GDPR Data Protection Policy

Für Deutsch, klicke HIER

Voor Nederlands, klik HIER

Per italiano, cliccare

Para español, hacer clic AQUI

Pour le français, cliquer ICI

For dansk, klik her

För Svenska, klicka HÄR

GDPR Data Protection 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.

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.

1. Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
5. Storage limitation	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.
6. Integrity and confidentiality	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.
7. Accountability	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 disapplied 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 counties 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

Personal data	Any information (including opinions and intentions) which relates to an identified or identifiable natural person
Data controller	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
Data subject	The identified or identifiable natural person to which the data refers
Consent	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
International organisation	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.
Supervisory Authority	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: www.ico.org.uk

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	

Datenschutzrichtlinie der DSGVO

Wichtige Informationen

Im Einklang mit Artikel 24 DSGVO (EU) 2016/679 hat die Gruppe unter Berücksichtigung von Art, Umfang, Kontext und Zweck der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen ergriffen zur Gewährleistung der Compliance und der Einhaltung der Datenschutz-Grundverordnung (DSGVO). Diese Richtlinie bildet den Eckpfeiler der Einhaltung der DSGVO durch die Gruppe und wird entsprechend überprüft und aktualisiert.

Allgemeine Datenschutzverordnung (DSGVO)

Die EU-Datenschutzgrundverordnung (Datenschutz-Grundverordnung) ersetzt die Datenschutzrichtlinie 95/46 / EG und soll die Datenschutzgesetze in Europa harmonisieren, den Datenschutz aller EU-Bürger schützen und stärken und die Art und Weise, wie Organisationen in der Region mit Datenschutz umgehen, neu gestalten.

Gemäß Artikel 5 der DSGVO muss die ayondo Gruppe jederzeit die folgenden Grundsätze einhalten.

1. Rechtmäßigkeit, Fairness und Transparenz	Personenbezogene Daten werden im Einklang mit dem Gesetz, gerecht und in transparenter Weise gegenüber der betroffenen Person verarbeitet.
2. Zweckbeschränkung	Personenbezogene Daten werden für bestimmte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer Weise verarbeitet, die mit diesen Zwecken nicht vereinbar ist.
3. Datenminimierung	Personenbezogene Daten müssen angemessen, relevant und auf das beschränkt sein, was für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
4. Richtigkeit	Personenbezogene Daten müssen korrekt sein und, wenn nötig, auf dem neuesten Stand gehalten werden.
5. Beschränkung der Speicherdauer	Personenbezogene Daten sind in einer Form aufzubewahren, in der die betroffenen Personen nicht länger als für die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, erforderlich sind, identifiziert werden können.
6. Integrität und Vertraulichkeit	Personenbezogene Daten werden so verarbeitet, dass eine angemessene Sicherheit der personenbezogenen Daten, einschließlich des Schutzes vor unbefugter oder rechtswidriger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Beschädigung, durch geeignete technische oder organisatorische Maßnahmen gewährleistet ist.
7. Rechenschaftspflicht	Der für die Verarbeitung zuständige Leiter ist für die Einhaltung der DSGVO verantwortlich und in der Lage, diese nachzuweisen.

BUX ist immer für die Einhaltung der zuvor beschriebenen Richtlinien verantwortlich und stets in der Lage, diese nachzuweisen.

Jede Verweisung auf "uns", "unser", "wir" oder "BUX" ist eine Bezugnahme auf jedes Unternehmen innerhalb der ayondo Gruppe, soweit der Kontext es erfordert und sofern nicht anders angegeben

Anwendbarkeit

Diese Datenschutzerklärung gilt für die Verarbeitungsaktivitäten der ayondo Gruppe. Die drei wichtigsten Handelseinheiten innerhalb der ayondo Gruppe sind:

- ✓ ayondo markets Limited: Ein in England und Wales unter der Nummer 03148972 registriertes Unternehmen. Die registrierte Adresse des Unternehmens ist 1. Stock, 7-10 Chandos Street, London, W1G 9DQ Vereinigtes Königreich. Es ist beim britischen Information Commissioner unter der Registriernummer Z1457804 registriert.
- ✓ ayondo portfolio management GmbH: eine in Deutschland eingetragene Gesellschaft, Handelsregister des Amtsgerichts Frankfurt am Main HRB 102933. Die eingetragene Anschrift der Gesellschaft lautet Niddastraße 91, 60329 Frankfurt am Main, Deutschland.
- ✓ ayondo GmbH: eine in Deutschland eingetragene Gesellschaft, Handelsregister des Amtsgerichts Frankfurt am Main 84169. Die eingetragene Anschrift der Gesellschaft lautet Niddastraße 91, 60329 Frankfurt am Main, Deutschland.

Die ayondo Gruppe bietet Einzelhändlern und gewerbetreibenden Kunden reine Ausführungs- und Social-Trading-Dienstleistungen für Spread Betting ('SB') - und Contract-for-Difference ('CFD') - Produkte über ihre Tochtergesellschaften, ayondo markets Limited, London bzw. ayondo Portfolio Management GmbH, Frankfurt. Die ayondo GmbH ist ein Vermittler von ayondo markets Limited. Die oben genannten Gruppenunternehmen sind in Bezug auf Ihre personenbezogenen Daten und auf die von ihnen erbrachten Dienstleistungen individuelle Datenverantwortliche.

Compliance-Überwachung

Um ein hohes Maß an Compliance in Bezug auf die in dieser Richtlinie festgelegten Regeln zu gewährleisten, führt die Gruppe einen jährlichen Datenschutz-Compliance-Audit durch. Durch die Durchführung eines gründlichen diagnostischen Audits kann die ayondo Gruppe Mängel oder Bereiche für Verbesserungen erkennen und entsprechende Abhilfe schaffen, Gewährleistung der vollständigen Einhaltung der DSGVO. Beispiele für die in einer Prüfung abgedeckten Bereiche sind:

(a) Datenschutz-Governance sowie die Strukturen, Richtlinien und Verfahren zur Gewährleistung der Einhaltung der DSGVO;
(b) Die Verfahren zur Verwaltung von sowohl elektronischen als auch manuellen Aufzeichnungen mit personenbezogenen Daten;
(c) Die Prozesse reagieren auf jede Anfrage nach personenbezogenen Daten;
(d) Die technischen und organisatorischen Maßnahmen zur Gewährleistung einer ausreichenden Sicherheit personenbezogener Daten;

(e) Die Bereitstellung und Überwachung von Schulungen zum Datenschutz für die Mitarbeiter und das Bewusstsein für den Datenschutz; und
(f) Datenaudit gemäß Anlage 2

Rechte un Anfragen von Datensubjekten

Die DSGVO bietet folgende Rechte für Einzelpersonen:

1. Das Recht, informiert zu werden;
2. Das Recht auf Zugang;
3. Das Recht auf Nachbesserung;
4. Das Recht auf Löschung;
5. Das Recht, die Verarbeitung zu beschränken;
6. Das Recht auf Datenübertragbarkeit;
7. Das Recht auf Widerspruch; und
8. Rechte in Bezug auf automatisierte Entscheidungsfindung und Profilerstellung.

Die ayondo Gruppe verfügt über angemessene Systeme und Kontrollen, um die Anwendung der oben aufgeführten acht datenschutzrechtlichen Bestimmungen zu ermöglichen und zu erleichtern.

Wenn eine betroffene Person eine Anfrage einreicht, wird die Gruppe einen pragmatischen Entscheidungsprozess einleiten, der vom Datenschutzbeauftragten geleitet wird.

Sofern die Gruppe nicht der Ansicht ist, dass Anträge übermäßig oder in ihrer Natur unnötig sind, wird den betroffenen Personen keine Gebühr für die Prüfung und / oder die Erfüllung solcher Anfragen in Rechnung gestellt.

Zugriffsrechte

Alle Anfragen dieser Art sollten an den Datenschutzbeauftragten weitergeleitet werden. Die ayondo Gruppe reagiert auf solche Anfragen innerhalb von 30 Tagen.

Die betroffene Person hat das Recht, folgende Informationen von ayondo zu erhalten:

(a) Die Zwecke der Verarbeitung;
(b) Die Kategorien der betroffenen personenbezogenen Daten;
(c) Die Empfänger oder Kategorien personenbezogener Daten, die für die betroffene Person gespeichert sind;
(d) Der geplante Zeitraum, für den die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien, die für die Bestimmung dieses Zeitraums verwendet wurden; und
(e) Der Einsatz automatisierter Entscheidungen wie z. B. Profiling.

Auf Anfrage stellt die Gruppe eine Kopie der gespeicherten personenbezogenen Daten zur Verfügung. Für weitere Kopien, die von der betroffenen Person angefordert werden, kann die Gruppe eine angemessene Gebühr basierend auf den Verwaltungskosten erheben. Wenn Anfragen auf elektronischem Wege erfolgen, muss die Gruppe die Daten in einer allgemein verwendeten elektronischen Form zur Verfügung stellen.

Recht auf Berichtigung

Die ayondo Gruppe stellt sicher, dass alle betroffenen Personen ihr Recht ausüben können, unverzüglich von dem Unternehmen die Berichtigung ungenauer personenbezogener Daten, die sie betreffen, zu erhalten.

Recht auf Löschung

Die ayondo Gruppe löscht unverzüglich personenbezogene Daten einer betroffenen Person, wenn dies verlangt wird, und wenn einer der folgenden Gründe zutrifft:

(a) Die personenbezogenen Daten sind nicht mehr in Bezug auf die Zwecke erforderlich, für die sie erhoben oder anderweitig verarbeitet wurden;
(b) Die betroffene Person widerruft die Zustimmung, auf die sich die Verarbeitung stützt, und wenn es keinen anderen rechtlichen Grund für die Verarbeitung gibt;
(c) Der Betroffene widerspricht der Verarbeitung und es gibt keine zwingenden legitimen Gründe für die Verarbeitung oder wenn die betroffene Person der Verarbeitung widerspricht;
(d) Die personenbezogenen Daten wurden rechtswidrig verarbeitet.
(e) Die personenbezogenen Daten müssen gemäß einer gesetzlichen Verpflichtung des Mitgliedsstaates gelöscht werden; und / oder
(f) Die personenbezogenen Daten wurden im Zusammenhang mit dem Angebot der Dienste der Informationsgesellschaft erhoben.

Artikel 17, 3 (b) DSGVO besagt, dass das Recht auf Löschung ausgeschlossen ist, wenn das Unternehmen Daten speichern muss, um anderen geltenden Vorschriften zu entsprechen. Die ersetzenden Bestimmungen in der ayondo Gruppe sind die Vorschriften zur Geldwäsche, nach denen Unternehmen KYC-Daten für 5 Jahre aufbewahren müssen, und MiFID II Artikel 16 Anforderungen an die Aufbewahrung von Aufzeichnungen. Dies wird in der Datenschutzmitteilung der ayondo Gruppe beschrieben.

Recht zur Einschränkung der Verarbeitung

Die ayondo Gruppe wird die Verarbeitung personenbezogener Daten unter folgenden Umständen einstellen:

(a) Wenn eine Einzelperson die Genauigkeit der personenbezogenen Daten bestreitet, wird die Gruppe die Verarbeitung einschränken, bis die Genauigkeit der Daten verifiziert ist;
(b) Wenn eine Einzelperson Einwände gegen die Verarbeitung erhoben hat und die Gruppe prüft, ob sie legitime Gründe hat, um die der Einzelperson außer Kraft zu setzen;
(c) Wenn sich die Verarbeitung als rechtswidrig herausstellt und die Person der Löschung widerspricht und stattdessen eine Einschränkung anfordert; und / oder
(d) Wenn die Gruppe die Daten nicht mehr benötigt, aber die Person die Daten benötigt, um einen Rechtsanspruch festzustellen, auszuüben oder zu verteidigen.

Recht auf Datenübertragbarkeit

Das Recht auf Übertragbarkeit gilt nur

(a) für personenbezogene Daten, die eine Person einem Verantwortlichen zur Verfügung gestellt hat;
(b) Wenn die Verarbeitung auf der Zustimmung des Einzelnen oder auf der Erfüllung eines Vertrags beruht; und
(c) Wenn die Verarbeitung automatisiert erfolgt.

Zum Zweck der Compliance muss die ayondo Gruppe Folgendes tun:

(d) Bereitstellung der personenbezogenen Daten in einem strukturierten, häufig verwendeten und maschinenlesbaren Format;
(e) Kostenlose Bereitstellung der Daten (sofern diese nicht übermäßig oder unnötig sind);
(f) Falls gewünscht und technisch machbar, Übermittlung der Daten direkt an eine andere Organisation; und
(g) Beachtung von ggfs. existierenden Ausschlüssen gegenüber den Rechten von Einzelpersonen, wenn die personenbezogenen Daten mehr als eine Person betreffen.

Zustimmung

Die Zustimmung muss durch eine klare zustimmende Handlung erfolgen, die eine frei gegebene, spezifische, informierte und eindeutige Angabe der Zustimmung der betroffenen Person zur Verarbeitung ihrer Daten enthält. Die ayondo Gruppe wird die Einwilligung durch eine schriftliche Erklärung, auf elektronischem Wege oder durch eine mündliche Erklärung erhalten.

Die ayondo Gruppe beantragt, verwaltet und protokolliert die Zustimmung gemäß den Artikeln 5, 6, 7 und 9 der DSGVO.

(a) Die ayondo Gruppe prüft, ob die Zustimmung die am besten geeignete rechtmäßige Grundlage für die Verarbeitung ist;
(b) Die ayondo Gruppe stellt den Antrag auf Einwilligung herausgehoben und getrennt von seinen Geschäftsbedingungen bereit;
(c) Die ayondo Gruppe fordert ein positives Opt-In an;
(d) Die ayondo Gruppe verwendet keine vorgekreuzten Kästchen oder eine andere Art von Standardzustimmung;
(e) Die ayondo Gruppe verwendet eine klare, einfache Sprache, die leicht zu verstehen ist.
(f) Die ayondo Gruppe gibt an, warum sie die Daten haben möchte sowie deren Zweck;
(g) Die ayondo Gruppe bietet granulare Optionen, um die verschiedenen Zwecke und Arten der Verarbeitung getrennt voneinander zu genehmigen;
(h) Die ayondo Gruppe benennt ihre Organisation und alle Verantwortlichen Dritter, die sich auf ihre Zustimmung verlassen;
(i) Die ayondo Gruppe stellt sicher, dass Einzelpersonen die Einwilligung ohne Nachteil verweigern können; und
(j) Die ayondo Gruppe vermeidet die Zustimmung als eine Vorbedingung für den Service.

Die ayondo Gruppe erfasst, wann und wie das Unternehmen die Zustimmung von Einzelpersonen erhalten hat. Die Firma speichert auch die genauen Informationen, die ursprünglich zur Verfügung gestellt wurden.

Ausübungen durch die ayondo Gruppe kann Folgendes durchführen, um die angemessene Verwaltung der Zustimmung zu gewährleisten:

(a) Die ayondo Gruppe überprüft regelmäßig die Zustimmungen, um zu überprüfen, dass sich die Beziehung, die Verarbeitung und die Zwecke nicht geändert haben;
(b) Die ayondo Gruppe verfügt über Verfahren, um die Einwilligung in angemessenen Zeitabständen, einschließlich etwaiger elterlicher Einwilligungen (falls zutreffend), zu aktualisieren.
(c) Die ayondo Gruppe erwägt, Datenschutz-Dashboards oder andere Tools zur Präferenzverwaltung als gute Praxis zu verwenden.
(d) Die ayondo Gruppe macht es für Einzelpersonen einfach, ihre Zustimmung jederzeit zurückzuziehen, und veröffentlicht die Art und Weise, wie dies getan wird;
(e) Die ayondo Gruppe handelt so schnell wie möglich bei dem Entzug der Einwilligung; und
(f) Die ayondo Gruppe bestraft niemanden, der seine Zustimmung widerrufen möchte.

Die ayondo Gruppe schließt keine Zustimmung aus Schweigen oder Inaktivität ein. Wenn die Verarbeitung personenbezogener Daten mehrere Zwecke erfüllt, wird die ayondo Gruppe die Zustimmung für alle diese erhalten. Wenn die Einwilligung der betroffenen Person aufgrund einer Anfrage auf elektronischem Wege erteilt wird, stellt die Gruppe sicher, dass die Anfrage klar, präzise und nicht unnötig störend für die Nutzung des Dienstes ist, für den sie bereitgestellt wird.

Datenschutz nach Design

Die ayondo Gruppe verfügt über technische und organisatorische Maßnahmen, die den Datenschutz in Verarbeitungsprozesse integrieren.

