BCLP. Client Intelligent

PRIVACY NOTICE

Bryan Cave Leighton Paisner (the " BCLP Group", "we", or "us") respects your privacy. This Privacy Notice ("Notice") explains how we use ("Process") your personal information (including personal information that you provide to us about other persons) (together, "Personal Information"). It also explains your privacy rights and how you can exercise them.

Bryan Cave Leighton Paisner LLP, the limited liability partnership established under the law of the State of Missouri ("BCLP US") and Bryan Cave Leighton Paisner LLP, the limited liability partnership registered in England & Wales under number OC315919 and with a registered office at Governor's House, 5 Laurence Pountney Hill, London EC4R 0BR, UK ("BCLP UK") are responsible (i.e. they are the 'Data Controllers') for the Personal Information they respectively collect about you (including through the www.bclplaw.com website). When you provide Personal Information to another BCLP Group entity ("BCLP Firm"), as named in the relevant email sign-off, letterhead or business card of your BCLP contact, that firm will be the Data Controller for that Personal Information.

The type of Personal Information we collect and how we Process it will vary depending on the relationship we have with you (e.g. whether you are a client, a supplier, applying for a role with us, or someone else) and the context - see the relationship-specific sections of this Notice for further details.

Please note in particular that:

1. As a law firm, we are required by applicable rules to undertake appropriate: (a) pre-hiring (and, for higher risk roles, periodic) checks of our Partners, lawyers and other employees; and (b) vetting of other third parties (including of our clients and related parties, and of suppliers). These checks/vetting will involve undertaking social media screening and the collection of criminal and regulatory records and legally permitted;

2. We monitor and record electronic communications to ensure compliance with applicable rules and law and our internal policies, and for business continuity purposes;

3. We use cookies, web beacons and similar technologies (together "Cookies") on our websites and in marketing emails. Where Cookies are placed by third parties (such as Google Analytics), your Personal Information may: (a) be processed by that third party in another jurisdiction for its own purposes; and (b) accessible to local government authorities. For further details, please see our Cookies Policy; and

4. As an international business, we will share certain Personal Information across the BCLP Group and with select third parties subject to appropriate safeguards.

We will publish updates to the Notice on this website. Where we hold or Process your Personal Information, we will also take appropriate measures to inform you of any amendments which have a material impact on you and your ability to exercise your privacy rights.

If you have any questions regarding our processing of your Personal Information or would like to exercise your privacy rights, please email us or see the 'Contacts and Other Important Privacy Information' section of this Privacy Notice page.

FURTHER INFORMATION FOR CLIENTS

The BCLP Firm you engage to provide legal services to you (as named in our engagement letter/confirmation email) is the Data Controller in respect of Your Personal Information.

To the extent that the engagement terms agreed with you include Data Processor requirements in respect of our use of Your Personal Information which conflict with the provisions of this Notice, those requirements will apply in respect of Your Personal Information which is collected and/or used by us solely as a Data Processor.

Subject to limited exceptions individuals have the right under applicable privacy laws to access and correct their Personal Information. If we have to provide Information in response to a request from someone whose data we hold in connection with your current or past matters (typically referred to as a 'Subject Access Request'), we will discuss this (and any associated costs) with you as appropriate.

Last updated: 21 March 2025 (minor updates)

HOW WE COLLECT YOUR PERSONAL INFORMATION

We collect Personal Information to provide our legal services, for legal and regulatory purposes and to manage our business and relationships. For further details, please see the 'Use of your Personal Information' section of this Notice below.

We collect your Personal Information in the following ways:

Directly from you	For example, when you engage us for our legal services or contact us.
Public information	For example, on your employer's website; public social and networking sites;

	the press; and relevant electronic data sources.
Information from third parties	For example, by our or your clients; agents; suppliers; advisers; consultants, lawyers and other professional experts; counterparties; previous, current and future employers; complainants, correspondents and enquirers; regulators and public authorities; relatives; and other persons.
Information collected through our websites	We use Cookies which collect your IP address and certain other information from you when you visit our websites or click on links in certain marketing emails. For further details, please see the 'Marketing and cookies' section below.

