them individually.

## **Compliance Monitoring**

In order to maintain a high level of compliance in relation to the rules stipulated within this policy, BUX carries out an annual Data Protection compliance audit. Conducting a thorough diagnostic audit allows BUX to recognise any deficiencies or areas for improvement; upon mitigation, ensuring total compliance to GDPR. Examples of the areas covered within an audit include:

- (a) Data protection governance, and the structures, policies and procedures to ensure GDPR compliance;
- (b) The processes for managing both electronic and manual records containing personal data;
- (c) The processes responding to any request for personal data;
- (d) The technical and organisational measures in place to ensure that there is adequate security over personal data;
- (e) The provision and monitoring of staff data protection training and the awareness of data protection; and
- (f) Data audit as per Appendix 2.

## **Data Subject Rights and Requests**

GDPR provides the following rights for individuals:

1. The right to be informed;

2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object; and
8. Rights in relation to automated decision making and profiling.

BUX has in place adequate systems and controls to enable and facilitate the application of the eight data subject rights listed above.

When a data subject makes a request, BUX will embark on a pragmatic decision-making process headed up by the Data Protection Officer.

Unless BUX deems requests to be excessive or unnecessary in their nature, no fee will be charged to the data subjects for considering and/or complying with such requests.

### **Rights to Access**

All requests of this nature should be referred to the Data Protection Officer. BUX shall respond to such requests within 30 days.

The data subject has the right to obtain the following information from BUX:

- (a) The purposes of the processing;
- (b) The categories of personal data concerned;
- (c) The recipients or categories of personal data stored for the data subject;
- (d) The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; and
- (e) The use of any automated decision-making e.g. profiling.

When requested, BUX shall provide a copy of the personal data held. For any further copies requested by the data subject, BUX may charge a reasonable fee based on administrative costs. Where requests are made via electronic means, BUX shall provide the data in a commonly used electronic form.

### **Right to Rectification**

BUX shall ensure all that data subjects are able to exercise their right to obtain from the firm, without undue delay, the rectification of inaccurate personal data concerning him or her.

### **Right to Erasure**

Without undue delay, BUX shall erase personal data of a data subject where requested, and where one of the following grounds applies:

- (a) The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- (b) The data subject withdraws consent which the processing is based on, and where there is no other legal ground for the processing;

- (c) The data subject objects to the processing and there are no overriding legitimate grounds for the processing, or where the data subject objects to processing;
- (d) The personal data has been unlawfully processed;
- (e) The personal data has to be erased compliant with a legal obligation in the member state law; and/or
- (f) The personal data has been collected in relation to the offer of information society services.

Article 17 3 (b) GDPR, states that the right to erasure is disappplied where the firm must retain data in order to comply with other applicable regulation. The superseding regulations in BUX's case are The Money Laundering Regulations requirement for firms to hold KYC data for 5 years, and MiFID II Article 16 requirements on record keeping. This is referred to in BUX's privacy notice.

### **Right to Restrict Processing**

BUX will cease the processing of personal data in the following circumstances:

- (a) Where an individual contests the accuracy of the personal data, BUX will restrict the processing until the accuracy of the data is verified;
- (b) Where an individual has objected to the processing and the Group is considering whether it has legitimate grounds to override those of the individual;
- (c) When processing is found to be unlawful and the individual opposes erasure and requests a restriction instead; and/or
- (d) If the Group no longer needs the data but the individual requires the data to establish, exercise or defend a legal claim.

### **Right to Data Portability**

The right to portability only applies:

- (a) To personal data an individual has provided to a controller;
- (b) Where the processing is based on the individual's consent or for the performance of a contract; and
- (c) When processing is carried out by automated means.

To comply, BUX must:

- (a) Provide the personal data in a structured, commonly used and machine readable format;
- (b) Provide the data free of charge (unless excessive or unnecessary);
- (c) If requested and technically feasible, transmit the data directly to another organisation; and
- (d) Consider possible prejudice of the rights of individuals, where the personal data concerns more than one individual.

### **Consent**

Consent must be given by a clear affirmative act, which establishes freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of their data. BUX will obtain consent via a written statement, by electronic means, or an oral statement.

BUX requests, manages and records consent pursuant to Articles 5, 6, 7 and 9 of GDPR.

- (a) BUX checks that consent is the most appropriate lawful basis for processing;
- (b) BUX makes the request for consent prominent and separate from its terms and conditions;
- (c) BUX requests a positive opt in;
- (d) BUX does not use pre-ticked boxes or any other type of default consent;
- (e) BUX uses clear, plain language that is easy to understand;
- (f) BUX specifies why it wants the data and its purpose;
- (g) BUX provides granular options to consent separately to different purposes and types of processing;
- (h) BUX names its organisation and any third party controllers who will be relying on its consent;
- (i) BUX ensures that individuals can refuse to consent without detriment; and
- (j) BUX avoids making consent a precondition of service.

BUX records when and how the firm obtained consent from individuals. The firm also keeps a record of the exact information originally provided.