Vertraulichkeit und Datenschutz sind in den frühen Phasen eines Projekts, das die Gruppe unternimmt, von zentraler Bedeutung

Zum Beispiel:

(a) Beim Aufbau neuer IT-Systeme zur Speicherung oder zum Zugriff auf personenbezogene Daten;
(b) Bei der Entwicklung von Rechtsvorschriften, Strategien oder Strategien mit Auswirkungen auf die Privatsphäre;
(c) Beim Einstieg in eine Datenfreigabe-Initiative; und / oder
(d) Bei der Verwendung von Daten für neue Zwecke.

Überlegungen zur Vertraulichkeit und zum Datenschutz werden in die Methoden und Richtlinien für das Risikomanagement des Konzerns einfließen.

Datenschutz-Folgenabschätzungen (DPIA)

Die ayondo Gruppe führt eine DPIA durch, bei der die Datenverarbeitung wahrscheinlich zu einem hohen Risiko für Einzelpersonen führt, zum Beispiel:

(a) bei der Implementierung einer neuen Technologie;
(b) wenn eine Profiling-Operation Personen wahrscheinlich erheblich beeinträchtigt; und / oder
(c) wenn es große Mengen von speziellen Datenkategorien gibt.

Bei der Beurteilung des Risikoniveaus berücksichtigt die Gruppe sowohl die Wahrscheinlichkeit, als auch die Schwere der Auswirkungen auf die betroffenen Personen.

Die ayondo Gruppe stellt sicher, dass die DPIA bei bestimmten Mitgliedern des Unternehmens gut verstanden wird.

(a) Die ayondo Gruppe bietet Schulungen an, so dass alle Mitarbeiter die Notwendigkeit verstehen, eine DPIA in den frühen Phasen eines jeden Plans mit personenbezogenen Daten zu berücksichtigen.
(b) Die bestehenden Richtlinien, Prozesse und Verfahren der ayondo Gruppe enthalten gegebenenfalls Verweise auf die DPIA-Anforderungen.
(c) Die ayondo Gruppe versteht die Verarbeitungsarten, die eine DPIA erfordern.
(d) Die ayondo Gruppe erstellt und dokumentiert einen robusten DPIA-Prozess; und
(e) Die ayondo Gruppe bietet Schulungen für relevante Mitarbeiter zur Durchführung einer DPIA.

Meldung von Verstößen

Im Falle einer Verletzung des Schutzes personenbezogener Daten teilt die Gruppe dies der zuständigen Aufsichtsbehörde unverzüglich und spätestens nach 72 Stunden nach Kenntniserlangung des Verstoßes, sofern dies praktikabel ist, mit. Dies ist nicht erforderlich, wenn die Verletzung keine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. Wenn die Benachrichtigung nicht innerhalb von 72 Stunden erfolgt, muss die ayondo Gruppe einen begründeten Grund für die Verzögerung angeben. Die Kontaktdaten der zuständigen Aufsichtsbehörden finden Sie in Anhang 1.

Benachrichtigungen der ayondo Gruppe müssen mindestens

(e) die Art der Verletzung des Schutzes personenbezogener Daten beschreiben;
(f) den Namen und die Kontaktdaten der zuständigen Abteilung, die die Datenverletzung behandelt, kommunizieren;
(g) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten beschreiben; und
(h) die Maßnahme beschreiben, die die Gruppe ayondo ergriffen oder vorgeschlagen hat, um die Verletzung des Schutzes personenbezogener Daten zu beheben, gegebenenfalls einschließlich Maßnahmen zur Abschwächung möglicher nachteiliger Auswirkungen.

Wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten von Subjekten führt, übermittelt die Gruppe die Datenverletzung unverzüglich der betroffenen Person.

Die ayondo Gruppe teilt der betroffenen Person in klarer und verständlicher Sprache die Art der Verletzung des Schutzes personenbezogener Daten mit, wobei mindestens die unter den Buchstaben b), c) und d) genannten Informationen zu nennen sind.

Aufzeichnungen

Die ayondo Gruppe beschäftigt weniger als 250 Personen und daher ist Artikel 30 DSGVO technisch nicht anwendbar. Aufgrund der anderen Datenüberwachungsanforderungen, die von der DSGVO und für bewährte Verfahren vorgeschrieben sind, muss die Gruppe jedoch Aufzeichnungen über die ihrer Verantwortung unterstehenden Verarbeitungstätigkeiten führen. Diese Aufzeichnung enthält folgende Informationen:

(a) Name und die Kontaktdaten des Verantwortlichen;
(b) Zwecke der Verarbeitung;
(c) Beschreibung der Kategorien der betroffenen Personen und der Kategorien personenbezogener Daten;
(d) Empfänger, an die die personenbezogenen Daten weitergegeben wurden oder werden, einschließlich der Empfänger in dritten Ländern oder internationalen Organisationen;
(e) Gegebenenfalls Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, einschließlich der Identifizierung dieses Drittlandes oder dieser internationalen Organisation;
(f) Soweit möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien; und
(g) Soweit möglich, eine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Die ayondo Gruppe führt die Aufzeichnungen schriftlich und in elektronischer Form.

Auf Antrag der zuständigen Aufsichtsbehörde stellt die Gruppe unverzüglich Aufzeichnungen zur Verfügung.

Umgang mit Beschwerden

Nach Eingang einer Beschwerde bei der betroffenen Person muss die Gruppe die Beschwerde intern untersuchen. Die ayondo Gruppe informiert die betroffene Person über den Fortschritt und anschließend über das Ergebnis der Beschwerde. Dies muss innerhalb einer angemessenen Frist mitgeteilt werden.

Wenn die Beschwerde nicht zwischen der betroffenen Person und der Gruppe gelöst werden kann, kann die betroffene Person beschließen, Wiedergutmachung durch Schlichtung, ein Gerichtsverfahren oder eine Beschwerde bei der Aufsichtsbehörde zu beantragen. Die ayondo Gruppe muss die betroffenen Personen über ihr Recht auf direkte Beschwerde an die zuständige Aufsichtsbehörde informieren.

Anhang 1

Personenbezogene Daten	Alle Informationen (einschließlich Meinungen und Absichten), die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
Datenverantwortlicher	Eine natürliche oder juristische Person, Behörde, Agentur oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt
Datensubjekt	Die identifizierte oder identifizierbare natürliche Person, auf die sich die Daten beziehen
Zustimmung	Jede frei gegebene, spezifische, informierte und unzweideutige Angabe der Wünsche der betroffenen Person, durch die er oder sie durch eine Erklärung oder eine eindeutige zustimmende Handlung die Zustimmung zur Verarbeitung der ihn / sie betreffenden personenbezogenen Daten erklärt
Internationale Organisation	Eine Organisation und ihre nachgeordneten Körperschaften, die dem Völkerrecht unterstehen, oder jede andere Einrichtung, die auf der Grundlage einer Vereinbarung zwischen zwei oder mehr Ländern gegründet wurde oder auf dieser Grundlage errichtet wurde.
Aufsichtsbehörde	Datenschutzaufsichtsbehörde für ayondo markets Limited: Information Commissioner's Office Wycliff House Water Lane Wilmslow Cheshire SK9 5AF Tel .: +44 (0) 303 123 1113 Fax: +44 (0) 1625 524 510 Website: www.ico.org.uk

Anhang 2

Checkliste Überwachungsdaten

Einzelheiten zu den Daten derayondo Gruppe	
Grund für die Aufbewahrung der Daten	
Methoden zum Erhalt der Daten	
Datum, an dem die Daten erhalten wurden	
Personen, die für die Daten verantwortlich sind	
Datenspeicherung	
Vorratsdatenspeicherung	
Datenlöschungsmethode	

AGV-beleid gegevensbescherming

Belangrijke informatie

Conform art. 24 GDPR (EU) 2016/679, rekening houdend met de aard, reikwijdte, context en doeleinden van verwerking alsmede met de risico's voor de rechten en vrijheden van natuurlijke personen heeft BUX de juiste technische en organisatorische maatregelen geïmplementeerd om de naleving van de Algemene Verordening Gegevensbescherming (Engels: *General Data Protection Regulation*, afgekort *GDPR*) te borgen en na te streven. Dit beleid vormt de hoeksteen van de naleving van de AGV door BUX, en wordt herzien en overeenkomstig geactualiseerd.

De Algemene Verordening Gegevensbescherming (AVG) [Engels: General Data Protection Regulation, afgekort GDPR]

De Algemene Verordening Gegevensbescherming van de EU vervangt de databeschermingsrichtlijn 95/46/EC en is bedoeld om de wetten op het gebied van gegevensbescherming in heel Europa te harmoniseren, de privacygegevens van alle EU-burgers te beschermen en te verbeteren en de manier waarop organisaties in dat hele gebied omgaan met privacygegevens opnieuw vorm te geven.

Conform art. 5 AVG moet BUX te allen tijde conform de volgende principes handelen.

1. rechtmatigheid, redelijkheid en transparantie	persoonsgegevens zullen rechtmatig, redelijk en op een transparante manier worden verwerkt in verhouding tot de betrokkene.
2. beperking van de doeleinden	persoonsgegevens zullen worden verzameld voor specifieke, expliciete en gerechtvaardigde doeleinden en verder niet worden verwerkt op een manier die niet strookt met die doeleinden.
3. gegevensminimalisering	persoonsgegevens zullen adequaat en relevant zijn, en beperkt tot wat noodzakelijk is in verhouding tot de doeleinden waarvoor ze worden verwerkt.
4. juistheid	persoonsgegevens zullen juist zijn en indien nodig worden geactualiseerd.
5. opslagbeperking	persoonsgegevens zullen in een vorm worden gehouden die het identificeren van gegevenssubjecten niet langer toestaat dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.
6. integriteit en vertrouwelijkheid	persoonsgegevens zullen zodanig worden verwerkt dat de adequate veiligheid van de persoonsgegevens verzekerd is, met inbegrip van bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen toevallig verlies, vernietiging of schade, waarbij de juiste technische en organisatorische maatregelen worden genomen.
7. verantwoording	de beheerder zal verantwoordelijk zijn voor de naleving van de AVG en in staat zijn om die naleving aan te tonen.

BUX is te allen tijde verantwoordelijk voor de naleving met de bovengenoemde principes en kan dat ook aantonen.

Iedere verwijzing naar 'ons', 'onze', 'wij' of 'BUX' is een referentie naar elk bedrijf van de groep binnen de ayondo Groep, al naar gelang de context, tenzij anders aangegeven.

Toepasbaarheid

Dit privacybeleid heeft betrekking op de verwerkingsactiviteiten van de ayondo Groep. De drie belangrijkste handelsenteiten binnen de ayondo Groep zijn:

- ✓ *ayondo markets Limited*: een in Engeland en Wales geregistreerd bedrijf met het registratienummer 03148972. Het geregistreerde adres van het bedrijf is: 1st Floor, 7-10 Chandos Street, London, W1G 9DQ Verenigd Koninkrijk. Het bedrijf is bij de *UK Information Commissioner* geregistreerd met het registratienummer is Z1457804.
- ✓ *ayondo portfolio management GmbH*: een in Duitsland geregistreerd bedrijf, Handelsregister Amtsgericht Frankfurt am Main, registratienummer HRB 102933. Het geregistreerde adres van het bedrijf is Niddastraße 91, D-60329 Frankfurt am Main, Duitsland.
- ✓ *ayondo GmbH*: een in Duitsland geregistreerd bedrijf, Handelsregister Amtsgericht Frankfurt am Main, registratienummer 84169. Het geregistreerde adres van het bedrijf is Niddastraße 91, D-60329 Frankfurt am Main, Duitsland.

ayondo Group zorgt alleen voor uitvoering en maatschappelijke handelsdiensten aan detailhandel en professionele cliënten in verband met producten in het kader van weddenschappen (*Spread Betting*, SB en *Contract for Difference*, CFD), en wel via zijn dochterondernemingen *ayondo markets Limited*, Londen resp. *ayondo portfolio management GmbH*, Frankfurt. *ayondo GmbH* is een verbonden agent van *ayondo markets Limited*. De hierboven genoemde groepseenheden zijn aparte beheerders van persoonsgegevens in verband met de diensten die elk van deze bedrijven zelf verleent.

Het monitoren van de naleving

Om een hoog niveau van naleving te bereiken in het kader van dit beleid vastgelegde regels voert BUX een jaarlijkse audit naleving van gegevensbescherming uit. Het uitvoeren van een grondige diagnostische audit stelt BUX in staat om alle tekortkomingen resp. punten van verbetering te herkennen; bij verbetering wordt de algehele naleving van de AVG geborgd. Voorbeelden van de punten die in het kader van zo'n audit worden bekeken omvatten:

(a) het beheer van de gegevensbescherming en de structuren, beleidslijnen en procedures om naleving van de AVG te borgen;
(b) de processen voor het managen van zowel elektronische en als handgeschreven registraties die persoonsgegevens bevatten;
(c) de processen in verband met het reageren op elk verzoek om persoonsgegevens;
(d) de technische en organisatorische maatregelen die ter beschikking staan om er zeker van te zijn dat er sprake is van adequate veiligheid in verband met persoonsgegevens;
(e) het aanbieden en monitoren van trainingen gegevensbescherming voor de staf met inbegrip van het bewustzijn in verband met gegevensbescherming; en
(f) auditgegevens zoals in bijlage 2.

De rechten en verzoeken van een betrokkene

De AVG geeft de volgende rechten voor individuele personen:

1. het recht om te worden geïnformeerd;
2. het recht op inzage;
3. het recht op rectificatie;
4. het recht op verwijdering;
5. het recht om verwerking te beperken;
6. het recht op dataportabiliteit;
7. het recht om bezwaar te maken; en
8. rechten in verband met geautomatiseerde besluitvorming en profilering.

BUX beschikt over adequate systemen en controles om het toepassen van de acht hierboven genoemde rechten van een betrokkene mogelijk te maken en te faciliteren.

Als een betrokkene een verzoek indient zal BUX een pragmatische besluitvormingsproces opstarten onder leiding van de functionaris gegevensbescherming.

Tenzij BUX van mening is dat een verzoek gezien de aard daarvan excessief of onnodig is, zullen er in verband met het in behandeling nemen van en/of het meewerken met zulke verzoeken geen kosten aan verbonden zijn voor de betrokkene

Recht op informatie/inzage

Al dit soort verzoeken moeten worden verwezen naar de functionaris gegevensbescherming. BUX zal binnen 30 dagen op zo'n verzoek reageren.

Het betrokkene heeft het recht om de volgende informatie van BUX te krijgen:

(a) de doeleinden van de verwerking;
(b) de categorieën van desbetreffende persoonsgegevens;
(c) de ontvangers van categorieën van persoonsgegevens die van de betrokkene zijn opgeslagen;
(d) de vermoedelijke periode waarin de persoonsgegevens opgeslagen zullen worden, of, als dat niet mogelijk is, de criteria die tot het vastleggen van die periode hebben geleid; en
(e) het gebruik van iedere vorm van geautomatiseerde besluitvorming resp. profilering.

Als daarom wordt verzocht zal BUX een kopie van de opgeslagen persoonsgegevens doen toekomen. Voor alle bijkomende kopieën die de betrokkene aanvraagt kan BUX een redelijke kostenbijdrage vragen, die gebaseerd is op de administratieve kosten. Als verzoeken via elektronische middelen worden ingediend zal BUX de gegevens in een algemeen gebruikelijke elektronische vorm aanleveren.

Recht op rectificatie/correctie

BUX zal ervoor zorgen dat alle gegevenssubjecten in staat zijn om hun recht van het bedrijf uit te oefenen, en wel zonder onnodige vertraging, de rectificatie van onjuiste persoonsgegevens die hem of haar betreffen.

Recht op verwijdering

Zonder onnodige vertraging zal BUX persoonsgegevens of een betrokkene verwijderen als daarom gevraagd wordt en een van de volgende redenen van toepassing is:

(a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor ze zijn verzameld of op andere wijze zijn verwerkt;
(b) de betrokkene trekt de toestemming waarop de verwerking is gebaseerd in, en er is geen andere wettelijke reden is voor het verwerken;
(c) de betrokkene maakt bezwaar tegen de verwerking en er is geen sprake van prevalerende gerechtvaardigde belangen voor het verwerken, of de betrokkene maakt bezwaar tegen de verwerking;
(d) de persoonsgegevens zijn onrechtmatig verwerkt;
(e) de persoonsgegevens moeten worden verwijderd conform een wettelijke verplichting in de wet van de lidstaat; en/of
(f) de persoonsgegevens zijn verzameld in samenhang met het aanbod van dienstverlening van de informatiemaatschappij services.