Sometimes the provision of your Personal Information to us by third parties will be unsolicited and/or provided in confidence (for example, reports made to us by regulators and other persons) and we will be unable to notify you of this. In all cases, we shall take such necessary steps to ensure that Personal Information is obtained and used in a fair and lawful way.

THE TYPES OF PERSONAL INFORMATION THAT WE COLLECT

The categories of Personal Information we collect will vary, depending on our specific relationship with you, and the context.

We will not be able to further our relationship with you (for example, to provide you with legal services if you are a client, recruit you, or engage you if you are a potential supplier) without certain Personal Information. We will inform you at the relevant time if this is the case.

We operate security and business continuity systems and procedures which involve the Processing of Personal Information where appropriate and applicable local law permits us to do so.

We will only request sensitive Personal Information, such as diversity and health data, and details of offences, regulatory action and related proceedings ("Sensitive Information") where necessary and where legally permitted, and will put in place enhanced safeguards to protect such Sensitive Information. Types of Personal Information and Sensitive Information which we will typically collect include:

Type of Data	**Examples**	**Context**
Work and bank account details	Name, job title, work address, office email and telephone number, bank account details	We will usually need this information for clients and suppliers.

Type of Data	Examples	Context
Identification details	Your passport/ID and proof of address	We will typically ask for this as part of our client and supplier due diligence, and pre-hiring checks. Please see the relevant relationship-specific section below for further details.
Personal contact details	Your home address, mobile number and personal email address	We will usually ask for this if you: (a) are applying for a position; (b) do not currently have office/work contact details; or (c) are a member of our alumni program.
Your activity on our websites	Including your IP address, web browser details and related information (e.g. your location, company name and industry, where this is identifiable from public sources based on your IP address), details of the webpages you visit, articles you download and the website you came to us from	These are collected through Cookies and other electronic logs which are created when you visit our websites. For further details, please see the 'Marketing and cookies' section below
Calls to our UK switchboard	Call recordings	In the UK, calls to our switchboard are directed to a supplier, who records the calls for training and quality purposes.
CCTV Images	Images captured by certain of our offices' CCTV cameras	In those offices where applicable local law permits us to, these are monitored by our security team based in London and other jurisdictions, and images will be recorded for security purposes and for the prevention of crime.
IT logs and online identifiers	Incoming and outgoing email, telephone and similar communications records; and other IT logs	Our IT systems automatically filter email and instant messaging communications for viruses and compliance with our internal policies. Usage of our IT systems (and access to secure office areas) is also automatically logged. Where appropriate and local law permits us to, we will monitor such communications and logs to ensure compliance with applicable rules and law and our internal policies, and for business continuity purposes.

Type of Data	Examples	Context
Sensitive Information	Diversity and health data and details of criminal offences, regulatory action and related proceedings. The definition of Sensitive Information varies from jurisdiction to jurisdiction (e.g. social security numbers are Sensitive in the United States, France and Belgium, and identity cards in Hong Kong and Singapore. In Saudi Arabia, official identity documents, credit data and data indicating that one or both parents are unknown are Sensitive, and biometric and genetic data are also deemed Sensitive in certain jurisdictions.	In those offices where applicable local law permits us to, this data is typically collected as part of our pre-hiring and ongoing checks, inclusivity and diversity surveys, and for regulatory, insurances and health and safety purposes. Sensitive Information may also be inadvertently disclosed to us, for example, if you provide us with your dietary requirements for the purpose of a business meal (which may give an indication of your religion or health), or where you make such information public (including in your public social media).

FURTHER INFORMATION FOR CLIENTS

If applicable and in addition to the information listed above, if you are a client, the amount of your Personal Information which we collect will typically be relatively limited. In certain circumstances, we will need to know more information about you and related persons. For example, where we are acting as a trustee or otherwise for you as an individual in respect of personal tax matters, wealth preservation and/or divorce proceedings we may need detailed Personal Information about your relatives (next of kin, dependents, beneficiaries, guardians and associates) and personal assets, amongst other things. Your matters may also involve Sensitive Information, for example where we are defending you from criminal prosecution, or on litigation/regulatory investigations or employment matters.

