CROSSBRIDGE
CAPITAL

General Data Protection Regulation Policy (GDPR)

Crossbridge Capital (Malta) Ltd, Crossbridge Capital (UK) Ltd, Crossbridge Capital LLP.

Dated 22nd June 2023 (Updated 6th December 2023)

Contents

1. Policy statement

The aim of this policy is to highlight the importance of how Crossbridge Capital (UK) Ltd and Crossbridge Capital LLP, Crossbridge Capital Ltd (Malta) (together "Crossbridge") handle and process personal and sensitive data. On May 25th, 2018, a new European privacy regulation called General Data Protection Regulation (GDPR) came into effect. 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").

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, any non-UK country would be referred to as a third-party (unless stated otherwise) under the UK GDPR; similarly, any non-EU country would be referred to as third-party under the EU GDPR, where specified.

Unless otherwise stated all references GDPR are to both UK and EU GDPR ("GDPR").

1.1 This policy draws attention to our procedure, our responsibility and reiterates on our duty to display **integrity**, **diligence** and **care** (*PRIN 2.1.1*) as a regulated firm as well as comply with all principles set out by the GDPR.

1.2 Data subjects are protected under GDPR, and have a right to how their data is stored, give consent on how their data is processed/handled, and accessing their data. During the course of our activities Crossbridge will collect, store and process personal information about our staff, customers, suppliers and other third parties.

1.3 Any breach of this policy will be taken seriously and may result in disciplinary action by the Crossbridge.

1.4 If you have any doubt as to whether certain information is subject to Data Protection or Group confidentiality restrictions, please consult data protection team.

2. Data Protection Team

2.1 The Data Protection Team comprises of Alpa Patel (Employee Data) and Ashok Bhudia (Data Protection regulation and Client Data). They are leading the data protection practices within the firm as well as reaching and maintaining compliance with GDPR requirements.

2.2 The Data Protection team was established by and reports to Crossbridge's Board of Directors.

2.3 To comply with Article 39, the Data Protection team is responsible for:

- Informing, advising and providing regular data protection reports to the Board of Directors on the application of GDPR requirements;
- Monitoring the firm's compliance with the GDPR;
- Providing training and advice to, and raising the awareness of, the firm's staff, as required; and
- Cooperating and acting as the point of contact with the ICO and other relevant supervisory

[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…"

authorities.

- Reporting major breaches to the ICO

3. About this Policy

3.1 The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, banks, clients, both of the Crossbridge (UK) Ltd and Crossbridge Capital LLP and from within the Crossbridge Group and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 which has now been replaced with EU General Data Protection Regulation (GDPR) 2016 which came into force on May 25th 2018. GDPR imposes restrictions on how we may use that information, within the UK and the European Union and expands to any global company which holds data on UK and EU citizens respectively. This policy mandates our Breach Policy and also our Privacy Policy.

3.2 This policy has been approved by Crossbridge management committee, in consult of our external advisors. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

3.4 Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Team

3.5 If you consider that there has been a breach of policy by yourself or others you should raise the matter with the Chief Executive Officer Tarek Khlat and the Data Protection Team.

3.6 The Employee Consent form, which forms part of each member of staff's contract of employment, sets out the agreed purposes for which Crossbridge processes employee personal data. Employees are required to sign a consent form prior employment authorising Crossbridge and/or an appointed third party in handling and processing their data.

4. Definition of data protection terms

4.1 'Data' is information which is stored electronically, on a computer, or in certain paper-based filing systems.

4.2 'Data subjects' for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK or EEA national or resident. Data Subjects include: employees (permanent, contractors, temps and interns), their family members, prospective or actual clients or investors, job applicants, office visitors, website users or third party suppliers. All data subjects have legal rights in relation to their personal data.

4.3 'Personal data' means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can expand further to a wide range of personal identifiers such as identification number, location data (e.g. IP address) or online identifier. Technology has evolved the way organisations gathers and interprets information about people.