Art. 17 3 (b) AVG houdt in dat het recht om te verwijderen niet van toepassing is als het bedrijf gegevens moet bewaren om aan andere toe te passen voorschriften te voldoen. De prevalerende voorschriften zijn in het geval van BUX de Engelse wet in verband met witwassen (*The Money Laundering Regulations*), de bepaling voor bedrijven om klantgegevens (*Know Your Customer- KYC*) 5 jaar te bewaren, en Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten ... (Engels: *Markets in Financial Instruments Directive*. afgekort MiFID II) art. 16 opgenomen vereisten ten aanzien van het bijhouden van registraties. Hier wordt naar verwezen in de privacyverklaring van BUX.

Recht om de verwerking te beperken

BUX zal de verwerking of persoonsgegevens stopzetten onder de volgende omstandigheden:

(a) als een individuele persoon de juistheid van de persoonsgegevens betwist zal BUX de verwerking beperken tot de juistheid van de gegevens is geverifieerd;
(b) als een individuele persoon bezwaar heeft gemaakt tegen het verwerken en de Groep overweegt of er gerechtvaardigde belangen zijn om die boven die van de individuele persoon te laten prevaleren;
(c) als de verwerking kennelijk onrechtmatig is en de individuele persoon bezwaar maakt tegen verwijdering en in plaats daarvan een beperking verlangt; en/of
(d) als de Groep de gegevens niet langer nodig heeft maar de individuele persoon verlangt de gegevens voor de vaststelling, uitoefening of onderbouwing van een rechtsvordering.

Recht op dataportabiliteit

Het recht op dataportabiliteit is alleen van toepassing:

(a) bij persoonsgegevens die een individuele persoon aan een beheerder heeft verstrekt;
(b) als de verwerking berust op de toestemming van de individuele persoon of voor het uitvoeren van een contract; en
(c) als de verwerking wordt uitgevoerd met behulp van geautomatiseerde middelen.

Om aan de eisen te voldoen moet BUX:

(a) de persoonsgegevens in een gestructureerd, gangbaar en machineleesbaar formaat verstrekken;
(b) de gegevens kosteloos verstrekken (tenzij excessief of onnodig);
(c) de gegevens - indien verlangd en technisch haalbaar - direct aan een andere organisatie doorgeven; en
(d) overwegen mogelijke prejudice of de rechten van individuele personen als de persoonsgegevens meer dan een individuele persoon betreffen.

Toestemming

Toestemming moet worden gegeven door een ondubbelzinnige actieve handeling waarmee de vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting van de betrokkene toestemt in de verwerking van hun gegevens. BUX zal die toestemming verkrijgen via een geschreven verklaring, door elektronische middelen, of een mondelinge verklaring.

BUX verzoekt om toestemming, beheert en registreert die conform art. 5, 6, 7 en 9 GDPR.

(a) BUX beziet of de toestemming de meest geschikte wettelijke grondslag voor verwerking is;
(b) BUX probeert om de toestemming prominent te presenteren, gescheiden van zijn algemene voorwaarden;
(c) BUX verlangt een positieve opt-in;
(d) BUX maakt geen gebruik van al aangevinkte vakjes of enig andere vorm van default toestemming;
(e) BUX gebruikt heldere en duidelijke taal die gemakkelijk te begrijpen is;
(f) BUX specificeert waarom de gegevens nodig zijn en wat het doel daarvan is;
(g) BUX zorgt voor nauwkeurig geformuleerde opties voor aparte toestemming voor verschillende doelstellingen en soorten verwerking;
(h) BUX benoemt de beheerders van de eigen organisatie en die van derde partijen die op toestemming kunnen vertrouwen;
(i) BUX zorgt ervoor dat individuele personen hun toestemming kunnen weigeren zonder daarvan nadeel te ondervinden; en
(j) BUX vermijdt het om toestemming een voorwaarde voor dienstverlening te maken.

BUX registreert wanneer en hoe het bedrijf toestemming van individuele personen heeft verkregen. Het bedrijf houdt ook een registratie bij van de exact informatie die oorspronkelijk is verstrekt.

Strategieën waarvan BUX gebruik kan maken om te zorgen voor het juiste management van de toestemming, met inbegrip van de volgende punten:

(a) BUX bekijkt de toestemming regelmatig om vast te stellen of de relatie, de verwerking en de doeleinden niet zijn veranderd;
(b) BUX beschikt over processen om de toestemming in geschikte intervallen te hernieuwen, met inbegrip van elke vorm toestemming van de ouders (indien van toepassing);

(c) BUX overweegt het gebruik van *privacy dashboards*[1] of andere beleidsinstrumenten waar men de voorkeur aan geeft als een zaak van *good practice*;
(d) BUX maakt het makkelijk voor individuele personen om hun toestemming te allen tijde in te trekken, en maakt bekend hoe dat kan worden gedaan;
(e) BUX reageert bij het intrekken van toestemming zo snel mogelijk; en
(f) BUX bestraft geen individuele personen die hu toestemming in willen trekken.

BUX zal geen toestemming afleiden uit stilte of inactiviteit. Als de verwerking van persoonsgegevens meerdere doeleinden heeft zal BUX toestemming vragen voor al die doeleinden. Als de toestemming van een betrokkene gegeven moet worden na een verzoek via elektronische middelen zal BUX ervoor zorgen dat het verzoek duidelijk is, beknopt en niet onnodig ontwrichtend met het oog op het gebruik van de diensten waarvoor de toestemming is bedoeld.

Gegevensprivacy by Design

BUX heeft de beschikking over technische en organisatorische maatregelen die gegevens-bescherming in verwerkingactiviteiten integreren.

Privacy en gegevensbescherming zijn belangrijke overwegingen in de vroege fases van elk project dat BUX opstart.

Bijvoorbeeld bij het:

(a) opzetten van nieuwe IT systemen voor het opslaan of toegang verkrijgen van persoonsgegevens;
(b) het ontwikkelen van wetgeving, beleid of strategieën die gevolgen hebben voor de privacy;
(c) starten van een initiatief om gegevens te delen; en/of
(d) gebruiken van gegevens voor nieuwe doeleinden.

Overwegingen ten aanzien van privacy en gegevensbescherming zullen in het risicomanagement methodologieën en beleidsrichtlijnen van BUX worden geïntegreerd.

Privacy effectbeoordelingen (*Data Protection Impact Assessments*, afgekort DPIA)

BUX voert een DPIA uit als de verwerking van gegevens vermoedelijk zal leiden tot een groot risico voor individuele personen, bijvoorbeeld:

(a) als een nieuwe technologie wordt geïmplementeerd;
(b) als een profileringsoperatie individuele personen vermoedelijk significant zal beïnvloeden; en/of
(c) als er een grootschalige verwerking van speciale categorieën van gegevens plaatsvindt.

Door het niveau van het risico in te schatten, BUX schat zowel de waarschijnlijkheid als ernst in van enige gevolgen voor de betrokken individuele personen.

[1]een informatief *privacy dashboard* kan verzamelde samenvattingen van de verzamelde of verwerkte persoonsgegevens voor een bepaalde gebruiker geven, *opm.vertaler*

BUX zorgt ervoor dat er sprake is van een gedegen begrip omtrent DPIA onder bepaalde leden van het bedrijf.

(a) BUX zorgt voor training zodat de hele staf de noodzaak begrijpt om aan een DPIA te denken in de vroege fases van elk plan dat persoonsgegevens betreft;
(b) het bestaande beleid en de processen en procedures van BUX, met inbegrip van verwijzingen naar vereisten in het kader van DPIA, indien toe te passen;
(c) BUX heeft inzicht in het soort verwerking dat een DPIA vereist;
(d) BUX zorgt voor een robuust DPIA proces en documenteert dat; en
(e) BUX zorgt voor training voor relevante staf over het thema hoe je een DPIA uitvoert.

Het melden van inbreuk

In geval van een inbreuk op persoonsgegevens zal BUX zonder onnodige vertraging en indien uitvoerbaar de relevante toezichthouder informeren, en wel niet later dan 72 uur na het constateren van de inbreuk. Dat is niet vereist als de inbreuk waarschijnlijk niet zal leiden tot een risico voor de rechten en vrijheden van natuurlijke personen. Als de melding niet binnen 72 uur is gedaan moet BUX een geldige reden voor de vertraging geven. De contactgegevens van de relevante toezichthouders vindt u in bijlage 1.

De door BUX gemaakte melding moet tenminste:

(a) de aard van de inbreuk op de persoonsgegevens beschrijven;
(b) de naam en de contactgegevens van de relevante afdeling noemen die de inbreuk op de gegevens afhandelt;
(c) de vermoedelijke consequentie van de inbreuk op de persoonsgegevens beschrijven; en
(d) de door BUX genomen of voorgestelde maatregel om de inbreuk op de persoonsgegevens aan te pakken, met inbegrip van, waar nodig, maatregelen om de mogelijke ongunstige effecten daarvan te verminderen.

Als de inbreuk op persoonsgegevens vermoedelijk zal resulteren in een groot risico voor de rechten en vrijheden van subjecten zal BUX de inbreuk op gegevens aan de betrokkene melden zonder onnodige vertraging.

BUX zal dit melden aan de betrokkene, en wel in duidelijke en eenvoudige taal, met informatie over de aard van de inbreuk op persoonsgegevens, waarbij in elk geval de informatie onder de hierboven genoemde punten (b), (c) en (d) gedetailleerd wordt meegedeeld.

Het bijhouden van de registratie

BUX heeft minder dan 250 werknemers in dienst, daarom is art. 30 AVG technisch gesproken niet van toepassing. Dat vooropgesteld, zal BUX - gezien de andere vereisten op het gebied van het monitoren van gegevens die worden opgelegd door de AVG en in het kader van *best practices* - een registratie van verwerkingsactiviteiten bijhouden die onder zijn verantwoordelijkheid vallen. Dat record zal de volgende informatie bevatten:

(a) de naam en contactgegevens van de beheerder;
(b) de doeleinden van het verwerken;
(c) een beschrijving van de categorieën van betrokkenen en de categorieën van persoonsgegevens;
(d) de ontvangers aan wie de persoonsgegevens bekend zijn gemaakt resp. bekend gemaakt zullen worden met inbegrip van ontvangers in derde landen van internationale organisaties;
(e) indien van toepassing, transfers van persoonsgegevens naar een derde land of een internationale organisatie, met inbegrip van de identificatie van dat derde land of die internationale organisatie;
(f) indien mogelijk, de voorziene tijdlimieten voor het wissen van de verschillende categorieën van gegevens; en
(g) indien mogelijk, een beschrijving van de technische en organisatorische maatregelen waarnaar in art. 32(1) wordt verwezen.

BUX zorgt voor een registratie in schriftelijke vorm en in een elektronisch formaat.

Indien de relevante toezichthouder daarom verzoekt zal BUX de registratie direct ter beschikking stellen.

Afhandeling van klachten

Bij ontvangst van een klacht van een betrokkene zal BUX de klacht intern onderzoeken. BUX zal de betrokkene informeren over de voortgang en vervolgens het eindresultaat van de klacht. Dat moet binnen een redelijke periode worden meegedeeld.

Als de klacht tussen de betrokkene en BUX niet kan worden opgelost kan de betrokkene ervoor kiezen om verhaal te zoeken door middel van mediatie, een rechtsgeding of het indienen van een klacht bij de toezichthouder. BUX moet de betrokkenen informeren over hun recht om direct een klacht in te dienen bij de relevante toezichthouder.

Bijlage 1

persoonsgegevens	Alle informatie (met inbegrip van opinies en intenties) die verband houdt met een geïdentificeerde of identificeerbare natuurlijke persoon
gegevensbeheerder	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat alleen of samen met anderen, de doeleinden en middelen met betrekking tot de verwerking van persoonsgegevens vastlegt.
betrokkene	De geïdentificeerde of identificeerbare natuurlijke persoon naar wie de gegevens verwijzen
toestemming	elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting van de betrokkene, waardoor hij of zij door middel van een verklaring of een ondubbelzinnige actieve handeling toestemming geeft voor het verwerken van persoonsgegevens die met hem of haar verband houden.
internationale organisatie	een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.
toezichthouder	De toezichthouder gegevensbescherming voor BUX: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Verenigd Koninkrijk Tel: +44 (0)303 123 1113 Fax: +44 (0)1625 524 510 Website: www.ico.org.uk

Bijlage 2

Checklist Monitoring gegevens

Details van de gegevens die door de *ayondo Groep* zijn opgeslagen	
Reden om de gegevens op te slaan	
Manieren om de gegevens te verkrijgen	
Datum waarop de gegevens zijn verkregen	
Individuele personen die verantwoordelijk zijn voor de gegevens	
Gegevensopslag	
Dataretentie	
Methodologie van het verwijderen van gegevens	

Politica sulla protezione dei dati RGPD

Informazioni importanti

In linea con l'Articolo 24 del RGPD (UE) 2016/679, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, BUX mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento è effettuato conformemente al Regolamento generale sulla protezione dei dati (RGPD). Questa politica è la pietra d'angolo dell'adempimento al RGPD da parte di BUX ed è analizzata e aggiornata di conseguenza.

Regolamento generale sulla protezione dei dati (RGPD)

Il Regolamento generale sulla protezione dei dati (RGPD) UE sostituisce la Direttiva sulla protezione dei dati 95/46/CE e intende armonizzare le leggi sulla riservatezza sui dati in tutta Europa, per proteggere e potenziare la riservatezza dei dati di tutti i cittadini UE e per riformare il modo in cui le aziende della regione gestiscono la riservatezza dei dati.

In linea con l'Articolo 5 del RGPD, BUX deve sempre conformarsi ai seguenti principi.

1. Liceità, correttezza e trasparenza	I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
2. Limitazioni della finalità	I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
3. Minimizzazione dai dati	I dati personali sono adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento.
4. Accuratezza	I dati personali sono accurati e, se necessario, tenuti aggiornati.
5. Limitazioni alla conservazione	I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
6. Integrità e riservatezza	I dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
7. Responsabilizzazione	Il titolare del trattamento è competente per il rispetto del RGPD e in grado di comprovarlo.

BUX deve dimostrare in qualsiasi momento di essere conforme a suddetti principi, per i quali è in ogni momento responsabile.

Qualsiasi riferimento a 'Noi', 'Nostro/i', 'Ci' o 'BUX' è un riferimento a ogni società del Gruppo ayondo, come richiesto dal contesto, salvo altrimenti espresso.

Applicabilità

Questa politica sulla riservatezza si applica alle attività di trattamento di ayondo Group. Le tre principali entità commerciali all'interno del Gruppo ayondo sono:

- ✓ ayondo markets Limited: società registrata in Inghilterra e Galles al numero di registrazione 03148972. La sede legale della società è 1st Floor, 7-10 Chandos Street, Londra, W1G 9DQ Regno Unito. È registrata presso l'Information Commissioner (Commissario delle informazioni) del Regno Unito al numero di registrazione Z1457804.
- ✓ ayondo portfolio management GmbH: società registrata in Germania, registro commerciale del Tribunale distrettuale di Francoforte sul Meno HRB 102933. La sede legale della società è Niddastraße 91, 60329 Francoforte sul Meno, Germania.
- ✓ ayondo GmbH: società registrata in Germania, registro commerciale del Tribunale distrettuale di Francoforte sul Meno 84169. La sede legale della società è Niddastraße 91, 60329 Francoforte sul Meno, Germania.

ayondo Group fornisce servizi "solo esecuzione" e di "social trading" a clienti al dettaglio e professionali per prodotti Spread Betting ('SB') e Contract for Difference ('CFD') attraverso le proprie consociate, rispettivamente ayondo markets Limited, Londra e ayondo portfolio management GmbH, Frankfurt. ayondo GmbH è un agente collegato di ayondo markets Limited. Le suddette entità del gruppo sono titolari individuali del trattamento di dati personali rispetto ai servizi forniti individualmente dalle stesse.

Monitoraggio dell'adempimento

Per mantenere un alto livello di adempimento rispetto alle regole stipulate all'interno di questa politica, BUX svolge una revisione dell'adempimento annuale sulla Protezione dei dati. Conducendo una revisione diagnostica accurata, BUX può riconoscere eventuali deficienze o settori da migliorare; dopo operazioni di mitigazione, può assicurare un adempimento totale al RGPD. Esempi dei settori oggetto di revisione comprendono:

(a) Governance della protezione dei dati e strutture, politiche e procedure per assicurare l'adempimento del RGPD;
(b) Le procedure per la gestione di registri elettronici e manuali contenenti dati personali;
(c) Le procedure che rispondono a richieste di dati personali;
(d) Le misure tecniche e organizzative predisposte per assicurare che vi sia una sicurezza adeguata dei dati personali;
(e) La fornitura e monitoraggio della formazione del personale e la consapevolezza della protezione dei dati; e
(f) Revisione dei dati come da Appendice 2.