Under applicable anti-money laundering laws we have to obtain and hold satisfactory evidence of the identity of our clients and sometimes of related persons (including shareholders, beneficial

owners, management, directors and officers), such as your/their passport/ID, proof of address and sources of wealth. Sometimes we will need to: (a) see original documents; (b) check the Personal Information you provide; (c) use Your Personal Information to check your identity and background through electronic data sources; and (d) ask you for up-to-date evidence of identity.

If you do not provide us with this Personal Information, or if it is not satisfactory, we may not be able to act, or to continue to act, for you.

We are also required to report to the regulatory authorities suspicions of money laundering and terrorist financing. This will involve the Processing of Sensitive Information where applicable, such as details of criminal allegations and/or findings, regulatory action, and related proceedings which are reported in the press and electronic/other data sources. For further details, please see the "Who will Your Personal Information be shared with?" section of this Notice below.

FURTHER INFORMATION FOR APPLICANTS FOR A ROLE

Our online recruitment portals

We use two suppliers to manage our respective online recruitment portals. When you apply for a role through our careers website, your Personal Information is stored on our behalf (and managed by us) in the UK or the United States, as applicable. We will also transfer your Personal Information to our systems.

In the UK, we outsource certain other functions to specialist suppliers where needed (for example for graduate contextual recruitment purposes; and to process brand ambassador roles), who will also have access to certain of your Personal Information. You will be informed at the relevant time if your application involves such services.

All suppliers used in our recruitment process are subject to information security and compliance due diligence checks, and contractual confidentiality obligations.

Pre-hiring checks

As a law firm, we are required to undertake appropriate pre-hiring (and, for higher risk roles, periodic) checks. These are undertaken once you accept an offer, and are subject to strict controls. We will only undertake checks which are legally permitted in the relevant jurisdictions.

If you do not provide the required Personal Information (or your consent to Personal Information held by third parties being disclosed to us where applicable), we will not be able to hire you.

We use external providers to undertake international professional verification, background and social media checks (including through electronic data sources, and directly with your current/previous employers, professional bodies/regulators and other third parties where appropriate) on our behalf. We will also undertake certain verifications ourselves.

We adopt a risk-based approach to our pre-hiring checks, which will include verifying your identity; nationality/right to work; academic/legal qualifications and experience; potential client conflicts of interests; and your regulatory history. The types of Personal Information which will typically be collected as part of our checks includes:

Personal details	Such as copies of your passport and/or ID card; your driving licence (where required in connection with your role); your home contact details; personal address history and proof of address. In the US we will also undertake a Social Security Trace Report.
Right to work	Including your nationality and any required work permit.
Professional and academic details	Including your educational, academic and vocational (e.g. LPC/BVC) certificates, admission certificate and practising certificate or registration/authorisation. We will also review your current employer's website and your LinkedIn profile to confirm your current position where appropriate.
References from the referees you provide to us as part of your application	Including confirmation of your work history, competencies and previous salary where appropriate.
Regulatory history	Including details of any regulatory investigations and sanctions imposed by a professional body or regulatory authority.
Public social media content	Where legally permitted the Firm will also conduct checks of your public social media (such as LinkedIn, X (Twitter), Facebook and Instagram) for inappropriate, offensive or illegal/discriminatory content and interactions.

Where we are legally permitted to do so, these checks will involve the Processing of Sensitive Information - for example, by asking you if there are any criminal offences or regulatory decisions, orders, or related factors (including details of any judgments involving the payment of money) which would affect our ability to hire or remunerate you for the particular role; or where you have made Sensitive Information public (including in your social media).