4.4 'Data controllers' are the people who or organisations which determine the purposes for which, and the means of processing data. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

4.5 'Data users' include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

4.6 'Data processors' include any person who has a responsibility of processing personal data on behalf of a data controller. Employees of data controllers are excluded from this definition. Within the terms of agreement with the data controller, and its contract, data processor may decide on the method used to store personal or sensitive data, security surrounding the data, means in which data is transferred and means used to delete or dispose of data. The list is not an exhaustive list of the role or decisions a data processor has.

4.7 'Processing' is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4.8 'Sensitive' or 'special category personal' data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any courtin such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned and processing is necessary for the purpose of carrying out obligations. Read more – ICO website and Official Journal of the European Union

4.9 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

4.10 'Data Breach' means 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.

4.11 The Information Commissioner ("ICO") is the supervisory authority responsible for the enforcement of the GDPR.

5. Territorial Scope

Under the UK GDPR, Article 3 sets out the territorial scope of the regulation which applies to

5.1 The processing of personal data from an establishment of a controller or processor in the UK, irrespective of whether the processing takes place in the UK or not; and

5.2 The processing of personal data subjects based in the UK by a controller or processor not established in the UK in relation to:

a) The offering of goods or services to data subjects in the UK; and

b) The monitoring of the behaviour of data subjects in the UK.

5.3 For best practice, GDPR will be rolled out across Crossbridge group however it does not replace local law or regulations.

Article 3 of the EU GDPR sets out the territorial scope of the regulation which applies to:

5.4 The processing of personal data from an establishment of a controller or processor in the EU, irrespective of whether the processing takes place in the EU or not; and

5.5 The processing of personal data subjects based in the EU by a controller or processor not established in the EU in relation to:

c) The offering of goods or services to data subjects in the EU; and

d) The monitoring of the behaviour of data subjects in the EU.

5.6 For best practice, GDPR will be rolled out across Crossbridge group however it does not replace local law or regulations.

6. Principles of GDPR

Under the *Official Journal of European Union, Regulation (EU) 2016/679 of the European Parliament and of the council, Article 5*, the policy has set out a guide relating to processing of data.

6.1 Fair and lawful processing

6.1.1 The regulation is intended not to prevent the processing of personal data, but to ensure that it is done lawfully, fairly and in a transparent manner without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, who the data controller's representative is (in this case the Data Protect Team), and the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred to.

6.1.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed.

6.1.3 Data about staff may be processed for legal, personnel, administrative and management purposes and to enable the data controller to meet its legal obligations as an employer, for example background checks on employees, monitor their performance; pay salaries and to confer benefits in connection with their employment. Examples of when sensitive personal data of staff is likely to be processed are set out below: (a) information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work; (b) the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation; (c) in order to comply with legal requirements and obligations to third parties; (d) banking information to pay salaries into.

6.1.4 Data about customers, suppliers and other third parties may be processed for the purpose of carrying on the Firm’s business, subject always to compliance with the overarching principles enshrined in the Compliance manual. If you have any doubt as to whether certain information is subject to Data Protection or Group confidentiality restrictions, please consult your Data Protection Team

6.2 Purpose Limitation

Personal data will only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by an authoritative body or to comply with any regulations or legislation. This means that personal data will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

6.3 Adequate, relevant and non-excessive processing

Personal data will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary or excessive for that purpose will not be collected in the first place. Assessment of the relevancy of the data and necessity should be applied before requesting such data from persons.

6.4 Accurate data

Personal data will be accurate and kept up to date. Crossbridge has a legal obligation to ensure that reasonable steps have been taken to ensure that inaccurate data are destroyed or rectified without delay. Accuracy of data should be checked at an agreed interval after the point of collection.

Request for rectification can verbal or in writing pending that reasonable steps has been taken to ensure data is accurate.

6.5 Storage Limitation

Personal and sensitive data should not be stored or filed longer than is necessary for the purpose for which the data are processed. Exemptions are given to storing personal data for archiving purposes in public interest, scientific, historical or statistical purposes subject to implementation of the appropriate authority or regulator, please speak to the appointed Date Protection Officer for clarification of storing data. The body governing the organisation will explicit declare the time limit imposed on personal and sensitive data which must be observed by the firm.