Diritti degli interessati e richieste

Il RGPD fornisce i seguenti diritti alle persone fisiche:

1. Il diritto di essere informati;
2. Il diritto di accesso;
3. Il diritto alla rettifica;
4. Il diritto alla cancellazione;
5. Il diritto a limitare il trattamento;
6. Il diritto alla portabilità dei dati;
7. Il diritto di opposizione; e
8. Diritti in merito al processo decisionale automatizzato e alla profilazione.

BUX ha predisposto sistemi e controlli adeguati per permettere e facilitare l'applicazione degli otto diritti degli interessati sopra elencati.

Quando un soggetto interessato fa una richiesta, BUX avvierà un processo decisionale pragmatico, guidato dal Responsabile della protezione dei dati.

Salvo BUX ritenga eccessiva e non necessaria la natura delle richieste, nessun onere sarà addebitato agli interessati per la valutazione e/o l'adempimento di dette richieste.

Diritto di accesso

Tutte le richieste di questa natura vanno rimesse al Responsabile della protezione dei dati. BUX risponderà a dette richieste entro 30 giorni.

L'interessato ha il diritto di ottenere le seguenti informazioni da BUX:

(a) Le finalità del trattamento;
(b) Le categorie dei dati personali in questione;
(c) I destinatari o le categorie di dati personali conservati per l'interessato;
(d) Il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e
(e) L'uso di un processo decisionale automatizzato, per esempio, la profilazione.

Su richiesta, BUX fornirà una copia dei dati personali conservati. Per ogni altra copia richiesta dagli interessati, BUY può addebitare un onere ragionevole basato su spese amministrative. Se le richieste avvengono con mezzi elettronici, BUX fornisce i dati in una forma elettronica comunemente utilizzata.

Diritto alla rettifica

BUX assicura che tutti gli interessati siano in grado di esercitare il proprio diritto a ottenere dall'azienda, senza indebito ritardo, la rettifica dei dati personali inaccurati che lo riguardano.

Diritto alla cancellazione

Senza indebiti ritardi, BUX cancella i dati personali di un interessato su richiesta e se si applica uno dei seguenti motivi:

(a) I dati personali non sono più necessari in relazione alle finalità per le quali sono stati raccolti o altrimenti trattati;

(b) L'interessato ritira il consenso sul quale è basato il trattamento, e se non vi è altra base legale per il trattamento;
(c) L'interessato si oppone al trattamento e non vi sono basi legittime prevalenti per il trattamento, o se l'interessato si oppone al trattamento;
(d) I dati personali sono stati trattati illegalmente;
(e) I dati personali devono essere cancellati in forza di un obbligo di legge dello Stato membro; e/o
(f) I dati personali sono stati raccolti in relazione all'offerta di servizi della società dell'informazione.

L'articolo 17 3 (b) del RGPD recita che il diritto alla cancellazione non si applica se l'azienda deve conservare dati per adempiere ad altre regole applicabili. I regolamenti prevalenti nel caso di BUX sono i requisiti del Regolamento sul riciclaggio di denaro, secondo i quali le aziende devono conservare i dati KYC (Know your customers, Conosci i tuoi clienti) per 5 anni, e i requisiti dell'Articolo 16 del MiFID II sulla conservazione di registri. Ne si parla nell'avviso sulla riservatezza di BUX.

Diritto alla limitazione del trattamento

BUX cesserà il trattamento dei dati personali nelle seguenti circostanze:

(a) Se una persona fisica contesta l'accuratezza dei dati personali, BUX limiterà il trattamento fino alla verifica dell'accuratezza dei dati;
(b) Se una persona fisica si è opposta al trattamento e il Gruppo sta valutando se ha basi legali legittime che prevalgono su quelli della persona fisica;
(c) Quando si riscontra che il trattamento è illegale e la persona fisica si oppone alla cancellazione e richiede invece una limitazione; e/o
(d) Se il Gruppo non necessita più dei dati, ma la persona fisica richiede i dati per proporre, esercitare o difendere una pretesa legale.

Diritto alla portabilità dei dati

Il diritto alla portabilità si applica solo:

(a) Ai dati personali che una persona fisica ha fornito a un titolare del trattamento;
(b) Se il trattamento è basato sul consenso della persona fisica o per l'esecuzione di un contratto; e
(c) Quando il trattamento è svolto da mezzi automatizzati.

Per adempiere, BUX deve:

(a) Fornire i dati personali in un formato strutturato, comunemente utilizzato e leggibile con una macchina;
(b) Fornire i dati gratuitamente (salvo sia eccessivo o non necessario);
(c) Se richiesto e tecnicamente fattibile, trasmettere i dati direttamente a un'altra azienda; e
(d) Considerare il possibile pregiudizio dei diritti delle persone fisiche, se i dati personali riguardano più di una persona fisica.

Consenso

Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano. BUX otterrà un consenso attraverso una dichiarazione scritta, con mezzi elettronici o una dichiarazione orale.

BUX richiede, gestisce e registra il consenso secondo gli Articoli 5, 6, 7 e 9 del RGPD.

(a) BUX verifica che il consenso sia la base legale più appropriata per il trattamento;
(b) BUX fa la richiesta di consenso in modo prominente e separato dalle proprie condizioni generali;
(c) BUX richiede un "opt in" positivo;
(d) BUX non utilizza caselle pre-selezionate o ogni altro tipo di consenso predefinito;
(e) BUX usa un linguaggio chiaro, semplice, facile da comprendere;
(f) BUX specifica perché vuole i dati e la loro finalità;
(g) BUX fornisce opzioni granulari per acconsentire separatamente a finalità e tipi di trattamento diversi;
(h) BUX nomina la propria azienda e i titolari di dati terzi, che si baseranno sul consenso;
(i) BUX assicura che le persone fisiche possono rifiutare il consenso senza subire pregiudizio; e
(j) BUX evita di fare del consenso una precondizione di servizio.

BUX registra quando e come l'azienda ha ottenuto un consenso dalle persone fisiche. L'azienda tiene anche un registro delle informazioni esatte originariamente fornite.

Le operazioni che BUX può svolgere per assicurare la gestione appropriata del consenso includono quanto segue:

(a) BUX analizza regolarmente i consensi per verificare che la relazione, il trattamento e le finalità non sono cambiati;
(b) BUX ha predisposto procedure per riconfermare il consenso a intervalli appropriati, inclusi i consensi genitoriali (se applicabili);
(c) BUX considera l'utilizzo di strumentazione sulla riservatezza o altri strumenti di gestione delle preferenze come buona pratica;
(d) BUX rende semplice per le persone fisiche ritirare il proprio consenso in qualsiasi momento, e ne pubblicizza la procedura;
(e) BUX agisce sui ritiri del consenso non appena possibile; e
(f) BUX non penalizza le persone fisiche che intendono ritirare il proprio consenso.

BUX non deduce il consenso da silenzio o inattività. Quando il trattamento dei dati personali ha finalità multiple, BUX ottiene il consenso per tutti dette finalità. Quando il consenso di un interessato va dato a seguito di una richiesta effettuata elettronicamente, BUX fa in modo che la richiesta sia chiara, concisa e non disturbi più del necessario l'uso del servizio per il quale è fornita.

Riservatezza dei dati nella progettazione:

BUX ha approntato misure tecniche e organizzative che integrano la protezione dei dati nelle attività di trattamento.

La protezione della riservatezza e dei dati è un fattore chiave nelle prime fasi di qualsiasi progetto svolto da BUX

Per esempio, quando:

(a) Costruisce nuovi sistemi informatici per memorizzare o accedere ai dati personali;
(b) Sviluppa norme, politiche o strategie che hanno implicazioni per la riservatezza;
(c) Avvia iniziative di condivisione dei dati; e/o
(d) Usa dati per nuove finalità.

Considerazioni su riservatezza e protezione dei dati sono integrate nelle metodologie e nelle politiche di gestione del rischio di BUX.

Valutazioni d'impatto sulla protezione dei dati (VIPD)

BUX svolge una VIPD se è probabile che il trattamento dei dati comporti un forte rischio per le persone fisiche, per esempio:

(a) Se viene implementata una nuova tecnologia;
(b) Se è probabile che un'operazione di profilazione influenzi significativamente le persone fisiche; e/o
(c) Se vi è un trattamento di dati su larga scala di categorie particolari di dati.

Nella valutazione del livello di rischio, BUX considera tanto la probabilità, quanto la gravità di un impatto per le persone fisiche coinvolte.

BUX fa in modo che vi sia una buona comprensione della VIPD tra alcuni membri dell'azienda.

(a) BUX fornisce formazione, in modo che tutto il personale capisca la necessità di considerare una VIPD nelle prime fasi di qualsiasi piano che coinvolga dati personali;
(b) Politiche esistenti, processi e procedure di BUX comprendono riferimenti ai requisiti di VIPD, ove applicabile;
(c) BUX comprende i tipi di elaborazione che richiedono una VIPD;
(d) BUX crea e documenta un robusto processo VIPD; e
(e) BUX fornisce una formazione per il personale pertinente su come svolgere una VIPD.

Denuncia di una violazione

In caso di violazione dei dati personali, BUX notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo non più tardi di 72 ore dal momento in cui ne è venuto a conoscenza. Ciò non è necessario se è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, BUX deve corredarla dei motivi del ritardo. I dettagli di contatto dell'autorità di controllo pertinente sono nell'Appendice 1.

Le notifiche fatte da BUX devono almeno:

(a) descrivere la natura della violazione dei dati personali;
(b) comunicare il nome e i dati di contatto dell'ufficio pertinente che si occupa della violazione dei dati;
(c) descrivere le probabili conseguenze della violazione dei dati personali;
(d) descrivere le misure adottate o di cui si propone l'adozione da parte di BUX per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, BUC comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato da parte di BUX descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni di alle lettere b), c) e d).

Conservazione di registri

Il personale di BUX è inferiore alle 250 unità e quindi l'Articolo 30 del RGPD non è applicabile tecnicamente. Ciò detto, visti gli altri requisiti di monitoraggio dei dati previsti nel RGPD e per la best practice, BUX tiene un registro delle attività di trattamento svolte sotto la propria responsabilità. Il registro deve contenere le seguenti informazioni:

(a) il nome e i dati di contatto del titolare del trattamento;
(b) Le finalità del trattamento;
(c) Una descrizione delle categorie di interessati e delle categorie di dati personali;
(d) I destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
(e) Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
(f) Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; e
(g) Ove possibile, una descrizione delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

BUX tiene registri scritti, e in formato elettronico.

Su richiesta dell'autorità di controllo pertinente, BUX renderà immediatamente disponibili i registri.

Gestione delle lamentele

Al ricevimento di una lamentela di un interessato, BUX indaga internamente sulla lamentela. BUX informa l'interessato del progresso e successivamente dell'esito della lamentela. Queste comunicazioni devono essere effettuate entro un periodo ragionevole.

Se la lamentela non può essere risolta tra l'interessato e BUX, l'interessato può scegliere di cercare di ottenere riparazione attraverso una mediazione, una vertenza o attraverso una lamentela all'autorità di controllo. BUX deve informare gli interessati del loro diritto di lamentarsi direttamente presso l'autorità di controllo.

Appendice 1

dati personali	Qualsiasi informazione (incluse opinioni e intenzioni) che si riferisca a una persona fisica identificata o identificabile
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali
Interessato	Persona fisica identificata o identificabile cui si riferiscono i dati
Consenso	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento
Organizzazione internazionale	Un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.
Autorità di controllo	Autorità di controllo della protezione dei dati per 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 Sito web: www.ico.org.uk

Appendice 2

Lista di controllo della sorveglianza dei dati

Dettagli dei dati conservati dal Gruppo ayondo	
Ragione per conservare i dati	
Metodi per l'ottenimento dei dati	
Data in cui sono stati ottenuti i dati	
Persone fisiche responsabili per i dati	
Memorizzazione dei dati	
Ritenzione dei dati	
Metodologia di cancellazione dei dati	

Política de protección de datos del GDPR

Información importante

De conformidad con el artículo 24 del GDPR (UE) 2016/679, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas, el Grupo ayondo ha implantado medidas técnicas y organizativas apropiadas para garantizar el cumplimiento y la aplicación del Reglamento general de protección de datos (GDPR, siglas inglesas). Esta política es la piedra angular del cumplimiento del GDPR por parte del Grupo ayondo y se revisa y actualiza en consecuencia.

Reglamento general de protección de datos (GDPR)

El Reglamento general de protección de datos (GDPR) de la UE reemplaza a la Directiva de protección de datos 95/46/CE y está diseñado para armonizar las leyes de privacidad de datos en toda Europa, proteger y potenciar la privacidad de datos de todos los ciudadanos de la UE y reformar el modo en que las organizaciones de toda la región abordan la privacidad de datos.

En línea con el artículo 5 del GDPR, el Grupo ayondo debe cumplir los siguientes principios en todo momento.

1. Licitud, lealtad y transparencia	Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.
2. Limitación de la finalidad	Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
3. Minimización de datos	Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
4. Exactitud	Los datos personales serán exactos y, si fuera necesario, actualizados.
5. Limitación del plazo de conservación	Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.
6. Integridad y confidencialidad	Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
7. Responsabilidad proactiva	El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el GDPR y capaz de demostrarlo.

BUX es en todo momento responsable y capaz de demostrar su cumplimiento de los principios citados anteriormente.

Cualquier referencia a los términos “Nosotros”, “Nuestro” o “BUX” hace referencia a cada una de las empresas del grupo de ayondo Group según lo requiera el contexto salvo que se indique lo contrario.

Aplicabilidad

Esta política de privacidad se aplica a las actividades de tratamiento del Grupo ayondo. Las tres principales entidades comerciales dentro del Grupo ayondo son:

- ✓ ayondo markets Limited: una empresa registrada en Inglaterra y Gales con número de registro 03148972. El domicilio social de la empresa es 1st Floor, 7-10 Chandos Street, Londres, W1G 9DQ Reino Unido. Está registrada en el Comisionado de Información del Reino Unido con número de registro Z1457804.
- ✓ ayondo portfolio management GmbH: una empresa registrada en Alemania, registro comercial del Tribunal de Distrito de Frankfurt am Main HRB 102933. El domicilio social de la empresa es Niddastraße 91, 60329 Frankfurt am Main, Alemania.
- ✓ ayondo GmbH: una empresa registrada en Alemania, registro comercial del Tribunal de Distrito de Frankfurt am Main 84169. El domicilio social de la empresa es Niddastraße 91, 60329 Frankfurt am Main, Alemania.

El Grupo ayondo ofrece servicios de de Social Trading y de trading a clientes minoristas y profesionales para productos de apuesta de margen ("SB", siglas inglesas) y contratos por diferencia ("CFD", siglas inglesas) a través de sus subsidiarias, ayondo markets Limited, Londres y ayondo portfolio management GmbH, Fráncfort, respectivamente. ayondo GmbH es un agente vinculado de ayondo markets Limited. Las citadas entidades del grupo son controladoras de datos individuales de datos personales con respecto a los servicios prestados por ellos individualmente.

Supervisión del cumplimiento normativo

Con el fin de mantener un alto nivel de cumplimiento normativo en relación con las reglas estipuladas en esta política, el Grupo ayondo lleva a cabo una auditoría anual de cumplimiento de la protección de datos. La realización de una auditoría de diagnóstico completa permite que el Grupo ayondo reconozca cualquier deficiencia o áreas de mejora; tras su mitigación, garantiza el cumplimiento total del GDPR. Entre los ejemplos de las áreas cubiertas en una auditoría figuran:

(a) La gobernanza de la protección de datos, y las estructuras, políticas y procedimientos para garantizar el cumplimiento del GDPR.
(b) Los procesos para gestionar registros electrónicos y manuales que contienen datos personales.
(c) Los procesos que responden a cualquier solicitud de datos personales.
(d) Las medidas técnicas y organizativas establecidas para garantizar que existe una seguridad adecuada de los datos personales.
(e) La prestación y la supervisión de la capacitación del personal en materia de protección de datos y la conciencia de la protección de datos.

(f) Auditoría de datos según el anexo 2.

Derechos y solicitudes de los interesados

El GDPR establece los siguientes derechos para las personas:

1. El derecho a estar informado.
2. El derecho de acceso.
3. El derecho de rectificación.
4. El derecho de supresión.
5. El derecho a limitar el tratamiento.
6. El derecho a la portabilidad de los datos.
7. El derecho de oposición.
8. Derechos en relación con las decisiones automatizadas y la elaboración de perfiles.

El Grupo ayondo aplica sistemas y controles adecuados para permitir y facilitar la aplicación de los ocho derechos de los interesados enumerados anteriormente.

Cuando un interesado hace una solicitud, el Grupo ayondo iniciará un proceso pragmático de toma de decisiones encabezado por el Delegado de Protección de Datos.