Exercises BUX may carry out to ensure the appropriate management of consent include the following:

- (a) BUX regularly reviews consents to check that the relationship, the processing and the purposes have not changed;
- (b) BUX has processes in place to refresh consent at appropriate intervals, including any parental consents (if so applicable);
- (c) BUX considers using privacy dashboards or other preference-management tools as a matter of good practice;
- (d) BUX makes it simple for individuals to withdraw their consent at any time, and publicises how this is done;
- (e) BUX acts on withdrawals of consent as soon as possible; and
- (f) BUX does not penalise individuals who wish to withdraw consent.

BUX will not infer consent from silence or inactivity. When the processing of personal data has multiple purposes, BUX will obtain consent for all of these. Where a data subject's consent is to be given following a request by electronic means, BUX will ensure the request is clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

### **Data Privacy by Design**

BUX has in place technical and organisational measures which integrate data protection into processing activities.

Privacy and data protection is a key consideration in the early stages of any project BUX undertakes

For example, when:

- (a) Building new IT systems for storing or accessing personal data;
- (b) Developing legislation, policy or strategies that have privacy implications;
- (c) Embarking on a data sharing initiative; and/or

- (d) Using data for new purposes.

Privacy and data protection considerations will be integrated within BUX risk management methodologies and policies.

### **Data Protection Impact Assessments (DPIA)**

BUX carries out a DPIA where data processing is likely to result in high risk to individuals, for example:

- (a) Where a new technology is being implemented;
- (b) Where a profiling operation is likely to significantly affect individuals; and/or
- (c) Where there is large scale processing of special categories of data.

In assessing the level of risk, BUX considers both the likelihood and severity of any impact to the individuals concerned.

BUX ensures that there is a sound understanding of DPIA amongst certain members of the firm.

- (a) BUX provides training so that all staff understand the need to consider a DPIA at the early stages of any plan involving personal data;
- (b) BUX's existing policies, processes and procedures include references to DPIA requirements, where applicable;
- (c) BUX understands the types of processing that requires a DPIA;
- (d) BUX creates and documents a robust DPIA process; and
- (e) BUX provides training for relevant staff on how to carry out a DPIA.

### **Breach Reporting**

In the case of a personal data breach, BUX shall without undue delay, and where practicable, notify the relevant supervisory authority not later than 72 hours after having become aware of the breach. This is not required where the breach will not likely result in a risk to the rights and freedoms of natural persons. Where the notification is not made within 72 hours, BUX must provide a valid reason for the delay. Relevant supervisory authorities contact details can be found within Appendix 1.

Notifications made by BUX shall at least:

- (a) Describe the nature of the personal data breach;
- (b) Communicate the name and contact details of the relevant department handling the data breach;
- (c) Describe the likely consequences of the personal data breach; and
- (d) Describe the measure taken or proposed to be taken by BUX to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of subjects, BUX shall communicate the data breach to the data subject without undue delay.

BUX shall communicate the matter to the data subject in clear and plain language the nature of the personal data breach, detailing at least the information in points (b), (c) and (d) as above.

### **Record Keeping**

BUX employs fewer than 250 people and therefore Article 30 GDPR is technically not applicable. That being said, due to the other data monitoring requirements dictated by GDPR and for best practice, BUX shall maintain a record of processing activities under its responsibility. That record shall contain the following information:

- (a) The name and contact details of the controller;
- (b) The purposes of the processing;
- (c) A description of the categories of data subjects and of the categories of personal data;
- (d) The recipients to whom the personal data has been or will be disclosed including recipients in third countries or international organisations;
- (e) Where applicable, transfers of personal data to a third country or international organisation, including the identification of that third country or international organisation;
- (f) Where possible, the envisaged time limits for erasure of the different categories of data; and
- (g) Where possible, a description of the technical and organisation measures referred to in Article 32(1).

BUX keeps records in writing, and in electronic format.

If requested by the relevant supervisory authority, BUX will make records available immediately.

### **Complaints Handling**

Upon receipt of a data subject complaint, BUX shall internally investigate the complaint. BUX shall inform the data subject of progress and subsequently the outcome of the complaint. This must be communicated within a reasonable period.

Where the complaint cannot be resolved between the data subject and BUX, the data subject may choose to seek redress through mediation, litigation procedure or via a complaint to the supervisory authority. BUX must inform data subjects of their right to complain directly to the relevant supervisory authority.



**Appendix 1**

<b>Personal data</b>	Any information (including opinions and intentions) which relates to an identified or identifiable natural person
<b>Data controller</b>	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
<b>Data subject</b>	The identified or identifiable natural person to which the data refers
<b>Consent</b>	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
<b>International organisation</b>	An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
<b>Supervisory Authority</b>	Data protection supervisory authority for BUX:  Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF  Tel: +44 (0)303 123 1113 Fax: +44 (0)1625 524 510  Website: <a href="http://www.ico.org.uk">www.ico.org.uk</a>

**Appendix 2****Monitoring Data checklist**

Details of the data held by ayondo Group	
Reason for holding the data	
Methods for obtaining the data	
Date that the data was obtained	
Individuals responsible for the data	
Data storage	
Data retention	
Data deletion methodology	