Bryan Cave Leighton Paisner LLP

Group Policy

3837672

Title:	**Data Privacy Policy**
Purpose:	To ensure compliance with applicable data privacy laws
Geographical scope:	Abu Dhabi, Belgium, China, Dubai, England, France, Germany, Hong Kong and Singapore offices (excluding non-EU legacy BC offices)
Staff scope:	Applies to all Partners and Staff
Policy Owner:	Compliance Officer for Data Protection
Translated versions:	French [#]; German [#]; and Russian [#];
Issued:	21 May 2018
Version:	1
Last Reviewed:	

Change History:

Version	Date	Change	Approver

Contents

1 INTRODUCTION

1.1 This policy sets out how the Firm will Process Personal Data, and the requirements on Partners and Staff when they handle Personal Data as part of their role. It applies to all Partners and Staff at the Firm, and to all Personal Data Processed in the course of business (regardless of the media on which that data is stored or whether it relates to past or present clients, partners, staff, suppliers, website users or any other Data Subject).

1.2 The Compliance Officer for Data Protection, Regional Privacy Officers and local Data Protection Officers (together the **"Privacy Officers"**) are responsible for overseeing compliance with this policy and the Data Privacy Laws and developing any related guidance. Please contact any of the Privacy Officers with any questions about the operation of this policy or the Data Privacy Laws.

1.3 The Firm recognises the importance of complying with the Data Privacy Laws which regulate our Processing of Personal Data. Protecting the confidentiality and integrity of Personal Data maintains confidence in the Firm and contributes to successful business operations.

1.4 The Firm is exposed to potential significant fines for failure to comply with the provisions of the Data Privacy Laws - including fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, under the GDPR. In addition, any breach is likely to have an adverse impact on the Firm's business and reputation.

1.5 Compliance with this policy is mandatory. All Partners and Staff at the Firm ("you", "your") must read, understand and comply with this policy when Processing Personal Data on the Firm's behalf and attend training, when requested to do so, on its requirements.

1.6 Any breach of this policy may result in disciplinary action.

2 THE FIRM'S POLICY

2.1 The key requirements which you must comply with are set out below. The regulatory rules and further details about these policy requirements are set out in the remaining sections of this policy. Although this policy is focussed on the requirements of GDPR, the policy requirements in it reflect the common requirements of applicable Privacy Laws which apply to the BCLP Group.

When can Personal Data be Processed?

2.2 You must only Process Personal Data for a legitimate business purpose and when required by your job duties. Under no circumstances can Personal Data be Processed for any reason unrelated to your job duties.

How must Personal Data be Processed?

2.3 Personal Data must be Processed in accordance with applicable Data Privacy Laws and the Firm's internal policies. In particular:

2.3.1 You must only collect specific Personal Data which is required for relevant business purposes – Personal Data cannot be collected just in case it might be needed in the future.

2.3.2 You must only use Personal Data for the relevant business purpose for which it was collected/received. Do not use Personal Data for new, different or incompatible purpose without approval from a Privacy Officer.

2.3.3 You must keep Personal Data confidential and secure, and treat it in accordance with its level of sensitivity. Other than work details (such as name, job title, employer and office contact details - which are generally in the public domain and can be saved in our accessible internal systems, such as Interaction, Personal Data must only be shared or transferred to those who have a need to know for the relevant business purpose, and where they are subject to appropriate safeguards. In particular:

(a) Documents containing Personal Data must be saved in the firm's Document Management System with appropriate access rights put in place (including use of an information barrier where appropriate), with hard copies locked away. They should not be saved in the S drive or otherwise be publicly accessible to everyone at the Firm. This is especially important for HR data, Office of the General Counsel data, and Private Client and Employment/Labour Group files.

(b) Personal Data must only be transferred to persons outside of the Firm (especially those located in other countries) where: (i) we have a legitimate reason and legal basis to do so; (ii) the sharing of the data is something the Data Subject would not be surprised about/would not object to (if you think they would be surprised/object, you must inform a Privacy Officer before transferring the data); and the intended recipients of the Personal Data are subject to appropriate safeguards (including the use of EU standard contractual clauses for transfers of data outside of the EEA, unless the Data Subject has provided Explicit Consent or a Privacy Officer has authorised the transfer).

2.3.4 If you become aware that Personal Data is inaccurate, irrelevant, outdated, or no longer needed, you must inform the relevant BCLP manager responsible for the data so that it may be amended, updated, anonymised or deleted as appropriate, subject to our legal and/or regulatory obligations.

2.3.5 You must comply with the Firm's data retention guidelines in respect of the retention and deletion of Personal Data.

Can we Process Sensitive Personal Data?