A menos que el Grupo ayondo considere que las solicitudes son de naturaleza excesiva o innecesaria, no se cobrará ninguna tarifa a los interesados por considerar o cumplir dichas solicitudes.

Derechos de acceso

Todas las solicitudes de esta naturaleza deben remitirse al Delegado de Protección de Datos. El Grupo ayondo responderá a dichas solicitudes en el plazo de 30 días.

El interesado tiene derecho a obtener la siguiente información del Grupo ayondo:

(a) Los fines del tratamiento.
(b) Las categorías de datos personales de que se trate.
(c) Los destinatarios o las categorías de datos personales almacenados para el interesado.
(d) El plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.
(e) El uso de decisiones automatizadas, por ejemplo, la elaboración de perfiles.

Cuando se solicite, el Grupo ayondo facilitara una copia de los datos personales almacenados. Para cualquier otra copia solicitada por el interesado, el Grupo ayondo puede cobrar una tarifa razonable basada en los costes administrativos. Cuando las solicitudes se realicen por medios electrónicos, el Grupo ayondo deberá facilitar los datos en un formato electrónico de uso común.

Derecho de rectificación

El Grupo ayondo se asegurará de que todos los interesados puedan ejercer su derecho a obtener de la empresa, sin dilación indebida, la rectificación de los datos personales inexactos que les conciernan.

Derecho de supresión

Sin dilación indebida, el Grupo ayondo suprimirá los datos personales de un interesado cuando así lo solicite, y cuando concurra alguna de las circunstancias siguientes:

(a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
(b) El interesado retire el consentimiento en que se basa el tratamiento, y este no se base en otro fundamento jurídico.
(c) El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento, o cuando el interesado se oponga al tratamiento.
(d) Los datos personales hayan sido tratados ilícitamente.
(e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho del Estado miembro.
(f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

El artículo 17 3 (b) del GDPR establece que el derecho de supresión no se aplica cuando la empresa debe conservar datos para cumplir otra normativa aplicable. La normativa sustitutiva en el caso del Grupo ayondo es el requisito del Reglamento de Blanqueo de Capitales de que las empresas conserven datos KYC durante 5 años y los requisitos de mantenimiento de registros del artículo 16 de MiFID II. Esto se menciona en la declaración de privacidad del Grupo ayondo.

Derecho a limitar el tratamiento

El Grupo ayondo dejará de tratar los datos personales en las siguientes circunstancias:

(a) Cuando una persona impugne la exactitud de los datos personales, el Grupo ayondo restringirá el tratamiento hasta que se verifique la exactitud de los mismos.
(b) Cuando una persona se haya opuesto al tratamiento y el Grupo esté considerando si tiene motivos legítimos para prevalecer sobre los de la persona.
(c) Cuando se determine que el procesamiento es ilícito y la persona se oponga a la supresión y solicite en su lugar una limitación.
(d) Si el Grupo ya no necesita los datos pero la persona los necesita para la formulación, el ejercicio o la defensa de una reclamación.

Derecho a la portabilidad de los datos

El derecho a la portabilidad solo se aplica:

(a) A los datos personales que una persona haya facilitado a un responsable del tratamiento.
(b) Cuando el tratamiento esté basado en el consentimiento de la persona o para la ejecución de un contrato.
(c) Cuando el tratamiento se efectúe por medios automatizados.

Para cumplir la normativa, el Grupo ayondo debe:

(a) Facilitar los datos personales en un formato estructurado, de uso común y lectura mecánica.
(b) Facilitar los datos de forma gratuita (a menos que sean excesivos o innecesarios).

(c) Si se solicita y es técnicamente posible, transmitir los datos directamente a otra organización.
(d) Considerar posibles perjuicios a los derechos de las personas, cuando los datos personales se refieran a más de una persona.

Consentimiento

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de sus datos. El Grupo ayondo obtendrá el consentimiento a través de una declaración por escrito, por medios electrónicos, o una declaración verbal.

El Grupo ayondo solicita, gestiona y registra el consentimiento de conformidad con los artículos 5, 6, 7 y 9 del GDPR.

(a) El Grupo ayondo comprueba que el consentimiento sea la base legal más apropiada para el tratamiento.
(b) El Grupo ayondo presenta la solicitud de consentimiento de forma prominente e independiente de sus términos y condiciones.
(c) El Grupo ayondo solicita una opción de inclusión positiva.
(d) El Grupo ayondo no usa casillas ya marcadas ni ningún otro tipo de consentimiento por defecto.
(e) El Grupo ayondo utiliza un lenguaje sencillo y claro que es fácil de entender.
(f) El Grupo ayondo especifica por qué quiere los datos y su finalidad.
(g) El Grupo ayondo facilita opciones detalladas para prestar el consentimiento por separado para diferentes fines y tipos de tratamiento.
(h) El Grupo ayondo designa su organización y cualquier tercero encargado del tratamiento que se basará en su consentimiento.
(i) El Grupo ayondo garantiza que las personas pueden denegar su consentimiento sin sufrir perjuicio alguno.
(j) El Grupo ayondo evita que el consentimiento sea una condición previa para el servicio.

El Grupo ayondo registra cuándo y cómo la empresa obtuvo el consentimiento de las personas. La empresa también mantiene un registro de la información exacta facilitada originalmente.

Las medidas que el Grupo ayondo puede adoptar para garantizar la gestión adecuada del consentimiento incluyen las siguientes:

(a) El Grupo ayondo revisa periódicamente el consentimiento para verificar que la relación, el tratamiento y los fines no hayan cambiado.
(b) El Grupo ayondo aplica procesos para actualizar el consentimiento a intervalos adecuados, incluidos los consentimientos de los padres (si corresponde).
(c) El Grupo ayondo considera el uso de paneles de privacidad u otros instrumentos de administración de preferencias como una buena práctica.
(d) El Grupo ayondo hace que sea sencillo para las personas retirar su consentimiento en cualquier momento, y divulga cómo se hace.

(e) El Grupo ayondo actúa sobre las retiradas de consentimiento tan pronto como sea posible.
(f) El Grupo ayondo no penaliza a las personas que desean retirar el consentimiento.

El Grupo ayondo no deducirá el consentimiento del silencio o la inactividad. Cuando el tratamiento de datos personales tenga varios fines, el Grupo ayondo obtendrá el consentimiento para todos ellos. Cuando el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, el Grupo ayondo garantizará que la solicitud sea clara, concisa y no perturbe innecesariamente el uso del servicio para el que se presta.

Privacidad de datos desde el diseño

El Grupo ayondo aplica medidas técnicas y organizativas que integran la protección de datos en las actividades de tratamiento.

La privacidad y la protección de datos es una consideración fundamental en las primeras etapas de cualquier proyecto que emprende el Grupo ayondo.

Por ejemplo, cuando:

(a) Construye nuevos sistemas de TI para almacenar datos personales o acceder a ellos.
(b) Desarrolla legislación, políticas o estrategias que tengan implicaciones de privacidad.
(c) Emprende una iniciativa de intercambio de datos.
(d) Usa datos para nuevos fines.

Las consideraciones de privacidad y protección de datos se integrarán dentro de las metodologías y políticas de gestión de riesgos del Grupo ayondo.

Evaluaciones de impacto relativas a la protección de datos (DPIA, siglas inglesas)

El Grupo ayondo lleva a cabo una DPIA cuando sea probable que el tratamiento de datos entrañe un alto riesgo para las personas, por ejemplo:

(a) Cuando se aplique una nueva tecnología.
(b) Cuando sea probable que una operación de elaboración de perfiles afecte significativamente a las personas.
(c) Cuando haya un tratamiento a gran escala de categorías particulares de datos.

Al evaluar el nivel de riesgo, el Grupo ayondo considera tanto la probabilidad como la gravedad de cualquier impacto en las personas en cuestión.

El Grupo ayondo garantiza que existe una sólida comprensión de la DPIA entre ciertos miembros de la empresa.

(a) El Grupo ayondo proporciona formación para que todo el personal entienda la necesidad de considerar una DPIA en las primeras etapas de cualquier plan que implique datos personales.

(b) Las políticas, procesos y procedimientos existentes del Grupo ayondo incluyen referencias a los requisitos de DPIA, cuando corresponda.
(c) El Grupo ayondo comprende los tipos de tratamiento que requieren una DPIA.
(d) El Grupo ayondo crea y documenta un proceso sólido de DPIA.
(e) El Grupo ayondo proporciona formación al personal correspondiente sobre cómo llevar a cabo una DPIA.

Notificación de violaciones

En el caso de violación de la seguridad de los datos personales, el Grupo ayondo la notificará a la autoridad de control pertinente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de la violación. Esto no se exige cuando sea improbable que la violación constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación no tiene lugar en el plazo de 72 horas, el Grupo ayondo deberá indicar un motivo válido de la dilación. Los datos de contacto de las autoridades de control correspondientes se encuentran en el anexo 1.

Las notificaciones realizadas por el Grupo ayondo deberán, como mínimo:

(a) Describir la naturaleza de la violación de la seguridad de los datos personales.
(b) Comunicar el nombre y los datos de contacto del departamento pertinente que gestiona la violación de la seguridad de los datos.
(c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
(d) Describir las medidas adoptadas o propuestas por el Grupo ayondo para para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de los interesados, el Grupo ayondo la comunicará al interesado sin dilación indebida.

El Grupo ayondo comunicará al interesado en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales, detallando al menos la información de los puntos (b), (c) y (d) indicados anteriormente.

Llevanza de registros

El Grupo ayondo emplea a menos de 250 personas y, por lo tanto, el artículo 30 del GDPR no es aplicable técnicamente. Dicho esto, debido a los demás requisitos de supervisión de datos dictados por el GDPR y para una buena práctica, el Grupo ayondo llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener la información indicada a continuación:

(a) El nombre y los datos de contacto del responsable del tratamiento.
(b) Los fines del tratamiento.
(c) Una descripción de las categorías de interesados y de las categorías de datos personales.

(d) Los destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
(e) En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional.
(f) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
(g) Cuando sea posible, una descripción de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

El Grupo ayondo lleva registros por escrito y en formato electrónico.

Si lo solicita la autoridad de control pertinente, el Grupo ayondo pondrá a disposición los registros de inmediato.

Tratamiento de reclamaciones

Tras recibir una reclamación de un interesado, el Grupo ayondo investigará internamente la reclamación. El Grupo ayondo informará al interesado sobre el curso y posteriormente sobre el resultado de la reclamación. Esto debe comunicarse en un plazo razonable.

Cuando la reclamación no pueda resolverse entre el interesado y el Grupo ayondo, el interesado puede optar por obtener una reparación mediante mediación, un procedimiento de litigio o mediante una reclamación ante la autoridad de control. El Grupo ayondo debe informar a los interesados sobre su derecho a presentar reclamaciones directamente ante la autoridad de control pertinente.

Apéndice 1

Datos personales	Toda información (incluidas opiniones e intenciones) sobre una persona física identificada o identificable.
Responsable del tratamiento	Una persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales.
Interesado	La persona física identificada o identificable a quien se refieren los datos.
Consentimiento	Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
Organización internacional	Una organización y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.
Autoridad de control	Autoridad de control de protección de datos para ayondo markets Limited: Oficina del Comisionado de Información Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Tel.: +44 (0) 303 123 1113 Fax: +44 (0) 1625 524 510 Sitio web: www.ico.org.uk

Apéndice 2

Lista de verificación de control de datos

Detalles de los datos en poder del Grupo ayondo	
Motivo para mantener los datos	
Métodos para obtener los datos	
Fecha en que se obtuvieron los datos	
Personas responsables de los datos	
Almacenamiento de datos	
Retención de datos	
Metodología de supresión de datos	

Politique de protection des données - RGPD

Informations importantes

Conformément à l'article 24 du Règlement (UE) 2016/679, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement des données ainsi que des risques pour les droits et libertés des personnes physiques, BUX a mis en œuvre des mesures techniques et organisationnelles appropriées pour assurer le respect et l'application du Règlement général sur la protection des données (GDPR). La présente politique représente la pierre angulaire des efforts de mise en conformité de BUX avec le GDPR. Elle est révisée et mise à jour en conséquence.

Règlement général sur la protection des données (RGPD)

Le Règlement général de l'UE sur la protection des données (RGPD) remplace la directive 95/46/CE sur la protection des données et vise à harmoniser les différentes législations en matière de protection de la vie privée en vigueur en Europe, à protéger et à renforcer la confidentialité des données de tous les citoyens de l'UE et à remodeler la manière dont les organisations exerçant au sein de l'Union abordent la confidentialité des données.

Conformément à l'article 5 du RGPD, BUX doit se conformer à tout moment aux principes suivants.

1. Licéité, loyauté, transparence	Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée.
2. Limitation des finalités	Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.
3. Minimisation des données	Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
4. Exactitude	Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour.
5. Limitation de la conservation	Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.
6. Intégrité et confidentialité	Les données à caractère personnel doivent être traitées de manière à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.
7. Responsabilité	Le responsable du traitement est responsable du respect du RGPD.

BUX est en tout temps responsable et capable de démontrer la conformité aux principes mentionnés précédemment.

Toute référence à "Nous", "Notre", "Nos" ou " BUX " est une référence à une société du Groupe ayondo, selon le contexte, sauf indication contraire.

Applicabilité

La présente politique de confidentialité s'applique aux activités de traitement des données du Groupe ayondo. Les trois principales entités commerciales du Groupe ayondo sont :

- ✓ ayondo markets Limited : société de droit anglais et gallois immatriculée sous le numéro 03148972. Le siège social de la société est sis 1st Floor, 7-10 Chandos Street, Londres, W1G 9DQ Royaume-Uni. Elle est enregistrée auprès du Commissaire à l'information du Royaume-Uni sous le numéro Z145757804.
- ✓ ayondo portfolio management GmbH : société de droit allemand immatriculée au Registre des sociétés du tribunal de district de Francfort-sur-le-Main HRB 102933. Le siège social de la société est sis Niddastraße 91, 60329 FFrancfort-sur-le-Main, Allemagne.
- ✓ ayondo GmbH : une société de droit allemand immatriculée au Registre des sociétés du tribunal de district de Francfort-sur-le-Main HRB 84169. Le siège social de la société est sis Niddastraße 91, 60329 Francfort-sur-le-Main, Allemagne.

Le Groupe ayondo fournit des services d'exécution et de négociation sociale aux clients particuliers et professionnels pour les produits Spread Betting ('SB') et Contract for Difference ('CFD') via ses filiales, ayondo markets Limited, Londres et ayondo portfolio management GmbH, Francfort. ayondo GmbH est un agent lié d'ayondo markets Limited. Les entités du groupe susmentionnées sont les responsables du traitement des données à caractère personnel concernant les services qu'elles fournissent individuellement.

Contrôle de la conformité

Afin de maintenir un niveau élevé de conformité aux dispositions de la présente politique, BUX effectue un audit annuel de la conformité aux normes de protection des données. La réalisation d'un audit diagnostique approfondi permet à BUX d'identifier toutes les éventuelles déficiences ou les domaines d'amélioration possible et, une fois les éventuelles actions correctives prises, de s'assurer de la conformité totale au RGPD. Voici quelques exemples des domaines couverts lors d'un audit :

(a) Gouvernance de la protection des données, ainsi que structures, politiques et procédures visant à assurer le respect des règles du RGPD ;
(b) Procédures de gestion des dossiers électroniques et physiques contenant des données à caractère personnel ;
(c) Procédures de réponse à toute demande de données à caractère personnel ;
(d) Mesures techniques et organisationnelles mises en place pour assurer une sécurité adéquate des données à caractère personnel ;
(e) Organisation et suivi de la formation du personnel en matière de protection des données et sensibilisation à la protection des données ; et
(f) Audit des données, tel que précisé en Annexe 2.

Droits et demandes des personnes concernées

Le RGPD offre aux personnes physiques les protections et droits suivants :

1. Droit d'être informé ;
2. Droit d'accès ;
3. Droit de rectification ;
4. Droit d'effacement ;
5. Droit de restriction du traitement ;
6. Droit à la portabilité des données ;
7. Droit de s'opposer ; et
8. Droits liés à la prise de décision et au profilage automatisés.

BUX a mis en place des systèmes et des contrôles adéquats pour permettre et faciliter l'application des huit droits susmentionnés des personnes concernées.

Lorsqu'une personne concernée présente une demande, BUX engage un processus décisionnel pragmatique, dirigé par le Délégué à la protection des données.

A moins que BUX ne juge les demandes excessives ou inutiles par nature, aucun frais ne sera facturé aux personnes concernées pour l'examen et/ou la réponse à de telles demandes.

Droit d'accès

Toutes les demandes de cette nature doivent être transmises au Délégué à la protection des données. BUX doit répondre à ces demandes dans un délai de 30 jours.