Enhanced pre-hiring checks

In the US and/or if you will have access to especially sensitive and/or confidential information as part of your role (for example if you are a fee earner, business development consultant, or in the Technology, Finance or Office General Counsel departments) and for more senior positions, we will undertake enhanced checks to ensure your trustworthiness, integrity and reliability for the role, and to confirm that there are no regulatory prohibitions on us hiring or remunerating you. Depending on your specific role, location and seniority these will include:

- Electoral roll check
- Credit and bankruptcy checks
- Adverse media checks
- Compliance and sanctions checks
- Directorship disqualification checks
- Basic criminal records checks

In addition:

- For roles in the UK and certain other offices we will also ask you to complete a basic medical questionnaire (and to undertake an occupational health assessment where appropriate) to determine if any work place adjustments are needed. The medical results are reviewed by our specialist healthcare provider, and will not be disclosed to us unless you consent – but if you do not consent, we will not be able to put adjustments in place for you.
- Where this is required by a regulator for your admission as a lawyer, your registration as a foreign lawyer, the processing of a work permit or for other regulatory purposes, it will be necessary for you to request a certificate of good standing from your home regulator; and/or to agree to enhanced criminal records checks being undertaken by the relevant regulator/ public/governmental authority, and to copies/the results being disclosed to us.
- In the US, UK and other offices where this is permitted under applicable local law, we will ask you to complete a diversity questionnaire as part of your job application (and, if successful, your onboarding) for equal opportunities monitoring and diversity reporting purposes. Completion of the diversity questionnaire is voluntary - and if you decide not to do so, this will not impact your application or your employment. Unless you specifically agree otherwise, your diversity data will only be shared in an aggregated format which cannot identify you.

For graduate roles in the UK and Asia, we will also invite you to complete a socio-economic questionnaire as part of your application for contextual recruitment purposes. Selecting the 'prefer not to say' option where applicable will not impact your application or your employment - but without your answers, we will not be able to apply contextual recruitment or take any relevant extenuating circumstances into account in your application. Your responses are shared with the Firm's Emerging Talent and hiring teams (and, if you specifically consent, with our specialist supplier).

All Personal Information Processed under our pre-hiring checks (and our broader Processing of Sensitive Information) are subject to enhanced confidentiality requirements, and shared strictly on a

need-to-know basis. Any relevant factors disclosed as part of the process will only be used in accordance with applicable equal opportunities legislation, and our related policies.

USE OF YOUR PERSONAL INFORMATION

Our Processing of your Personal Information will include obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, copying, analysing, amending, retrieving, using, systemising, storing (including in the cloud), disclosing, transferring, retaining, archiving, anonymising, erasing or destroying it by automated or non-automated means.

The UK and EU GDPR and applicable US state and other privacy laws require us to communicate to you the purposes for which we Process your Personal Information (the "Permitted Purposes"). The UK and EU GDPR additionally require a disclosure of the corresponding 'Legal Basis'. These are summarised in the tables below. There are similar laws in other countries where we have offices. Data collected for specific Permitted Purposes will not be subsequently used in a manner inconsistent with those purposes unless legally permitted.

Although applicable Data Privacy Laws in jurisdictions outside the European Economic Area (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 our Privacy Officers (see the 'Contacts and other important privacy information' below). In the event of any inconsistency, the local legislation will prevail. In particular - where applicable laws in certain jurisdictions require consent, your provision of Personal Information to us (and, if you are a client, your agreement to our engagement terms) will be deemed as confirmation of your consent to such Processing where appropriate. Where required, we will also ask you to provide your explicit written consent.

Permitted Purposes

We Process Your Personal Information for one or more of the general Permitted Purposes set out below. Where we are legally permitted to do so and one of the general Permitted Purposes apply, we may also Process Sensitive Information as set out below:

Legal Basis	Permitted Purpose

Legal Basis	Permitted Purpose
Where it is necessary to perform our contract with you or to take steps at your request to enter into the contract	**For example:** (a) to perform our legal and related services and provide legal advice if you are a client (including related client files management; order/matter acceptance, modification and processing; and for billing purposes and billing follow-up as applicable); (b) to employ/engage you if you are applying for a position; (c) to enter into or perform our agreement with you if you are a supplier or external adviser (including supplier account management; purchase order processing; and for payment of invoices); or (d) to enter into or perform any other contract/agreement we may have with you.
Where it is necessary for compliance with a legal obligation	**For example:** (a) to carry out internal conflicts and other regulatory checks on new client matters and to undertake appropriate client due diligence in accordance with anti-money laundering laws; (b) to perform appropriate pre-hiring and ongoing checks in accordance with our professional obligations; (c) to undertake appropriate vetting of suppliers and external advisers (for example, to comply with our obligations under applicable privacy, tax payment and tax evasion, modern slavery, anti-bribery and corruption and confidentiality rules); (d) to protect our and our clients' Personal Information, and other information, property and assets; (e) for health and safety and workplace accident prevention compliance; (f) for equal opportunities monitoring and reporting purposes; (g) to co-operate with our regulators and other public authorities (including by responding to their requests for information; undertaking internal investigations; and complying with our reporting and other professional obligations); and (h) to comply with any other obligation to which we are subject under applicable rules and law.