2.3.6 You can only Process Sensitive Personal Data where this is necessary for an HR, legal, regulatory or compliance purpose, or for a client matter on which we are currently acting; or in a medical emergency. The Processing of Personal Data relating to criminal offences and convictions in particular is deemed especially sensitive, and must only be Processed under the oversight of the Privacy Officers.

What about direct marketing?

2.3.7 All direct marketing (e.g. client marketing mailers) must be managed/approved by the Marketing team.

2.3.8 If a client (or other Data Subject) complains to you about the marketing communications (including calls and emails) that they are receiving or otherwise objects to direct marketing, the Marketing team must be immediately notified.

How does this policy affect any new business initiatives or IT systems my department is looking at adopting?

2.4 You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data.

2.5 You should conduct a Privacy Impact Assessment (and discuss your findings with the relevant Privacy Officer) when implementing system or process changes involving the Processing of Personal Data including: (a) use of new or changing technologies (programs, systems or processes); (b) Automated Processing including profiling and ADM; (c) large scale Processing of Sensitive Data; and (c) large scale, systematic monitoring of Data Subjects.

When must I speak to a Privacy Officer?

2.6 You must immediately: (a) notify a Privacy Officer, the Office of General Counsel, the CIO and/or the IT Director of any knowledge or suspicion of a Personal Data Breach or of a breach of this policy. You should email databreach@bclplaw.com; and (b) forward any Data Subject request (including a request to access, rectify or delete their Personal Data) that you receive to a Privacy Officer.

2.7 The Privacy Officers should also be promptly contacted if you: (a) are unsure of the lawful basis upon which you are relying to process Personal Data (including the specific legitimate interests of the Firm where applicable); (b) need to rely on Consent and/or need to capture Explicit Consent; (c) need to draft Privacy Notices; (d) are unsure about the retention period for the Personal Data being Processed; (e) are unsure about what security or other measures you need to implement to protect Personal Data; (f) are unsure about the basis to transfer Personal Data outside the EEA; (g) are engaging in a significant new, or change in, Processing activity which is likely to require a PIA or plan to use Personal Data for purposes other than what it was originally collected for; (h) plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making; (i) need help complying with the Data Privacy Laws when carrying out direct marketing activities; or (j) need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our suppliers); or (k) need to Process Sensitive Personal Data.

Am I required to attend data privacy training?

2.8 You must complete all mandatory data privacy related training.

3 PERSONAL DATA PROTECTION PRINCIPLES

3.1 We adhere to the principles relating to Processing of Personal Data set out in the Data Privacy Laws including the GDPR which essentially require Personal Data to be:

(a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

(d) accurate and where necessary kept up to date (Accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

(f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

(g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

(h) made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

3.3 To achieve compliance, the Firm will ensure that:

(a) Privacy Officers and other specialist staff are appointed to provide advice and assistance on issues arising under the Data Privacy Laws;

(b) everyone managing and handling Personal Data understands that they are responsible for following best practice guidance in relation to data privacy;

(c) everyone managing and handling Personal Data is appropriately trained and supervised;

(d) queries about handling Personal Data are promptly and courteously dealt with;

(e) procedures for handling Personal Data are clearly described; and

(f) a regular review is made of the way Personal Data is managed.

3.4 The responsibility for compliance primarily rests with the Firm; however, all Partners and Staff have an individual responsibility to ensure compliance.

3.5 **Lawfulness, fairness, transparency**

3.5.1 Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

3.6 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. These specified lawful purposes are not intended to prevent Processing, but to ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

3.6.1 Under GDPR, the specified lawful purposes include:

(a) the Data Subject has given Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue the Firm's legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

3.6.2 Processing of Sensitive Personal Data is subject to enhanced restrictions and additional specified lawful purposes for Processing, which include:

(a) the Data Subject has given Explicit Consent;

(b) the Processing is necessary for the purposes of employment laws;

(c) to protect the Data Subject's vital interests (in situations where the Data Subject is physically and legally incapable of giving consent);

(d) the processing is necessary to pursue or defend a legal claim; or

(e) the processing is necessary for medical diagnosis or to assess the working capacity of the Data Subject (and is carried out by a medical professional).

3.6.3 You can only Process Sensitive Personal Data where this is necessary for an HR, legal, regulatory or compliance purpose, or for a client matter on which we are currently acting; or in a medical emergency. The Processing of Personal Data relating to criminal offences and convictions in particular is deemed especially sensitive, and must only be Processed under the oversight of the Privacy Officers.

3.6.4 The Firm has to identify and document the legal ground being relied on for each Processing activity.

3.7 Although applicable Data Privacy Laws in relevant jurisdictions outside the EEA adopt similar purposes of processing, there may be circumstances where some of these lawful purposes are modified by local legislation. Further information can be sought from your Regional Privacy Officer. In the case of any inconsistency, the local legislation will prevail.