La personne concernée a le droit d'obtenir, auprès de BUX, les informations suivantes :

(a) Les finalités du traitement ;
(b) Les catégories de données à caractère personnel concernées ;
(c) Les destinataires ou les catégories de destinataires des données à caractère personnel stockées pour la personne concernée ;
(d) Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ; et
(e) L'existence d'une prise de décision automatisée, par exemple une procédure de profilage.

BUX doit remettre sur demande une copie des données à caractère personnel détenues. Pour toute autre copie demandée par la personne concernée, BUX peut facturer des frais raisonnables sur la base des frais administratifs encourus. Lorsque les demandes sont faites par voie électronique, BUX fournit les données sous une forme électronique couramment utilisée.

Droit de rectification

BUX veille à ce que toutes les personnes concernées puissent exercer leur droit d'obtenir de sa part, sans retard injustifié, la rectification de données personnelles inexactes les concernant.

Droit d'effacement

BUX doit effacer sans retard injustifié les données à caractère personnel d'une personne concernée lorsque la demande lui en est faite et que s'applique l'un des motifs suivants :

(a) Les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
(b) La personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ;
(c) La personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement ;
(d) Les données à caractère personnel ont fait l'objet d'un traitement illicite;
(e) Les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'État membre auquel le responsable du traitement est soumis; et/ou
(f) Les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information.

L'article 17, paragraphe 3, point b), du RGPD stipule que le droit à l'effacement n'est pas applicable lorsque l'entreprise est tenue de conserver des données afin de se conformer à d'autres réglementations applicables. Dans le cas de BUX, les réglementations qui supplantent les obligations précédemment mentionnées sont l'obligation pour les entreprises de conserver les données de type KYC pendant 5 ans ainsi que l'article 16 de la loi MiFID II sur la tenue de registres. Ce point est mentionné dans l'avis de confidentialité de BUX.

Droit à la limitation du traitement des données :

BUX mettra fin au traitement des données à caractère personnel dans les hypothèses suivantes :

(a) Lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée, BUX limitera le traitement des données pendant une durée lui permettant de vérifier leur exactitude ;
(b) Lorsque la personne concernée s'oppose audit traitement et que le groupe évalue le bien-fondé d'une telle demande ;
(c) Lorsque le traitement est illicite et la personne concernée s'oppose à l'effacement des données et exige à la place la limitation de leur utilisation et/ou
(d) Si le groupe n'a plus besoin des données mais que la personne concernée les demande aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice.

Droit à la portabilité des données

Le droit à la portabilité des données ne s'applique que :

(a) Aux données à caractère personnel qu'une personne physique à remises à un responsable des données ;
(b) Lorsque le traitement est fondé sur un consentement ou en vue de l'exécution d'un contrat et
(c) Lorsque le traitement est réalisé de manière automatisée.

Pour se conformer à ces obligations, BUX doit :

(a) Fournir les données à caractère personnel dans un format structuré, couramment utilisé et lisible par machine ;
(b) Fournir les données sans frais (sauf si les demandes de la personne concernée sont manifestement infondées ou excessives) ;
(c) Si cela est demandé et techniquement possible, transmettre directement les données à une autre organisation ; et
(d) Prendre en compte le préjudice possible au droit des personnes si les données à caractère personnel concernent plus d'une personne physique.

Consentement

Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant. BUX obtiendra un tel consentement sous forme écrite, par voie électronique, ou sous forme verbale.

BUX demande, gère et enregistre ce consentement conformément aux articles 5, 6, 7 et 9 du RGPD.

(a) BUX s'assure que le consentement est le fondement juridique le plus approprié pour le traitement des données ;
(b) BUX rend la demande de consentement visible et distincte de ses termes et conditions ;
(c) BUX demande une réponse positive ;
(d) BUX n'utilise pas de cases pré-cochées ou tout autre type de consentement par défaut ;
(e) BUX utilise des termes clairs et simples, faciles à comprendre ;
(f) BUX spécifie pourquoi il veut les données et la finalité de leur traitement ;
(g) BUX propose des options distinctes permettant de consentir séparément à différents buts et types de traitement ;
(h) BUX désigne son organisation ainsi que tout contrôleur tiers qui s'appuiera sur ledit consentement ;
(i) BUX s'assure que les personnes concernées peuvent refuser de donner leur consentement sans préjudice ; et
(j) BUX évite de faire du consentement une condition préalable à la prestation de service.

BUX enregistre quand et comment l'entreprise a obtenu le consentement des personnes concernées. L'entreprise tient également un registre des informations exactes fournies à l'origine.

Les mesures que BUX peut appliquer pour assurer une gestion appropriée des consentements comprennent les éléments suivants :

(a) BUX examine régulièrement les consentements pour vérifier que la relation, le traitement et les finalités n'ont pas changé ;
(b) BUX a mis en place des procédures pour actualiser le consentement à des intervalles de temps appropriés, y compris les consentements parentaux (le cas échéant) ;
(c) BUX considère l'utilisation de tableaux de bord sur la protection de la vie privée ou d'autres outils de gestion des préférences comme une bonne pratique ;
(d) BUX permet aux individus de retirer leur consentement à tout moment et rend publique la manière dont ce retrait peut être effectué ;

(e) BUX agit au plus vite en cas de retrait du consentement et
(f) BUX ne pénalise pas les personnes qui souhaitent retirer leur consentement.

BUX ne déduira pas un consentement d'un silence ou d'une inactivité. Lorsque le traitement des données à caractère personnel a des finalités multiples, BUX obtiendra le consentement pour toutes ces finalités. Lorsque le consentement de la personne concernée doit être donné à la suite d'une demande par voie électronique, BUX veillera à ce que la demande soit claire, concise et ne perturbe pas inutilement l'utilisation du service pour lequel elle est fournie.

Principes de protection des données dès la conception

BUX a mis en place des mesures techniques et organisationnelles qui intègrent la protection des données dans les activités de traitement.

La protection de la vie privée et des données est une considération clé dès les premières étapes de tout projet que BUX entreprend.

Par exemple lors des moments ci-après :

(a) Mise en place de nouveaux systèmes informatiques pour le stockage ou l'accès aux données à caractère personnel ;

(b) Élaboration de règles, de politiques ou de stratégies qui ont des répercussions sur la protection de la vie privée ;

(c) Engagement dans une initiative de partage des données ; et/ou

(d) Utilisation des données à de nouvelles fins.

Les considérations relatives à la protection de la vie privée et des données seront intégrées dans les méthodologies et politiques de gestion des risques de BUX.

Analyses d'impact relatives à la protection des données (AIPD)

BUX réalise une AIPD lorsque le traitement des données est susceptible d'entraîner un risque élevé pour les personnes, par exemple :

(a) Lorsqu'une nouvelle technologie est mise en place ;
(b) Lorsqu'une opération de profilage est susceptible d'affecter de manière significative des personnes concernées; et/ou
(c) En cas de traitement à grande échelle de catégories particulières de données.

Pour évaluer le niveau de risque, BUX tient compte à la fois de la probabilité et de la gravité d'un impact sur les personnes concernées.

BUX s'assure de la bonne compréhension de l'AIPD parmi les membres concernés de la société.

(a) BUX propose une formation qui permet à l'ensemble des membres de son personnel de comprendre la nécessité d'envisager une AIPD dès les premières étapes d'un plan impliquant des données à caractère personnel ;
(b) Les politiques, processus et procédures en place de BUX comprennent des références aux exigences d'AIPD, le cas échéant ;
(c) BUX comprend les types de traitement qui nécessitent une AIPD ;
(d) BUX crée et documente un processus d'AIPD robuste ; et
(e) BUX dispense aux membres concernés de son personnel une formation sur la manière de réaliser une AIPD.

Signalement des violations

Dès que BUX apprend qu'une violation de données à caractère personnel s'est produite, il s'engage à en informer l'autorité de contrôle dans les meilleurs délais et, lorsque c'est possible, 72 heures au plus tard après en avoir pris connaissance. Cette obligation ne concerne que les situations dans lesquelles la violation fera survenir de manière probable un risque pour les droits et libertés des personnes concernées/ Si une telle notification ne peut avoir lieu dans ce délai de 72 heures, elle doit être assortie des motifs du retard. Les coordonnées des autorités de contrôle concernées sont indiquées en Annexe 1.

Les signalements réalisés par BUX doivent au minimum :

(a) Décrire la nature de la violation de données à caractère personnel ;
(b) Communiquer le nom et les coordonnées du service prenant en charge la violation :
(c) Décrire les conséquences probables de la violation de données à caractère personnel ;
(d) Décrire les mesures prises ou que BUX propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, BUX communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées aux points b), c) et d) ci-dessus.

Tenue des dossiers et registres

BUX emploie moins de 250 personnes. Par conséquent, l'article 30 du RGPD n'est techniquement pas applicable. Cela étant dit, en raison des autres exigences de contrôle des données dictées par le

RGPD et afin de garantir les meilleures pratiques, BUX tiendra un registre des activités de traitement réalisées sous sa responsabilité. Ce registre contiendra les informations suivantes :

(a) Le nom et les coordonnées du responsable du traitement ;
(b) Les finalités du traitement ;
(c) Une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
(d) Les destinataires auprès desquels les données à caractère personnel ont été ou seront divulguées, y compris les destinataires situés dans des pays tiers ou des organisations internationales ;
(e) Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, comprenant l'identification de ce dernier ou de cette dernière ;
(f) Si possible, les délais envisagés pour l'effacement des différentes catégories de données ; et
(g) Si possible, une description des mesures techniques et organisationnelles visées à l'Article 32, paragraphe 1.

BUX conserve ses dossiers et registres par écrit et au format électronique.

BUX met immédiatement ces documents à disposition de l'autorité de surveillance compétente à la demande de cette dernière.

Prise en charge des réclamations

Dès réception d'une réclamation d'une personne concernée, BUX procédera à une enquête interne. BUX informera la personne concernée de l'état d'avancement et, par la suite, de l'issue donnée à sa réclamation. Ces informations doivent être communiquées dans un délai raisonnable.

Lorsque la réclamation ne peut être résolue entre la personne concernée et BUX, la personne concernée peut choisir de demander réparation par le biais d'une médiation, d'une procédure judiciaire ou d'une plainte auprès de l'autorité de contrôle concerné. BUX doit informer les personnes concernées de leur droit de présenter directement une réclamation auprès de l'autorité de contrôle compétente.

Annexe 1

Données à caractère personnel	Toute information (y compris les opinions et les intentions) qui concerne une personne physique identifiée ou identifiable.
Contrôleur de données	La personne physique ou morale, autorité publique, service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données.
Personne concernée	La personne physique identifiée ou identifiable à laquelle se rapportent les données.
Consentement	Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.
Organisation internationale	Une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.
Autorité de contrôle :	Autorité de supervision de la protection des données pour BUX : Bureau du Préposé à la protection des données Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Tél : +44 (0)303 123 1113 Fax : +44 (0)1625 524 510 Site internet : www.ico.org.uk

Annexe 2

Liste de contrôle du suivi des données

Détail des données détenues par le Groupe ayondo	
Raison pour laquelle les données sont conservées	
Méthode d'obtention des données	
Date d'obtention des données	
Personnes responsables des données	
Conservation des données	
Stockage des données	
Méthode de suppression des données	

GDPR Databeskyttelsespolitik

Vigtige oplysninger

I overensstemmelse med artikel 24 i GDPR (EU) 2016/679 har koncernen, under hensyntagen til arten, omfanget, konteksten og formålet med behandlingen samt risiciene for fysiske personers rettigheder og frihedsrettigheder, indført passende tekniske og organisatoriske foranstaltninger til at sikre overholdelse og overholdelse af den generelle databeskyttelsesforordning (GDPR). Denne politik står som hjørnestenen i ayondo-koncernens overholdelse af GDPR og gennemgås og opdateres i overensstemmelse hermed.

Databeskyttelsesforordningen (GDPR)

EU's databeskyttelsesforordning (GDPR) erstatter databeskyttelsesdirektivet 95/46/EF og har til formål at harmonisere lovgivningen om beskyttelse af personlige oplysninger i hele Europa for at beskytte og styrke alle EU-borgernes personlige oplysninger og omforme den måde, hvorpå organisationer over hele regionen behandler personlige oplysninger på.

I overensstemmelse med artikel 5 i GDPR skal ayondo-koncernen til enhver tid overholde følgende principper.

1. Lovlighed, retfærdighed og gennemsigtighed	Personlige oplysninger skal behandles lovligt, retfærdigt og på en gennemsigtig måde i forhold til dataemnet.
2. Begrænsning af formål	Personlige oplysninger skal indsamles til angivne, udtrykkelige og legitime formål og ikke viderebehandles på en måde, der er uforenelig med disse formål.
3. Dataminimering	Personlige oplysninger skal være tilstrækkelige, relevante og begrænsede til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.
4. Nøjagtighed	Personlige oplysninger skal være nøjagtige og om nødvendigt holdes ajourførte.
5. Begrænsning af opbevaring	Personlige oplysninger skal opbevares i et format, der ikke tillader identifikation af dataemner længere end nødvendigt for de formål, som de personlige oplysninger behandles.
6. Integritet og fortrolighed	Personlige oplysninger skal behandles på en måde, der sikrer passende sikkerhed af de personlige oplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og imod utilsigtet tab, ødelæggelse eller skade ved hjælp af passende tekniske eller organisatoriske foranstaltninger.
7. Ansvarlighed	Controlleren skal være ansvarlig for og kunne dokumentere overholdelse af GDPR.

BUX er til enhver tid ansvarlig for, og kan påvise overensstemmelse med, de ovenstående principper.

Alle henvisninger til "os", "vores", "vi" eller "BUX" refererer til hvert koncernselskab i ayondo Group, i overenstemmelse med konteksten, medmindre andet er angivet.

Anvendelsesområde

Denne fortrolighedspolitik gælder for behandlingsaktiviteterne i ayondo-koncernen. De tre vigtigste handelsenheder i ayondo-koncernen er:

- ✓ Ayondo Markets Limited er et selskab registreret i England og Wales under registreringsnummer 03148972. Selskabets registrerede adresse er 1st Floor, 7-10 Chandos Street, London, W1G 9DQ Storbritannien. Det er registreret hos UK Information Commissioner under registreringsnummer Z1457804.
- ✓ ayondo portfolio management GmbH: Et selskab registreret i Tyskland, handelsregisteret for distriktsdomstolen i Frankfurt am Main HRB 102933. Selskabets registrerede adresse er Niddastraße 91, 60329 Frankfurt am Main, Tyskland.
- ✓ ayondo GmbH: et selskab registreret i Tyskland, handelsregisteret for distriktsdomstolen i Frankfurt am Main 84169. Selskabets registrerede adresse er Niddastraße 91, 60329 Frankfurt am Main, Tyskland.

ayondo-koncernen tilbyder kun eksekvering og henholdsvis sociale handelstjenester til detail- og professionelle kunder for Spread Betting ('SB') og Contract for Difference ('CFD')-produkter via dets datterselskaber, ayondo markets Limited, London og ayondo portfolio management GmbH, Frankfurt. ayondo GmbH er en bundet agent tilhørende ayondo markets Limited. Ovennævnte koncernenheder er individuelle datacontrollere af dine personlige oplysninger med hensyn til de tjenester, de leverer individuelt.

Overvågning af compliance

For at opretholde et højt niveau af overholdelse i forhold til de regler, der er fastsat i denne politik, udfører ayondo-koncernen en årlig databeskyttelsesovervågningsrevision. En grundig diagnostisk revision giver ayondo-koncernen mulighed for at genkende eventuelle mangler eller forbedringsområder; ved afbødning, der sikrer total overholdelse af GDPR. Eksempler på de områder, der er omfattet af en revision, omfatter:

(a) Håndtering af databeskyttelse og strukturer, politikker og procedurer til sikring af overholdelse af GDPR
(b) Processerne til styring af både elektroniske og manuelle poster indeholdende personlige oplysninger;
(c) Processerne svarer til enhver anmodning om personlige oplysninger;
(d) De tekniske og organisatoriske foranstaltninger til at sikre, at der er tilstrækkelig sikkerhed over personlige oplysninger
(e) Tilvejebringelse og overvågning af personaleuddannelse om og bevidstgørelse om databeskyttelse, og
(f) Datarevisioner som pr. Bilag 2.

Dataemners rettigheder og forespørgsler

GDPR giver følgende rettigheder til enkeltpersoner:

1. Retten til at blive informeret
2. Retten til adgang
3. Retten til berigtigelse
4. Retten til at slette
5. Retten til at begrænse behandling
6. Retten til dataoverførbarhed
7. Retten til at gøre indsigelse og
8. Rettigheder i forbindelse med automatiseret beslutningstagning og profilering.

ayondo-koncernen har indført tilstrækkelige systemer og kontroller til at muliggøre og lette anvendelsen af de ovennævnte otte rettigheder for dataemner.