Legal Basis	Permitted Purpose
Where it is necessary for the purposes of our or another party's legitimate interests, except where these are overridden by your interests, rights or freedoms	**For example:** (a) to ensure compliance with our internal policies and Code of Conduct; (b) for general security and business continuity purposes; (c) for business management and financial planning (including management of suppliers; business process improvement and quality purposes; management reporting and reviewing records; accounting and auditing; and corporate due diligence); (d) for managing insurances, complaints, potential and actual claims; (e) to ensure the effective provision of legal services to clients and enhance our international business and cross-border offerings; (f) for the improvement of our recruitment and other business processes; (g) for training and continuing professional development purposes; (h) to manage our alumni program and network; (i) for advertising, marketing and public relations purposes, including preparing client pitches and other business development material such as deal credentials; sending you legal blogs, legal updates, news and industry updates, events, promotions and competitions, reports and other information; (j) to organize corporate events and to carry out market research campaigns; (k) to protect, manage and improve our websites, and other services (including: (i) to make sure our websites function as they should; (ii) to recognize you and your preferences when you return to the websites; (iii) to analyse how our websites and online services are performing; and (c) to present you with customized options relating to your interests;) (l) for any other legitimate purpose communicated to you at the time of collection of your Personal Information. We consider that our legitimate interests and these uses are proportionate, and compatible with your interests, legal rights or freedoms. Details of the balancing test undertaken in respect of such Processing is available upon request.

Legal Basis	Permitted Purpose
Where you provide your consent	**For example:** (a) to deal with your enquiries and requests for information about our firm and services; (b) where applicable laws in certain jurisdictions require your consent for advertising, marketing, for conducting background checks and other processing, and for public relations purposes; (c) where you ask us to apply for or to renew, your practicing certificate, foreign lawyer registration, work visa or other regulatory registration/authorization on your behalf; and (d) where you otherwise provide us with your valid consent.
Where it is necessary to protect your vital interests or that of another person	**For example:** For the disclosure of your Personal Information in the event of medical emergencies.
Where it is necessary for reasons of substantial public interest, on the basis of applicable law	**For example:** (a) In jurisdictions where this is legally permitted, Processing details of criminal and regulatory offences, allegations and other Sensitive Information: (i) for the prevention or detection of fraud and other unlawful acts; (ii) to comply with our money laundering and terrorist financing reporting requirements; and/or (iii) to protect the public against dishonesty, malpractice or other seriously improper conduct; unfitness or incompetence; mismanagement or failures in services. (b) In jurisdictions where this is legally permitted, Processing of data concerning your health, diversity data and other Sensitive Information for equal opportunities monitoring and reporting purposes. (c) Processing which is necessary for any other valid public interest reason.
Where it is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, on the basis of applicable law.	**For example** to monitor, prevent and/or control the spread of an epidemic or other serious threat to health in accordance with applicable law/public health requirements.