3.7.1 The Data Privacy Laws require Data Controllers to provide detailed, specific information to Data Subjects about how we Process their Personal Data (including for what purpose). This information is set out in our privacy notices:

(a) Full Privacy Notices:

(i) Our website Privacy Notice applies to clients and third parties, and is available at http://www.blplaw.com/legal/privacy-notice; and

(ii) Our Staff and Partners Privacy Notice;

(b) 'Primary layer'/just in time' Privacy notices - we have also put in place shorter, summarised privacy notices in our: (i) email, fax, invoice and letterhead footers; (ii) client terms of business and supplier contracts; (iii) Staff contracts; and (iv) on our websites and extranets, which provide the key privacy information, and link/refer to the Full Privacy Notices.

3.8 **Purpose limitation**

3.8.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

3.8.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

3.9 **Data minimisation**

3.9.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

3.10 You must only Process Personal Data where performing your job duties requires it and any data collected must not be excessive. You cannot Process Personal Data for any reason unrelated to your job duties. Doing so without permission from the Data Controller (via one of the Privacy Officers) **is a criminal offence**.

3.10.1 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with any data retention guidelines issued by the Firm.

3.11 **Accuracy**

3.11.1 Personal Data must be accurate, relevant to the purpose for which it is collected and, where necessary, kept up to date.

3.11.2 If you become aware that Personal Data is inaccurate, irrelevant, outdated, or no longer needed, you must inform the relevant manager responsible for the data so that it may be amended, updated, anonymised or deleted as appropriate, subject to our legal and/or regulatory obligations.

3.12 **Storage limitation**

3.12.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

3.12.2 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected including for the purpose of satisfying any legal, accounting or reporting requirements.

3.12.3 You must comply with any data retention guidelines issued by the Firm to ensure that Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

3.13 **Security integrity and confidentiality**

3.13.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

3.13.2 The Firm has implemented and will maintain safeguards appropriate to its size, scope and business, our available resources, the amount and sensitivity of the Personal Data that we own or maintain on behalf of others and identified risks. We

will exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

3.13.3 We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

3.13.4 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-parties who have adequate security measures in place and who agree to comply with any specific policies and procedures, as requested**.**

3.13.5 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

(b) integrity means that Personal Data is accurate and suitable for the purpose for which it is processed;

(c) availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our Information Security programme, and related policies and procedures.

3.14 **Transfer limitation**

3.14.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

3.14.2 Intra-group data transfers are governed by an intra-group agreement. For other transfers outside the EEA, for example, to suppliers, you may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which the Personal Data is to be transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms (currently Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay);

(b) appropriate safeguards are in place such as standard contractual clauses approved by the European Commission;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR (check with one of the Privacy Officers) and, in some limited cases, for our legitimate interest.

3.14.3 Similar restrictions apply under other applicable Data Privacy Laws. Where you are transferring Personal Data cross-border from a non-EU jurisdiction, please speak with a Privacy Officer for further guidance.

4 SHARING PERSONAL DATA

4.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

4.2 You may only share the Personal Data we hold with another employee, agent or representative of the Firm if:

(a) the recipient has a job-related need to know the information; and

(b) the transfer complies with any applicable cross-border transfer restrictions.

4.3 You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

5 DIRECT MARKETING

5.1 We are subject to certain restrictions when marketing to our clients and other third parties. For example, for some types of Data Subjects and/or in certain jurisdictions, prior consent is required for electronic direct marketing by email. In addition, the right to object to direct marketing must be explicitly offered to the Data Subject.

5.2 A Data Subject's objection to direct marketing must be promptly honoured. If a client (or other) opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

5.3 All direct marketing must be managed/approved by the Marketing team.

6 REPORTING A PERSONAL DATA BREACH

6.1 Under GDPR, Data Controllers are required to notify certain Personal Data Breaches to the applicable Regulator(s) and, in certain instances, to the affected Data Subject(s). Other applicable Data Privacy Laws either require or encourage notification.

6.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable Regulator where we are legally required to do so.

6.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact a Privacy Officer, the Office of General Counsel, the CIO and/or the IT Director. You should email databreach@bclplaw.com.

7 DATA SUBJECT'S RIGHTS AND REQUESTS

7.1 Data Subjects have rights when it comes to how we handle their Personal Data. Under GDPR, these include rights to:

(a) withdraw Consent to Processing (where our Processing is based on Consent);

(b) receive certain information about the Data Controller's Processing activities – we include this information in our Privacy Notices;

(c) request access to their Personal Data;

(d) object to our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to a Supervisory Authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

7.2 For further details about these rights under GDPR (including their limitations), please see the European Commission's website on https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_e or speak to a Privacy Officer.