As a firm regulated by the Financial Conduct Authority (FCA), the FCA rules stipulates that a firm must retain all records to be kept of all services, activities and transactions undertaken which are sufficient to enable the competent authority to fulfil its supervisory tasks and ascertain that the firm has complied with all obligations.

Under the new SYSC rule in principle, for data no longer required, records are to be kept for five years, although the FCA reserves the right to extend this to seven years. For information about data retention, contact the Data Protection Team

6.6 Security, integrity and confidentiality

We have a duty to ensure appropriate security measures are in place to protect against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The regulation requires us to put in place procedures and technologies in order to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if there is an SLA between the firm and the third party; if the third party agrees to comply with those procedures and policies; and if an adequate infrastructure has been put in place by the party.

Under the GDPR, transfers to a third-country are only permissible in limited situations including:

- Where the European Commission/UK has determined that third-country offers equivalent protectionfor personal data (‘adequacy decision’)
- Where appropriate safeguards are in place such as appropriate contractual clauses authorised by the supervisory authority
- Where the transfers will be subject to binding corporate rules (only relevant between members within a group of undertakings or engaged in a joint economic activity)
- Where the individual has **explicitly consented** to the proposed transfer after being made aware of the potential risks
- Where the transfer is necessary for the performance, or conclusion, of a contract

To prove that data processors (third parties) have kept our data secure, we will send an e-mail requesting for confirmation that they are complaint with GDPR and have applied any update to the policies to their procedure.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

7. Clear Desk Policy

The Clear-Desk Policy aims to reduce access by unauthorised persons to sensitive and personal information (documents and files) and valuables. By complying with this instruction, you will ensure that information is kept confidential and also prevent the theft of sensitive documents and valuables. As part of training and monitoring, Crossbridge may periodically assess each employee compliance by conducting a random review how data is managed at their after or before working hours.

Crossbridge has installed locks on cupboards, to ensure all private and sensitive information is kept secured overnight and on non-working days. The cupboards can only be accessed by special codes which can be changed, employees are also reminded to not disclose the access codes to any unauthorised person.

8. Lawfulness of Processing

Crossbridge adheres to the terms set out by the GDPR when processing our data. Each data subject is assessed to ensure we are meetings our legal duties, we have approached the matter in a reasonable manner.

a) Data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract, the data subject is a party to such contract or in the course of being subject to the contract;

c) processing of data is necessary for compliance with any legal or regulated obligations to which the controller is subject to;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) 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;

f) processing is necessary for the purpose of 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 a child or a vulnerable person is the subject of such data.

9. Consent

At Crossbridge, we understand that the GDPR sets high standards for consentGiven the legal requirement for consent to be a clear, unambiguous affirmative action, we are ensuring all our collections, handling and processing of data has had explicit consent from data subjects.

Some ways in which Crossbridge have ensured consent, please note this is not an exhaustive list;

- 'Opting-in' for access to our monthly newsletter
- Consent forms for employees
- Terms of business for clients
- Clearly outlining consent in all contracts

We respect data subject's right to withdraw their consent and advise our data subject of such rights.

If you are an employee of Crossbridge and would like to know more about employee's consent please refer to 'Consent to Our Processing of Your Personal Data' for more information, alternatively you can speak to the Data Protection Team.

10. Individual Rights

GDPR provides rights to protect data subjects covered by various Articles in the *Regulation (EU) 2016/679 and UK GDPR*. The rights of individuals are detailed below:

10.1 Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

At Crossbridge, informing data subjects about how to treat, use, handle and process their personal data is an essential part of our operation. *Under Article 13 of the GDPR* we provide data subjects with information ruled out by GDPR (ICO – Right to be informed)

10.2 Right of Access

All individuals have a right to access their personal data, this allows individuals to be aware of the lawfulness of the processing.

