Calibrate Partners

Calibrate Management Ltd
General Data Protection Regulation Policy

1. Introduction

This document represents Calibrate Management Ltd's ("Calibrate Partners" or "Firm") General Data Protection Regulation ('GDPR') Policy. This policy should be read in conjunction with the Firm's Privacy Policy on its website at https://www.calibrate-partners.com/.

The UK General Data Protection Regulation ("**UK GDPR**") is the retained EU law version of the General Data Protection Regulation ('**EU GDPR**' – EU 2016/679). UK GDPR was effectively incorporated into domestic law on the 31 December 2020 by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection Act 2018 ('**DPA**'). In this policy, UK GDPR and EU GDPR, unless stated otherwise, are referred to as 'GDPR'.

Whilst a UK firm is subject to UK GDPR, a UK firm could also be subject to EU GDPR if it handles the data of EU persons (which include EU clients and investors) as per EU GDPR Article 3(2).[1] Hence forth, unless otherwise stated all references GDPR are to both UK and EU GDPR ("GDPR").

GDPR sets requirements on the obligations of firms and the processing of personal data.

This policy also contains the following Annexes:

- **Annex I**: Definitions of some commonly used terms in the UK GDPR
- **Annex II**: Lawfulness of processing
- **Annex III**: Information to be provided to the individual concerned
- **Annex IV**: The six principles of processing personal data

2. The Information Commissioner's Office and ICO Fee

The Information Commissioner's Office ('ICO') is the regulator in the UK in respect to data protection matters. It is a non-departmental public body which reports directly to the Parliament of the United. The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO's website is at: https://ico.org.uk/.

The Data Protection (Charges and Information) Regulations 2018 requires every organisation that processes personal information to pay a fee to the ICO unless they are exempt. Failure to do so will result in a fixed penalty. The Firm is duly registered as a fee payer with the ICO (no. ZA392859). Calibrate Partners LLP is also registered (no. ZB067604). This registration (and payment of fee) is refreshed annually.

3. Applicability to the Firm

As set out in Annex I, **personal data** is any information relating to an identified or identifiable **natural person**. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, a file reference etc. **Processing** includes, but is not limited

[1] EU GDPR Article 3(2): "This Regulation applies to the processing of personal data of data subjects who are in the Union **by a controller or processor not established in the Union**, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union…"

to, collecting, storing and using personal data. For the purposes of the GDPR, the Firm will be primarily a '**data controller**' but will also process personal data.

4. Scope

This document sets out Calibrate Partners' policy for adherence to the GDPR and expected behaviours and applies to all of the Firm's employees and outsourced service providers when personal data is processed. Unless specified to the contrary, any reference to the Firm's processing data can also be read to refer to third parties that process data on behalf of the Firm.

5. Data Collection

Personal data can be collected by Firm in respect of:

- Staff for the purposes of e.g. maintaining employment and sickness records, payroll etc.
- Clients/investors (either actual or proposed)
- Firms providing services to Firm]

All personal data will be collected and processed in accordance with the 'lawfulness of processing' ('legal basis') obligations under the GDPR (see Annex II). Generally, personal data relating to clients/investors and the Firm's employees will be for the purposes of '**legitimate interests**'. However, each case will be considered and determined in line with the 'lawfulness of processing' requirements. Where deemed appropriate e.g. for marketing purposes, then **freely given** specific **consent** will be requested (see Annex II).

For these purposes 'freely given' means that the individual has made a **positive decision** to consent to the processing of their personal data. As such, a pre-ticked box or a general statement etc. that consent is assumed will **not** be deemed to be freely given.

Where the provision of a service is **conditional** on consent being given to the processing of personal data that is **not necessary** for the provision of that service e.g. a requirement to consent to the receipt of marketing material then this will **not** be deemed to be freely given.

Personal data will be retained no longer than is necessary for the purposes for which it processed, subject to any legal or regulatory obligations imposed upon Firm.

6. Informing data subjects

When personal data is collected **directly** from the data subject then that individual will be provided with the information required under the GDPR **at the time the personal data are collected**. This includes, but is not limited to, the purposes of the processing, the legal basis for the processing and whether there is an intention to transfer personal data outside the UK ('third-country') (see Annex III).

Where personal data is collected from someone **other than** the data subject then the latter will be informed of this in accordance with GDPR requirements.

7. Limitation of data collected and purpose

The collection of personal data by Firm] will be limited to that necessary for:

- Providing services, including administration services, to clients/investors
- The general day-to-day running of Firm

- Marketing, including newsletters

8. Sensitive data

The GDPR imposes further requirements on the processing of certain categories of data. Such personal data includes e.g. that revealing ethnic origin, political opinions, religious beliefs, criminal convictions etc.

9. Data transfers

Firm makes use of services provided by various third-parties ('outsourcing').

Due diligence on these providers has been undertaken by Firm] to ensure they are able to meet the standards expected by Firm]. Some of these entities will be involved in the **transfer** of, and the processing of, personal data on behalf of the firm and as such will be '**data processors**'.