7.3 Although applicable Data Privacy Laws outside the EEA afford similar rights, there may be circumstances where some of these rights are modified by local law. Further information can be sought from your Regional Privacy Officer. In the case of any inconsistency, the local legislation will prevail.

7.4 There a strict time limits for responding to Data Subject requests. You must immediately forward any Data Subject request you receive to your Regional Privacy Officer who will verify the identity of the individual requesting data under any of the rights listed above (and ensure that Personal Data is not disclosed to third parties without proper authorisation).

8 ACCOUNTABILITY

8.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

8.2 Under GDPR the Firm is required to keep full and accurate records of all its data Processing activities. You must contact a Privacy Officer in relation to any new (or significant changes to) Processing activities to ensure that our records are kept up to date.

8.3 The Firm is required to ensure all its Staff and Partners are adequately trained to enable them to comply with the Data Privacy Laws. You must complete all mandatory data privacy related training.

8.4 The Privacy Officers will regularly review all systems and processes to ensure they comply with the Data Privacy Laws and this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

8.5 Under GDPR and certain other applicable Data Privacy Laws, we are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles. You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data.

8.6 You should conduct a PIA (and discuss your findings with a Privacy Officer) when implementing system or process changes involving the Processing of Personal Data including:

(a) use of new or changing technologies (programs, systems or processes);

(b) Automated Processing including profiling and ADM;

(c) large scale Processing of Sensitive Data; and

(d) large scale, systematic monitoring of Data Subjects.

A PIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

Click here for a template PIA.

9 CHANGES TO THIS POLICY

9.1 This policy will be reviewed annually to ensure that it reflects current legislation and regulations.

9.2 This policy does not override any applicable national data privacy laws and regulations in countries where the Firm operates.

GLOSSARY

"**Automated Decision-Making**" or "**ADM**"	means when a decision is made solely on the basis of Automated Processing (including profiling), and that decision produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
"**Automated Processing**"	means any form of automated Processing of Personal Data, where that Personal Data is used to evaluate certain personal characteristics and related aspects of an individual – in particular to analyse or predict the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
"BCLP Group"	the Firm and its affiliated and associated firms and entities
"**Compliance Officer for Data Protection**"	The person appointed by the Firm to lead the Privacy Team.
"**Consent**"	means an agreement which is freely given, specific and informed. Consent must be in the form of an unambiguous indication (by way of a statement or a clear positive action), of the individual's wish to signify agreement to the Processing of Personal Data relating to them.
"**Data Controller**"	means the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. The Firm is the Data Controller of all Personal Data relating to our staff, and all other Personal Data used by it for business purposes.
"Data Privacy Laws"	means all applicable data protection and privacy laws, including the GDPR
"**Data Subject**"	means a living, identified or identifiable individual whose Personal Data we hold. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

"**EEA**"	Means the European Economic Area as constituted at the date of this policy by the 28 member states of the European Union, together with Iceland, Liechtenstein and Norway.
"**Explicit Consent**"	is consent which is given by a very clear and specific statement (that is, not just action).
"Firm"	The BCLP Group entities which provide legal services, excluding the non-EU legacy BC offices
"**General Data Protection Regulation**" or "**GDPR**"	means the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.
"**Personal Data**"	Means: (i) any information identifying a Data Subject; or (ii) information relating to a Data Subject whom we can identify (directly or indirectly) from that data alone or in combination with other identifiers that we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
"**Personal Data Breach**"	means any act or omission that compromises: (i) the security, confidentiality, integrity or availability of Personal Data; or (ii) the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
"**Privacy by Design**"	means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
"**Privacy Impact Assessment**" or	means tools and assessments used to

"**PIA**"	identify and reduce risks of a data processing activity. PIAs can be carried out as part of Privacy by Design and should be conducted for all major system or process implementations/changes involving the Processing of Personal Data.
"**Privacy Notices**"	means the relevant notices issued by the Firm, which explain to Data Subjects how we collect and use their Personal Data. Privacy Notices may take the form of general privacy statements applicable to a specific group of individuals (for example, the Firm's staff privacy notice or the website privacy notice) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.
"Privacy Team"	means the group of individuals who have primary responsibility for overseeing compliance with this policy and applicable Data Privacy Laws.
"**Processing**" or "**Process**"	means any activity that involves the use of Personal 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, systemising, storing, anonymising, disclosing, erasing or destroying it by automated or non-automated means. Processing also includes transmitting or transferring Personal Data to third parties or giving access to Personal Data.
"Regional Privacy Officers"	means the persons (whether formally appointed under the GDPR as a Data Protection Officer or otherwise) who lead the Privacy Team with responsibility for data protection compliance across the BCLP Group.
"**Sensitive Personal Data**"	means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.