Legal Basis	Permitted Purpose
Where the processing is necessary for the establishment, exercise or defense of legal or regulatory claims	**For example:** In jurisdictions where this is legally permitted, where the Processing of details of criminal and regulatory offences, allegations and proceedings and other Sensitive Information is necessary: (a) to make or defend a claim, complaint or regulatory allegation on your behalf if you are a client; (b) to exercise our legal rights against third parties; (c) to defend claims, complaints or regulatory allegations made by you or other persons against us; and/or (d) for the establishment, exercise or defence of any other claim.
Where the processing relates to Sensitive Information manifestly made public by you	**For example:,** Sensitive Information included on your employer's website, your public social media, the press, or otherwise online and/or in public, which is Processed for one or more of the general Permitted Purposes.
Where it is necessary to protect your vital interests or that of another person where you/they are physically or legally incapable of giving consent	**For example:** The disclosure of your Sensitive Information in the event of medical emergencies in circumstances where consent cannot be provided.
Where you provide your explicit consent, except where applicable law prevents it	**For example:** (a) Where you ask us to apply for or to renew, your practicing certificate, foreign lawyer registration, work visa or other regulatory registration/authorization on your behalf which requires the disclosure of details of criminal and regulatory offences, allegations and proceedings and other Sensitive Information; (b) For completion of voluntary diversity and inclusivity surveys, and where you ask us to include information about your racial or ethnic origin or sexual orientation for consideration in public diversity awards; (c) You consent to us using your witness statement to investigate a health and safety incident or workplace accident; and/or (c) You otherwise provide your valid explicit consent.

THE PROVISION OF PERSONAL INFORMATION AS DESCRIBED IN THIS NOTICE IS PARTLY A STATUTORY REQUIREMENT AND PARTLY A CONTRACTUAL REQUIREMENT. IN GENERAL, YOU ARE REQUIRED TO PROVIDE SUCH PERSONAL INFORMATION, EXCEPT IN LIMITED INSTANCES WHEN WE INDICATE THAT THE PROVISION OF CERTAIN INFORMATION IS VOLUNTARY.

MARKETING AND COOKIES

We generally rely on our legitimate interests to Process your Personal Information for marketing purposes.

We will inform you in advance of sending you marketing (unless this is reasonably obvious in the circumstances - for example, when you provide us with your business card during a formal meeting).

To the extent applicable laws in certain jurisdictions require consent, your provision of Personal Information to us will be deemed as confirmation of your consent to such Processing where appropriate. Where required, we will also ask you to provide your explicit written consent.

SEE OUR COOKIES POLICY FOR FURTHER INFORMATION ABOUT THE COOKIES WE USE.

MARKETING PREFERENCES

Where you are known to us and have been added to our contacts database, we will use your marketing and content preferences, and other Personal Information you provide to us (including details of your attendance at, or interest in, events) in an identifiable format and information about how you review our marketing emails and interact with us to try and ensure that you only receive material and information from us that you are likely to find of interest.

CHANGING YOUR MARKETING PREFERENCES

You can change your preferences for receiving group marketing emails, legal updates and other information from us by clicking on the ‘update your preferences’ link in a BCLP Group marketing email.

You also have the right to ask us not to process your Personal Information for marketing purposes - and can exercise the right at any time by sending us an email at privacy@bclplaw.com, or clicking on 'unsubscribe' in a BCLP Group marketing email.

WHERE IS PERSONAL INFORMATION STORED AND SHARED WITH

We understand the importance of keeping your Personal Information secure.

Electronic information is securely stored, managed and accessed from geographically dispersed datacentres, which are fully controlled on least privileged basis. Our regions are divided into Europe, Asia and the US with datacentres and hosting facilities located in Europe, the UK, US and Singapore. In those jurisdictions where there are applicable local rules on the storage of Personal Information, we will put in place appropriate arrangements to comply with those local requirements.

Your Personal Information will, where appropriate, be disclosed internally within the BCLP Group. Please refer to the Our Locations section of our website for a list of our current offices and their locations. We will also at times need to disclose some of your Personal Information with select third parties, such as those set out below.

If you are an applicant, we do not disclose your Personal Information to any other third parties (except with your explicit consent for contextual recruitment purposes where you are applying for a UK or Asia graduate role). Additionally, we do not sell or share, as such terms are defined under applicable laws, specifically your applicant Personal Information.