For such firms, the due diligence performed by Firm] will include a review of the procedures and processes developed to ensure compliance with the GDPR and the security of personal data processed. In addition, processing of personal data will be governed by a contract whose terms are in accord with that specified in the GDPR.

Any intention to transfer personal data to a **third-country** must be notified to the data subject when the data is collected (see 'Informing data subjects' above). Transfers to a third-country are only permissible in limited situations including:

- Where the UK has determined that third-country offers equivalent protection for personal data ('**adequacy regulations**')
    - This includes countries in the European Economic Area ('EEA');

- If there are no adequacy regulations in relation to the country of data transfer, where the UK has determined the data transfer is subject to '**appropriate safeguards**':
    - Including where the transfers will be subject to UK binding corporate rules (only relevant between members within a group of undertakings or engaged in a joint economic activity); and or
    - Standard contractual clauses issued by the Information Commissioner's Office.

- If there are no adequacy regulations or appropriate safeguards in relation to the country of data transfer, where transfers are covered by '**exceptions**':
    - Including where the individual has explicitly consented to the proposed transfer after being made aware of the potential risks
    - Including where the transfer is necessary for the performance, or conclusion, of a contract

As the UK is now a third country under EU GDPR, any intention to transfer data from the EU to the UK will be treated as such. The EU granted an 'adequacy decision' (similar to adequacy regulations under UK GDPR) to the UK on 28 June 2021, meaning data transfers from the EU to the UK are permissible. The adequacy decision granted under EU GDPR to the UK will expire on 27 June 2025.

10. EU Representative

As required under Article 27 of the EU GDPR the Firm will appoint a representative in a EU Member State if we process or control the personal data of data subjects in the EU.

11. Rights of data subjects

The GDPR provides data subjects with the following rights:

- An individual has the right to be informed about the collection and use of their personal data ('right to be informed'). The Firm has a Privacy Policy on its website for this purpose.
- An individual has the right to confirmation of whether their personal data is being processed and to access and receive a copy of their personal data ('right of access')
- An individual has the right to require 'without undue delay' rectification of inaccurate personal data ('right to rectification)
- An individual has the right to be forgotten, subject to the limited circumstances set out in UK GDPR, including when consent is withdrawn ('right to erasure')
- An individual has the right to restrict processing of personal data in certain circumstances including where the accuracy of the data is contested by the individual ('right to restrict processing')
- An individual has the right to receive personal data concerning the individual and the right to have it transmitted to another data controller ('right to data portability')
- An individual can object to the processing of personal data which is being processed on the basis of 'legitimate interest' unless the controller demonstrates compelling legitimate grounds. Where the processing is for direct marketing purposes then the controller must desist from any further processing for these purposes ('right to object')
- An individual has the right not to be subject to a decision based solely upon automated processing or profiling ('rights related to automated decision making including profiling')

Not all of the above rights will be applicable to Firm's business model e.g. 'profiling' and nor are they absolute e.g. the right to be forgotten will not apply to the extent that the processing is in compliance with a legal obligation. The Firm will consider any such requests from data subjects on a case-by-case basis.

12. Communication with data subjects

Information provided to data subjects, whether as a result of the exercise of a data subject's rights or when informing the individual that their personal data is being collected and its purpose, will be **free of charge**. However, where such requests are excessive or manifestly unfounded then Firm reserves the right to charge a reasonable fee.

13. Data Protection Officer

The appointment of a 'Data Protection Officer' (DPO) is required for those firms that process large amounts of sensitive data or that undertake regular and systematic monitoring of data subjects. As such this obligation does not apply to Firm.

The Firm has appointed the Compliance Officer to:

- Implement GDPR
- Oversee the firm's continuing compliance with GDPR
- Act as the focal point for the notification of any personal data breaches
- Act as the firm's contact person with the ICO

14. Personal Data: The Role of Firm's Employees

Although this Policy is based upon the firm's responsibilities under the GDPR, all members of staff have a role to play in ensuring that Firm] complies with these responsibilities.

UK GDPR provides for the imposition of administrative fines for breaches of its obligations of up to £17.5 million (or 4% of worldwide total turnover if higher).It is also an offence for a person to obtain, disclose or retain personal data without the consent of the controller.

15. Personal Data: Breaches

Any personal data breach(es) must be immediately notified to the Compliance Officer (or to another senior manager or Director in the Compliance Officer's absence). Where possible, such notifications should include:

- The nature of the breach including categories and approximate number of data subjects concerned and data records concerned
- A description of the likely consequences of the personal data breach
- A description of any measures taken, or proposed, to address the data breach and to mitigate its possible adverse effects

The Firm is required to notify the ICO **within 72 hours** of becoming aware of a personal data breach **unless** the breach is unlikely to result to result in a risk to the rights and freedoms of natural persons

Where it is deemed that the personal data breach is likely to result in a **high** risk to the rights and freedoms of natural persons then the data subjects must **also** be notified "without undue delay". Exceptions to this requirement include:

- When the data affected is e.g. encrypted so that the data is unintelligible to persons not authorised to access it
- If it would involve disproportionate effort, in which case a public communication, or similar measure, will be required
- Where subsequent measures are taken to ensure that the high risk to the rights and freedom of data subjects is no longer likely to materialise

The Compliance Officer will document and assess the breach to determine the need to alert data subjects and/or the ICO. An assessment will also be made of the need to inform the FCA as the supervisory authority for Firm's day-to-day activities.