Når et dataemne stiller en anmodning, vil ayondo-koncernen påbegynde en pragmatisk beslutningsproces opstillet af virksomhedens Data Protection Officer.

Medmindre ayondo-koncernen anser anmodninger for at være for store eller unødvendige i deres natur, vil dataemnerne ikke blive opkrævet gebyrer for at overveje og/eller overholde sådanne anmodninger.

Retten til adgang

Alle anmodninger af denne art skal rettes til virksomhedens Data Protection Officer. ayondo-koncernen skal svare på sådanne anmodninger inden for 30 dage.

Dataemnet har ret til at få følgende oplysninger fra ayondo-koncernen:

(a) Formålet med behandlingen
(b) Kategorierne af de pågældende personlige oplysninger
(c) Modtagere eller kategorier af de personlige oplysninger, som er gemt om dataemnet
(d) Den planlagte periode, for hvilken de personlige oplysninger vil blive gemt eller, hvis det ikke er muligt, de kriterier, der anvendes til at fastsætte denne periode, og
(e) Brugen af enhver automatiseret beslutningstagning f.eks. profilering.

Efter anmodning skal ayondo-koncernen give en kopi af de indeholdte personlige oplysninger. For eventuelle yderligere kopier, som dataemnet har anmodet om, kan ayondo-koncernen opkræve et rimeligt gebyr baseret på de administrative omkostninger. Hvis anmodninger foretages via elektroniske midler, skal ayondo-koncernen give oplysningerne i et almindeligt anvendt elektronisk format.

Ret til berigtigelse

ayondo-koncernen skal sikre, at alle dataemner er i stand til at udøve deres ret til uden unødig forsinkelse at rette unøjagtige personlige oplysninger om ham eller hende.

Ret til sletning

Uden unødig forsinkelse skal ayondo-koncernen slette personlige oplysninger om et dataemne efter anmodning, og hvor en af følgende grunde finder anvendelse:

(a) De personlige oplysninger er ikke længere nødvendige i forhold til de formål, hvortil de blev indsamlet eller på anden måde behandlet
(b) Dataemner trækker sig samtykke tilbage, som behandlingen er baseret på, og hvor der ikke er nogen anden juridisk grund til behandlingen
(c) Dataemnet protesterer mod behandlingen, og der ikke er nogen overvejende legitime grunde til behandlingen
(d) De personlige oplysninger er blevet behandlet ulovligt
(e) De personlige oplysninger skal slettes i overensstemmelse med en juridisk forpligtelse i medlemslandets lovgivning, og/eller
(f) De personlige oplysninger er indsamlet i forhold til tilbuddet om informationssamfundstjenester.

Artikel 17, stk. 3, litra b), GDPR, fastslår, at retten til sletning ikke finder anvendelse, hvor virksomheden skal opbevare oplysninger for at overholde andre gældende regler. Erstatningsbestemmelser i ayondo-koncernens tilfælde er kravet i forordningen mod hvidvaskning af penge om, at virksomheder skal holde KYC-data i 5 år og MiFID II § 16 krav til registrering. Dette er omtalt i ayondo-koncernens fortrolighedsmeddelelse.

Ret til at begrænse behandling

ayondo-koncernen ophører med at behandle personlige oplysninger under følgende omstændigheder:

(a) Hvis en person bestrider nøjagtigheden af de personlige oplysninger, vil ayondo-koncernen begrænse behandlingen, indtil oplysningerne er nøjagtige
(b) Hvor en person har gjort indsigelse mod behandlingen, og koncernen overvejer, om den har legitime grunde til at tilsidesætte individets
(c) Når behandlingen er fundet ulovlig, og personen modsætter sig sletning og anmoder om en begrænsning i stedet, og/eller
(d) Hvis koncernen ikke længere har brug for oplysningerne, men personen kræver oplysningerne for at etablere, udøve eller forsvare et juridisk krav.

Ret til dataoverførbarhed

Retten til overførbarhed gælder kun:

(a) For personlige oplysninger, som en person har givet en controller
(b) Hvor behandlingen er baseret på personens samtykke eller for udførelsen af en kontrakt, og
(c) Når behandlingen udføres med automatiserede midler.

For at overholde, skal ayondo-koncernen:

(a) Give de personlige oplysninger i et struktureret, almindeligt anvendt og maskinlæsbart format
(b) Give oplysningerne gratis (medmindre det er overdrevet eller unødvendigt)

(c) Hvis det ønskes og teknisk muligt, overføre oplysningerne direkte til en anden organisation. og
(d) Overveje mulige enkeltpersoners rettigheder, hvor de personlige oplysninger vedrører mere end én person.

Samtykke

Samtykke skal gives ved en klar bekræftende handling, der fastlægger frit givet, specifik, informeret og entydig angivelse af dataemnets samtykke til behandlingen af deres data. ayondo-koncernen opnår samtykke via en skriftlig, elektronisk eller en mundtlig erklæring.

ayondo-koncernen anmoder om, håndterer og registrerer samtykke i henhold til artikel 5, 6, 7 og 9 i GDPR.

(a) ayondo-koncernen kontrollerer, at samtykket er det mest hensigtsmæssige lovlige grundlag for behandling
(b) ayondo-koncernen gør anmodningen om samtykke fremtrædende og adskilt fra dens vilkår og betingelser
(c) ayondo-koncernen anmoder om et positivt tilvalg
(d) ayondo-koncernen anvender ikke forudkrydsede felter eller nogen anden form for standard-samtykke
(e) ayondo-koncernen bruger et klart sprog, der er let at forstå
(f) ayondo-koncernen specificerer, hvorfor den vil have oplysninger, og deres formål
(g) ayondo-koncernen giver granulære muligheder for at give særskilt samtykke til forskellige formål og typer af behandling
(h) ayondo-koncernen nævner sin organisation og eventuelle tredjepartscontrollere, som vil afhænge af samtykket
(i) ayondo-koncernen sikrer, at enkeltpersoner kan nægte at give sit samtykke, uden skade, og
(j) ayondo-koncernen undgår at gøre et samtykke til en forudsætning for en tjeneste.

ayondo-koncernen registrerer, hvornår og hvordan selskabet har opnået samtykke fra enkeltpersoner. Selskabet fører også en fortegnelse over de nøjagtige oplysninger, der oprindeligt blev leveret.

Øvelser, som ayondo-koncernen kan udføre for at sikre en passende forvaltning af samtykke, omfatter følgende:

(a) ayondo-koncernen gennemgår regelmæssigt tilladelser for at kontrollere, at forholdet, behandlingen og formålene ikke er ændret
(b) ayondo-koncernen har indført processer til at opdatere samtykke med passende mellemrum, herunder eventuelle forældres samtykker (hvis det er relevant)
(c) ayondo-koncernen overvejer at bruge fortrolighedspaneler eller andre præferencehåndteringsværktøjer som god praksis
(d) ayondo-koncernen gør det nemt for enkeltpersoner til enhver tid at kunne tilbagekalde deres samtykke og offentliggør, hvordan dette gøres
(e) ayondo-koncernen handler på tilbagekaldelse af samtykke hurtigst muligt, og

(f) ayondo-koncernen straffer ikke personer, der ønsker at tilbagekalde deres samtykke.

ayondo-koncernen vil ikke udlede samtykke fra stilhed eller inaktivitet. Når behandlingen af personlige oplysninger har flere formål, vil ayondo-koncernen opnå samtykke til alle disse. Hvis et dataemnes samtykke skal gives efter en anmodning elektronisk, vil ayondo-koncernen sikre, at anmodningen er klar, kortfattet og ikke unødigt forstyrrende for brugen af den tjeneste, den leveres til.

Datasikkerhed ved design

ayondo-koncernen har indført tekniske og organisatoriske foranstaltninger, der integrerer databeskyttelse i behandlingsaktiviteter.

Beskyttelse af personlige oplysninger og databeskyttelse er en vigtig betragtning i de tidlige stadier af ethvert projekt, ayondo-koncernen forpligter sig til

For eksempel ved:

(a) Opbygning af nye it-systemer til opbevaring eller adgang til personlige oplysninger
(b) Udvikling af lovgivning, politik eller strategier, der har konsekvenser for privatlivets fred
(c) Introduktion til et datadelingsinitiativ, og/eller
(d) Brug af oplysninger til nye formål.

Beskyttelse af personlige oplysninger og databeskyttelse vil blive integreret inden for ayondo-koncernens risikostyringsmetoder og -politikker.

Databeskyttelsespåvirkningsvurderinger (DPIA)

ayondo-koncernen udfører en DPIA, hvor databehandling sandsynligvis vil medføre høj risiko for enkeltpersoner, for eksempel:

(a) Hvor en ny teknologi implementeres
(b) Hvor en profileringsaktivitet sandsynligvis vil påvirke personer væsentligt, og/eller
(c) Hvor der er behandling i stor skala af særlige kategorier af oplysninger.

Ved vurderingen af risikoniveauet vurderer ayondo-koncernen både sandsynligheden for og alvorligheden af eventuelle konsekvenser for de berørte personer.

ayondo-koncernen sikrer, at der er en god forståelse af DPIA blandt visse medlemmer af selskabet.

(a) ayondo-koncernen tilbyder uddannelse, så alle medarbejdere forstår behovet for at overveje en DPIA i de tidlige stadier af enhver plan, der involverer personlige oplysninger
(b) ayondo-koncernens eksisterende politikker, processer og procedurer omfatter henvisninger til DPIA-krav, hvor det er relevant
(c) ayondo-koncernen forstår de typer af behandling, der kræver en DPIA

(d) ayondo-koncernen opretter og dokumenterer en robust DPIA-proces, og
(e) ayondo-koncernen tilbyder uddannelse til relevant personale om, hvordan man udfører en DPIA.

Rapportering af brud

I tilfælde af brud på personlige oplysninger skal ayondo-koncernen uden unødig forsinkelse og om muligt underrette den relevante tilsynsmyndighed senest 72 timer efter at have fået kendskab til bruddet. Dette er ikke påkrævet, hvis bruddet sandsynligvis ikke vil medføre en risiko for fysiske personers rettigheder og friheder. Hvis rapporteringen ikke er foretaget inden for 72 timer, skal ayondo-koncernengive en gyldig grund til forsinkelsen. Kontaktoplysninger til relevante tilsynsmyndigheder findes i Bilag 1.

Meddelelser foretaget af ayondo-koncernen skal mindst:

(a) Beskrive karakteren af bruddet af de personlige oplysninger
(b) Indeholde navn og kontaktoplysninger til den relevante afdeling, der håndterer databruddet
(c) Beskrive de sandsynlige konsekvenser af bruddet af de personlige oplysninger, og
(d) Beskrive den foranstaltning, der er truffet eller foreslået af ayondo-koncernen for at afhjælpe bruddet af de personlige oplysninger, herunder om nødvendigt foranstaltninger til afhjælpning af mulige bivirkninger.

Hvor overtrædelsen af personlige oplysninger sandsynligvis vil medføre stor risiko for dataemnets rettigheder og friheder, meddeler ayondo-koncernen databruddet til dataemnet uden unødig forsinkelse.

ayondo-koncernen underretter dataemnet på et klart og tydeligt sprog om arten af bruddet af de personlige oplysninger, idet de i det mindste beskriver oplysningerne i litra b), c) og d) som ovenfor.

Journalføring

ayondo-koncernen beskæftiger færre end 250 personer, og derfor er artikel 30 i GDPR teknisk set ikke relevant. På grund af de øvrige dataovervågningskrav dikteret af GDPR og for bedste praksis, vil ayondo-koncernen dog føre en journal over behandlingsaktiviteter under sit ansvar. Journalen skal indeholde følgende oplysninger:

(a) Navn og kontaktoplysninger på controlleren
(b) Formålet med behandlingen
(c) En beskrivelse af kategorierne af dataemner og af kategorierne af personlige oplysninger
(d) Modtagere til hvem de personlige oplysninger er blevet eller vil blive offentliggjort, herunder modtagere i tredjelande eller internationale organisationer
(e) Hvor det er relevant, overførsel af personlige oplysninger til et tredjeland eller en international organisation, herunder identifikation af dette tredjeland eller internationale organisation
(f) Hvor det er muligt, de planlagte tidsfrister for sletning af de forskellige kategorier af oplysninger, og

(g) Hvor det er muligt, en beskrivelse af de tekniske og organisatoriske foranstaltninger, der er omhandlet i artikel 32, stk. 1.

ayondo-koncernen fører journaler skriftligt og i elektronisk format.

ayondo-koncernen vil omgående stille journalerne til rådighed efter anmodning fra den relevante tilsynsmyndighed.

Klagerhåndtering

Efter modtagelse af en klage fra et dataemne skal ayondo-koncernen undersøge klagen internt. ayondo-koncernen skal informere dataemner om fremskridtene og efterfølgende resultatet af klagen. Dette skal meddeles inden for en rimelig periode.

Hvis klagen ikke kan løses mellem dataemnet og ayondo-koncernen, kan dataemnet vælge at søge erstatning gennem mægling, retssagsprocedure eller via en klage til tilsynsmyndigheden. ayondo-koncernen skal informere dataemnerne om deres ret til at klage direkte til den relevante tilsynsmyndighed.

Bilag 1

Personlig oplysninger	Eventuelle oplysninger (herunder meninger og hensigter), der vedrører en identificeret eller identificerbar fysisk person
Datacontroller	En fysisk eller juridisk person, offentlig myndighed, et agentur eller et andet organ, som alene eller i fællesskab med andre bestemmer formålene med og midlerne til behandling af personlige oplysninger
Dataemne	Den identificerede eller identificerbare fysiske person, som oplysningerne refererer til
Samtykke	Enhver frit givet, specifik, informeret og entydig angivelse af dataemnets ønsker, hvormed han eller hun ved en erklæring eller ved en klar bekræftende handling siger sig enig i behandling af personlige oplysninger vedrørende ham eller hende
International organisation	En organisation og dens underordnede organer underlagt folkeretten eller ethvert andet organ, der er oprettet af eller på grundlag af en aftale mellem to eller flere lande.
Tilsynsmyndighed	Databeskyttelsesmyndighed for ayondo markets Limited: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Tlf.: +44 (0)303 123 1113 Fax: +44 (0)1625 524 510 Websted: www.ico.org.uk

Bilag 2

Tjekliste til overvågning af oplysninger

Detaljer om oplysninger, som opbevares af ayondo-koncernen	
Årsag til at opbevare oplysningerne	
Metoder til opnåelse af oplysningerne	
Dato, hvor oplysningerne blev opnået	
Personer, der er ansvarlige for oplysningerne	
Datalagring	
Databevaring	
Datasletningsmetode	

Dataskyddspolicy enligt dataskyddsförordningen (GDPR)

Viktig information

Bux har i överensstämmelse med artikel 24 i förordning 2016/679 (EU) (dataskyddsförordningen) och med beaktande av behandlingens art, omfattning, kontext och syften samt risker för fysiska personers rättigheter och friheter, genomfört lämpliga tekniska och organisatoriska åtgärder i syfte att säkerställa efterlevnad och tillämpning av den allmänna dataskyddsförordningen (GDPR). Denna policy utgör hörnstenen i BUX efterlevnad av dataskyddsförordningen och granskas och uppdateras i enlighet därmed.

BUX utgör handelsnamnet för ayondo markets Limited. ayondo markets Limited är ett bolag registrerat i England and Wales med organisationsnummer 03148972. ayondo markets Limited är godkänt och regleras av Financial Conduct Authority (FCA) med FCA-registernummer 184333.

Dataskyddsförordningen

EU:s dataskyddsförordning (GDPR) ersätter dataskyddsdirektiv 95/46/EG och syftar till att harmonisera de europeiska dataskyddslagarna, skydda och förstärka samtliga EU-medborgares integritet med avseende på personuppgifter samt omforma det tillvägagångssätt som organisationer i regionen handskas med skyddet av personuppgifter.

Bux måste i enlighet med artikel 5 i GDPR alltid efterleva följande principer:

1. Laglighet, korrekthet och öppenhet	Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.
2. Begränsning av ändamål	De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.
3. Uppgiftsminimering	De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.
4. Korrekthet	De ska vara korrekta och om nödvändigt uppdaterade.
5. Lagringsminimering	De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.
6. Integritet och konfidentialitet	De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.
7. Ansvarsskyldighet	Den personuppgiftsansvarige ska ansvara för och kunna visa att dataskyddsförordningen efterlevs.

BUX ansvarar alltid för och kan alltid uppvisa att bolaget efterföljer de förutnämnda principerna.