Crossbridge provides a copy of information free. Prior information being provided, verification of the person making the request has to be performed under reasonable means.

10.3 Right to Rectification

Crossbridge is obligated under GDPR 'Accuracy of Data' (Art. 5.1.d of the *GDPR)* to have inaccurate personal data rectified, or completed if incomplete.

Please refer to point 6.4 of this policy

10.4 Right to Erasure

Under certain circumstances, data subjects can request a right to be forgotten.

Such request should be bought to the attention of and discussed with the Data Protection Team.

10.5 Right to Restrict Processing

Individuals may have a right to restrict their personal data and limit the way Crossbridge processes their data.

Such request should be bought to the attention of and discussed with the Data Protection Team.

10.6 Right to Data Portability

Individuals have a right under GDPR to reuse their personal data for their personal purposes, however Crossbridge reserves the right under FCA regulation and other legal obligations to access the security of such data portability from one IT environment to another.

All data portability, containing any personal or sensitive details should be password protected using a suitable file format. An additional email containing the password to the file should be sent separately.

If you have any issues over data portability request, discuss this with the Data Protection Team.

10.7 Right to Object

Data subjects have a right to object, or 'opt-out' of direct marketing, promotions, research or processing based upon public task. If such request is made please contact a relevant member of staff to unsubscribe subject.

If you have any query, speak with the Data Protection Team.

10.8 Rights in relation to automated decision making & profiling

GDPR has applied an additional rule to protect individuals from having legal or significant effects on them being based solely on automated decisions or profiling with no human involvement.

At Crossbridge, our data is processed with human involvement, each outcome is discussed and thoroughly analysed by humans. We do not rely solely on automated decisions or internal profiling when processing data.

10.9 Data Subject Requests

Data Subjects can request to exercise the rights set out at 10.1 to 10.8 in any reasonable form of communication.

Data Subjects must provide additional information upon request for the employee or Data Protection Team to successfully verify their identity.

Any Employees who receives a complex request to exercise a right must discuss these requests with the Data Protection Team. A response to each request must be legally provided within 30 days from the receipt of the request from the Data Subject.

There is no administration fee chargeable to the Data Subject or authorised requestor for reasonable requests, in keeping with the principles of the GDPR.

11. Training and Monitoring Policy

This policy is reviewed annually by Crossbridge to ensure alignment with any new rules and make necessary amendments.

Mandatory GDPR training is provided to all employees of the Crossbridge staff. The training must be completed as part of staff induction training within one month of joining the firm and thereafter annually. Crossbridge maintain a record of all training completed by staff.

12. Reporting Data Breaches

Any Employee who suspects that a Personal Data Breach has occurred must immediately notify the Data Protection Team with a description of the incident and when it occurred.

Please refer to the Crossbridge breach policy found on the shared drive.

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 in 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

Ashok Bhudia 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 Crossbridge's day-to-day activities.

13. Consequences of Non-Compliance

Failure to demonstrate compliance with this comply with this Policy, could seriously impact the reputation of Crossbridge Group. If the Crossbridge Group is found to be in breach of the GDPR, we can be fined up to 4% of annual global turnover or €20/£17.5Million (whichever is greater).

14. Version control and Amendments

Written By	Date	Details of amendments	Version no.
Elizabeth Anjorin	10/04/2018	Original	001
Reviewed by: External Compliance and Katie Schouten	25/05/2018		
Reviewed by Compliance Officer and Consultants	22/05/2020	1. Added transfers to 3rd country section 2. Added ICO notification details and process	
Reviewed by Compliance Officer and Consultants	16/06/2021	3. Amended staff details to include Ashok Bhudia and Alpa Patel.	
Reviewed by Compliance Officer and Consultants	TBC	4. Updated to reflect UK onshoring of EU GDPR following Brexit	

Approved by	Date	Method of Approval
Tarek Khlat		Original
Tarek Khlat	16/06/2021	Review of staff amendments.
Tarek Khlat	15/04/2024	Review of Optima Amendments (Brexit).