16. Informing the ICO or/and the FCA of a breach

The Firm will report a breach to the ICO as follows:

- By calling the ICO on 0303 123 1113 (Monday to Friday, 9am and 5pm). The ICO will record the breach and give the Firm advice about what to do next.
- Outside business hours, the Firm will online at https://ico.org.uk/for-organisations/report-a-breach/. The webpage also includes an online 'self-assessment' to help determine whether firms need to report to the ICO.

If required / necessary, the Firm will also inform the FCA by submitting a Principle 11 notification (see SUP 15.2 of the FCA Handbook).

Annex I Definitions

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.

Data subject
See 'personal data' below.

Data Controller
The 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; where the purposes and means of such processing are determined by UK law, the controller or the specific criteria for its nomination may be provided for by UK law.

Data portability
A data subject can request receipt of their personal data which they have provided to a controller and has the right to transmit it to another data controller without hindrance (or can request that data be transmitted directly to another data controller where technically feasible).

Data Processor
A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing then it will be considered to be a controller.

Data Protection Impact Assessment
An assessment of the impact of processing operations on the protection of personal data. Sometimes referred to as a 'privacy impact assessment'.

Lawfulness of processing
Personal data must be processed lawfully and in a transparent manner in relation to the data subject. Article 6 of the GDPR (reproduced in **Annex II**) sets out six scenarios, including consent to the processing being given by the data subject, which will comply with 'lawfulness of processing'.

Personal data
Any information relating to an identified or identifiable **natural person** ('**data subject'**). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

A low bar is set for "identifiable"; if anyone can identify a natural person using "all means reasonably likely to be used" the information is personal data, so data may be personal data even if the organisation holding the data cannot itself identify a natural person (e.g. name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address). Online identifiers are expressly called out in Recital 30 with IP addresses, cookies and radio frequency identification tags all listed as examples.

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing
Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Privacy impact assessment
Also known as a 'Data Protection Impact Assessment' (see above).

Special categories of personal data ('sensitive data')
Terms used in the GDPR to refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, also capture genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Article 9 of the GDPR prohibits the processing of such data unless it meets one of the conditions set out therein e.g. **explicit** consent. Article 10 of UK GDPR imposes stricter requirements on the processing of personal data relating to criminal convictions and offences.

Restricted transfers
Under UK GDPR, a restricted transfer is a data transfer from the UK to a third country. Such transfers are restricted unless covered by adequacy regulations, appropriate safeguards or exceptions.

Adequacy regulations
UK GDPR adequacy regulations (under EU GDPR, these are known as 'adequacy decision') set out the legal framework for making permitted transfers of personal data from the UK to third countries. These set out in law that that the legal framework in that third country has been assessed as providing 'adequate' protection for individuals' rights and freedoms for their personal data. For example, countries in the EEA are covered by adequacy regulations under UK GDPR.

Appropriate safeguards

If there are no UK adequacy regulations in relation to the country of data transfer, UK GDPR requires that transfer is made subject to appropriate safeguards, as listed under UK GDPR. These ensure that both parties of the restricted transfer are legally required to protect individuals' rights and freedoms in relation to personal data.

Exceptions

UK GDPR also permits data transfers to third countries if the transfer is covered by an exception, such as the individual has given explicit consent, the transfer relates to a contract or transfer is required to establish, make or defend a legal claim.

Annex II Lawfulness of processing

Processing is **lawful only** if and to the extent that **at least one** of the following applies:

1. the data subject has **given consent** to the processing of his or her personal data for one or more specific purposes;

2. processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

3. processing is necessary for compliance with a **legal obligation** to which the controller is subject;

4. processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;

5. processing is necessary for the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller;

6. processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Annex III Information to be provided to the data subject

Information to be provided where personal data are collected from the data subject (refer to Article 14 for information to be provided where personal data have not been collected from the data subject)

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, **at the time when personal data are obtained**, provide the data subject with **all** of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the **legitimate interests** pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. **In addition** to the information referred to in paragraph 1, the controller shall, **at the time when personal data are obtained**, provide the data subject with the following **further information** necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) ('consent') or point (a) of Article 9(2) ('explicit consent' re 'special categories'), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the

personal data were collected, the controller shall provide the data subject prior to that further processing with

information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information

Annex IV Principles relating to processing of personal data

A data controller is responsible for, and be able to demonstrate compliance with, the following principles.

Lawfulness, fairly and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

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 are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

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.

Accountability

The accountability principle requires data controllers to take responsibility for what they do with personal data and how they comply with the other principles.

Data controllers must have appropriate measures and records in place to be able to demonstrate compliance.