Varje hänvisning till "oss", "vår", "vi" eller "BUX" är en hänvisning till varje koncernföretag inom ayondokoncernen i enlighet med vad sammanhanget kräver, såtillvida inte annat har angetts.

Tillämpbarhet

Denna integritetspolicy gäller för ayondokoncernen behandlingsaktiviteter. De tre huvudsakliga handlande enheterna inom ayondokoncernen utgörs av:

- ✓ ayondo markets Limited: ett bolag grundat i England och Wales med organisationsnummer 03148972. Bolagets registrerade adress är: 1st Floor, 7-10 Chandos Street, London, W1G 9DQ Storbritannien. Bolaget är registrerat hos den brittiska personuppgiftsombudsmannen under registreringsnummer Z1457804.
- ✓ ayondo portfolio management GmbH: ett bolag registrerat i Tyskland och registrerat i handelsregistret vid distriktsdomstolen för Frankfurt am Main HRB 102933. Bolagets registrerade adress är Niddastraße 91, 60329 Frankfurt am Main, Tyskland.
- ✓ ayondo GmbH: ett bolag registrerat i Tyskland i handelsregistret vid distriktsdomstolen för Frankfurt am Main 84169. Bolagets registrerade adress är Niddastraße 91, 60329 Frankfurt am Main, Tyskland.

ayondo Group tillhandahåller endast exekveringstjänster och sociala handelstjänster till Spread Bettings ("SB") detaljhandelskunder och professionella kunder, samt produkter i form av CFD-kontrakt (Contract for Difference) via dess dotterbolag, ayondo markets Limited, London och ayondo portfolio management GmbH i Frankfurt. ayondo GmbH är ett anknutet ombud för ayondo markets Limited. De ovannämnda koncernenheterna är enskilt personuppgiftsansvariga med avseende på de tjänster som de erbjuder var för sig.

Övervakning av regelefterlevnad

I syfte att vidmakthålla en hög efterlevnadsnivå gällande reglerna som uppställs inom ramen för denna policy, genomför BUX årligen en regelefterlevnadsrevision av dataskyddsområdet. Genom en grundlig diagnostisk revision kan BUX upptäcka förekommande brister eller områden som kräver förbättring, vilka efter förbättringsåtgärder säkerställer en fullständig efterlevnad av dataskyddsförordningen. Exempel på områden som omfattas av revisionen är:

(a) Styrning av dataskydd, och inrättade strukturer, riktlinjer och förfaranden för att säkerställa efterlevnad av dataskyddsförordningen,
(b) Processer för att hantera såväl elektroniska som manuella personuppgiftsposter
(c) Hanteringsprocesser för förekommande begäranden om personuppgifter,
(d) Tekniska och organisatoriska åtgärder som införts för att säkerställa att personuppgifter skyddas på ett adekvat sätt
(e) Personalutbildningar inom dataskydd, dataskyddskontroller och dataskyddsmedvetenhet samt
(f) Datarevision i enlighet med bilaga 2.

Registrerade och begäranden

Dataskyddsförordningen uppställer följande rättigheter för individer:

1. Rätten till information
2. Rätten till tillträde
3. Rätten till rättelse
4. Rätten till radering
5. Rätten till begränsning av behandling
6. Rätten till dataportabilitet
7. Rätten att göra invändningar och
8. Rättigheter gällande automatiserat beslutsfattande och profilering

BUX har infört adekvata system och kontroller för att möjliggöra och underlätta tillämpningen av de åtta rättigheter för registrerade som anges ovan.

När en registrerad inkommer med en förfrågan kommer BUX att inleda en pragmatiskt inriktad beslutsfattandeprocess som leds av dataskyddsombudet.

Såvida inte BUX bedömer begäranden vara överflödiga eller onödiga till sina natur, kommer ingen avgift att uppbäras av de registrerade för prövning och/eller tillmötesgående av sådana begäranden.

Rätten till tillträde

Samtliga begäranden av denna art bör hänskjutas till dataskyddsombudet. BUX kommer att besvara sådana begäranden inom 30 dagars tid.

Den registrerade har rätt att få följande information från BUX:

(a) Behandlingens ändamål
(b) Uppgiftskategorier som behandlas
(c) Mottagare eller kategorier av den registrerades personuppgifter som lagras,;
(d) Den planerade lagringstiden för personuppgifter, och om detta inte är möjligt, fastställelsekriterierna för den perioden och
(e) Huruvida eventuellt förekommande automatiserat beslutsfattande används, t.ex. profilering.

På begäran ska BUX tillhandahålla en kopia av de lagrade personuppgifterna. Om den registrerade efterfrågar ytterligare kopior kan BUX välja att ta ut en skälig avgift för administrativa kostnader. När en begäran görs på elektronisk väg ska BUX tillhandahålla uppgifterna i en vanligt förekommande elektronisk form.

Rätten till rättelse

BUX ska säkerställa att registrerade kan utöva sin rätt att få tillträde till sina uppgifter från företaget samt rätt till rättelse av inkorrekta uppgifter utan otillbörligt dröjsmål.

Rätten till rättelse

BUX ska utan otillbörligt dröjsmål radera personuppgifter om en registrerad på begäran samt när något av de följande skälen föreligger:

(a) när personuppgifterna inte längre behövs för de ändamål för vilka de samlades in, eller på annat sätt behandlades för,

(b) när de registrerade återkallar samtycket som behandlingen utgår ifrån och när det inte finns någon annan rättslig grund för behandlingen,
(c) när den registrerade gör invändningar mot behandlingen och det inte föreligger behöriga skäl som åsidosätter den, eller när den registrerade invänder mot behandlingen
(d) när personuppgifterna har behandlats på ett olagligt sätt,
(e) när personuppgifterna måste raderas i enlighet med en lagstadgad skyldighet i medlemsstatens lagstiftning och/eller
(f) när personuppgifterna har samlats in i samband med ett erbjudande av informationssamhällets tjänster.

Artikel 17.3 b i dataskyddsförordningen anger att rätten till radering upphör att gälla om företaget måste kvarhålla uppgifter för att efterleva övrig gällande lagstiftning. När det gäller BUX utgörs de åsidosättande lagbestämmelserna av kraven som ställs på företag i penningtvättsförordningen om att kvarhålla KYC-uppgifter (Know-Your-Customer) under fem års tid samt journalföringskraven i artikel 16 av MiFID-direktiv II. Det görs en hänvisning till detta i BUX integritetsmeddelande.

Rätten till begränsning av behandling

BUX kommer att sluta behandla personuppgifter under följande omständigheter:

(a) om en individ bestrider riktigheten i personuppgifterna kommer BUX att begränsa behandlingen fram till dess uppgifternas korrekthet har verifierats,
(b) om en individ har gjort invändningar mot behandlingen och koncernen överväger huruvida den har rättmätiga skäl att åsidosätta individens rättigheter eller inte,
(c) om behandlingen befinns vara olaglig och individen motsätter sig radering och istället begär en begränsning, och/eller
(d) om koncernen inte längre behöver uppgifterna men en enskilda person är i behov av dem för att framföra eller försvara sig mot ett rättsligt anspråk.

Rätt till dataportabilitet

Rätten till dataportabilitet gäller endast:

(a) För personuppgifter som en individ har tillhandahållit en personuppgiftsansvarig.
(b) När behandlingen sker i enlighet med individens samtycke eller för avtalsutförande.
(c) När behandlingen genomförs genom automatisk behandling.

För att efterleva detta måste BUX:

(a) Tillhandahålla personuppgifterna i ett strukturerat, allmänt använt och maskinläsbart format.
(b) Tillhandahålla uppgifterna kostnadsfritt (såvida de inte är överflödiga eller onödiga).
(c) Ifall det har efterfrågats och det är tekniskt möjligt ska uppgifterna överföras direkt till en annan organisation.
(d) Göra ett övervägande om individuella rättigheters möjliga skadliga inverkan när uppgifter berör fler än en person.

Samtycke

Samtycke måste lämnas genom en entydig bekräftande handling som anger en frivilligt avlämnad, specifik, informerat och otvetydig anvisning om den registrerades samtycke till att dennas uppgifter behandlas. BUX kommer att införskaffa samtycke genom skriftlig förklaring, på elektronisk väg, eller genom en muntliga förklaring.

BUX efterfrågar, hanterar och registrerar samtycken i enlighet med artikel 5, 6, 7, och 9 i dataskyddsförordningen.

(a) BUX kontrollerar att samtycke är den mest lämpliga grunden för behandlingen,
(b) BUX säkerställer att samtycket lyfts fram och avskiljs från dessa villkor och bestämmelser,
(c) BUX begär ett bekräftande aktivt val,
(d) BUX använder inte förkryssade rutor eller någon annan form av standardsamtycke,
(e) BUX använder sig av ett tydligt och enkelt språk som är lättförståeligt,
(f) BUX specificerar varför uppgifterna behövs och deras ändamål,
(g) BUX tillhandahåller granulära samtyckes alternativ som är avskilda från övriga behandlingsändamål och behandlingsförfaranden,
(h) BUX utser sin organisation, samt eventuella personuppgiftsbiträden hos tredje part som kommer att förlita sig på dennas samtycke,
(i) BUX säkerställer att en individ kan neka att lämna samtycke utan att riskera negativa påföljder, och
(j) BUX undviker att villkora en tjänst med samtycke.

BUX registrerar när och hur företaget införskaffar samtycken från individer. Företaget registerför även den exakta information som ursprungligen tillhandahölls.

Rutiner som BUX kan genomföra för att tillse en lämplig hantering av samtycken inbegriper följande:

(a) BUX granskar regelbundet samtycken för att kontrollera att relationen, behandlingen och ändamålen inte har förändrats,
(b) BUX har inrättat processer för att uppdatera samtycken vid regelbundna tidsintervaller, däribland eventuella föräldrasamtycken (i tillämpliga fall),
(c) BUX överväger att använda sekretessinstrumentpaneler eller andra preferenshanteringsverktyg som en fråga om god praxis,
(d) BUX underlättar för individer att återkalla sitt samtycke vid valfri tidpunkt, och offentliggör hur detta går till väga,
(e) BUX reagerar på återkallade samtycken inom kortast möjliga tid och
(f) BUX bötlägger/straffar inte individer som önskar återkalla sitt samtycke.

BUX uppfattar inte tystnad eller inaktivitet som ett samtycke. När behandlingen av uppgifter har fler än ett syfte kommer BUX att införskaffa samtycken för samtliga ändamål. När en registrerad persons ska ges samtycke till följd av en begäran som har inkommit på elektronisk väg, kommer BUX att tillse att begäran är tydlig, koncis och får inte onödigtvis störa användningen av den tjänst som den avser.

Inbyggt integritetsskydd

BUX har infört tekniska och organisatoriska åtgärder som integrerar skydd i uppgiftsbehandlingen.

Integritetsskydd pch skydd av personuppgifter utgör huvudöverväganden under de tidiga stadierna av varje projekt som BUX genomför.

Exempelvis då:

(a) IT-system utformas för lagring och tillträde till personuppgifter,
(b) lagstiftning, policyer eller strategier som berör uppgiftsskydd tas fram,
(c) ett datadelningsinitiativ inleds och/eller
(d) uppgifter används för nya ändamål.

Beaktanden av integritets- och dataskydd kommer att integreras i BUX riskhanteringsmetoder och -policyer.

Konsekvensbedömning avseende dataskydd (DPIA - Data Protection Impact Assessments)

BUX genomför en konsekvensbedömning avseende uppgiftsskydd när behandlingen sannolik medför en hög risk för enskilda personer, t.ex.:

(a) när en ny teknik införs,
(b) när en profileringsprocess sannolikt kommer att påverka enskilda personer och/eller
(c) vid behandling av vissa kategorier av personuppgifter i större omfattning.

Vid risknivåbedömning ska BUX både beakta sannolikheten för påverkan och hur svår den kan bli för den berörda individen.

BUX säkerställer att vissa personer i företaget har en god förståelse för DPIA.

(a) BUX erbjuder utbildning så att samtlig personal förstår behovet av att DPIA beaktas under ett tidigt stadium av varje plan som inbegriper personuppgifter.
(b) BUX befintliga policyer, förfarande och processer inbegriper referenser till DPIA-krav i tillämpliga fall.
(c) BUX förstår vilka slags behandlingar som fordrar DPIA.
(d) BUX utformar och dokumenterar en robust DPIA-process.
(e) BUX tillhandahåller utbildning om hur DPIA genomförs för berörd personal.

Rapportering av personuppgiftsincidenter

I händelse av en personuppgiftsincident kommer BUX att utan otillbörligt dröjsmål, och där det är möjligt, meddela den behöriga tillsynsmyndigheten senast 72 timmar efter att ha uppmärksammat incidenten. Detta krävs inte när incidenten sannolikt inte kommer att innebära ett hot mot fysiska personers rättigheter och friheter. Om ett meddelande inte lämnas inom 72 timmar, måste BUX tillhandahålla ett giltigt skäl till dröjsmålet. Behöriga tillsynsmyndigheters kontaktuppgifter återfinns i bilaga 1.
Meddelanden från BUX ska åtminstone:

(a) Beskriva vad för slags personuppgiftsincident det handlar om.

(b) Innehålla namn och kontaktuppgifter till den behöriga avdelningen som handlägger incidenten.
(c) Beskriva de sannolika konsekvenserna av personuppgiftsincidenten.
(d) Beskriva de åtgärder som har vidtagits eller föreslagits av BUX för att åtgärda personuppgiftsincidenten, och i tillämpliga fall, åtgärder för att mildra dess potentiella negativa effekter.

Där det är sannolikt att personuppgiftsincidenten kan leda till att fysiska personers rättigheter och friheter hotas ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om incidenten.

Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d, som ovan.

Redovisning

BUX har mindre än 250 anställda och därför är artikel 30 i dataskyddsförordningen tekniskt sett inte tillämplig. Trots detta ska BUX, på grund av andra dataövervakningskrav som föreskrivs i dataskyddsförordningen , samt för bästa praxis, upprätthålla ett register över behandlingsaktiviteter som BUX ansvarar för. Registret ska innehålla följande information:

(a) Personuppgiftsansvariges namn och kontaktuppgifter.
(b) Behandlingens ändamål.
(c) En beskrivning av kategorierna av registrerade och personuppgiftkategorierna
(d) De mottagare som personuppgifterna har eller kommer att lämnas ut till, däribland mottagare i tredje land eller internationella organisationer.
(e) I tillämpliga fall överföringar till ett tredje land eller en internationell organisation, inklusive identifieringen av det tredje landet eller den internationella organisationen.
(f) Om möjligt, de emotsedda tidsfristerna för radering av olika uppgiftskategorier.
(g) Om möjligt, en beskrivning av de tekniska och organisatoriska åtgärder som det hänvisas till i artikel 31.1.

Bux för skriftliga och elektroniska register.

Om den behöriga tillsynsmyndigheten begär det ska BUX omedelbart ställa registren till förfogande.

Klagomålshantering

Efter att ett klagomål har inkommit från en registrerad ska BUX utreda klagomålet internt. BUX ska underrätta den registrerade om ärendets framskridande och senare om resultatet av ärendet. Resultatet måste meddelas inom en rimlig tidsperiod.

Om den registrerade och BUX inte kan lösa klagomålet sinsemellan, kan den registrerade välja att söka upprättelse genom medling, skiljeförfarande eller genom att lämna in ett klagomål till tillsynsmyndigheten. BUX måste informera alla registrerade om deras rätt att inge klagomål direkt till tillsynsmyndigheten.

Bilaga 1

Personuppgifter	Samtliga uppgifter (inklusive åsikter och avsikter) som hänför sig till en identifierad eller identifierbar fysisk person.
Personuppgiftsansvarig	En fysisk eller juridisk person, offentlig myndighet eller annat organ som på egen hand eller gemensamt fastställer ändamålen och förfarandena för att behandla personuppgifter.
Registrerad	Den identifierade eller identifierbara fysiska person som uppgifterna hänför sig till.
Samtycke	Varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.
Internationell organisation	En organisation och dess underställda organ som styrs av folkrätten eller ett annat organ som inrättas genom eller på grundval av en överenskommelse mellan två eller fler länder.
Tillsynsmyndighet	Dataskyddsmyndighet/tillsynsmyndighet för BUX: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Telefon: +44 030 312 31 113 Fax: +44 016 255 24 510 Webbplats: www.ico.org.uk

Bilaga 2

Checklista för dataövervakning

Uppgifter om data som innehas av ayondokoncernen	
Orsaker till att datauppgifterna sparas	
Metoder för att inhämta datauppgifterna	
Det datum datauppgifterna erhölls	
Personer som ansvarar för datauppgifterna	
Datalagring	
Datalagring	
Dataraderingsmetod	