If you are a client, your work contact details and a marketing profile will be added to our internal contacts database (which is accessible to BCLP Group offices). Your name, employer and job title may also appear in certain internal client matter summaries. We will only share more Personal Information where appropriate. For example:

- Our internal Compliance team (who are primarily based in England, Singapore and the US) handle new client and matter opening (including client due diligence). They (in addition to individuals in our relevant offices working on your matters) will therefore have access to such Personal Information.
- Under applicable rules and laws (including those in respect of anti-money laundering and any economic, financial, political, legal and other sanctions imposed by the United Kingdom, European Union, United States or other relevant country or international organisation ("Sanctions")) or court orders we will, exceptionally, have to disclose details of your affairs (including Sensitive Information) to the relevant authorities. We will not always have the right to tell you that this has happened.
- In certain circumstances we will also have to share some of this Personal Information with Select Third Parties who need limited access in order to provide services to us, or to enable us to provide services to you.

THIRD PARTIES

Persons related to you	Your agents, consultants, other advisers, counterparties, beneficiaries, trustees, banks and related persons who operate or are based around the

	world, where you ask us to, or as otherwise necessary for the Permitted Purposes.
Persons related to us	Our agents, consultants and other professionals, suppliers and external agencies/administrators who assist us with legal, administrative, financial, operational and other services, and may have access to certain of your Personal Information as part of their role. These will include, for example: (a) IT software, applications and services, including cloud providers, web content management, recruitment and telecommunications services suppliers; website, online portal and client extranet providers; (b) business continuity/disaster recovery and data back-up providers; (c) our file storage and management suppliers; (d) third party due diligence and identity/background verification suppliers; (e) our banks and other financial providers (such as currency exchange, e-billing and outsourced payroll suppliers); (f) our insurers, insurance brokers and lawyers; (g) our auditors and other professionals engaged for audit purposes; (h) debt collection agencies; (i) local lawyers, tax advisors or experts; and (i) other professional advisors. Current or potential affiliates and successors in title to our business, who may be based around the world. Business partners (for example, other law firms or financial/tax advisers and other professionals) with whom we collaborate to provide joint services to you or to organize joint corporate events.
Courts/tribunals; and law enforcement, regulatory and public authorities	Where disclosure is required by applicable rules and law, or by any court, tribunal, law enforcement, regulatory, public or quasi-governmental authority or department around the world.
Other involved persons	If you attend an event organized or hosted by us, we may disclose your details to others who attend or participate in the organization of that event (as notified to you). Any other persons with whom we may interact on your behalf or at your request and/or where this is otherwise necessary in connection with the Permitted Purposes.

SECURITY OF YOUR PERSONAL INFORMATION AND DATA BREACHES

We operate a range of technical, non-technical and procedural controls to safeguard your Personal Information (including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage). In particular:

The use of: (a) firewalls, encryption, filtering, vulnerability scanning tools and periodic penetration tests; (b) physical and technical controls on, and monitoring of, access to our premises and systems; and (c) Business Continuity and Disaster Recovery Plans.
We only engage reputable suppliers. We undertake appropriate information security and regulatory compliance due diligence on them and enter into appropriate contractual terms.
We have internal compliance policies and provide appropriate internal data privacy and information security training.
Where your Personal Information is transferred to other countries, we will put appropriate safeguards in place to ensure the lawfulness and security of the transfer. For example, all transfers of Personal Information across the BCLP Group including to our offices outside of the EEA are based on the EU Commission's standard contractual clauses, which may be read on https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en ; and (ii) the UK, are based on the ICO's International data transfer agreement, which may be read at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/ . We will also put such arrangements in place with third parties as appropriate. Where required under applicable local law, we will seek your consent to the transfer.

We keep these arrangements under regular review, taking into account security and compliance best practices, current risks, threats, vulnerabilities, mitigating controls, technology, and changes in applicable legal requirements.

However, the transmission of information via the internet is not completely secure. Although we do our best to protect your Personal Information, we cannot guarantee the security of your Personal Information transmitted to our websites – and any such transmission is at your own risk. Our websites may also, from time to time, contain links to third party websites - which are outside of our control and are not covered by this Notice. If you access other websites using the links provided, please check their privacy notice before submitting any Personal Information to them.

If a data breach (leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, your Personal Information) occurs which is likely to result in a high risk of adversely affecting your rights and freedoms, we will inform you of this without undue delay.

Where legally permitted, any such notifications will be made either via email, post or telephone.

HOW LONG WE KEEP YOUR INFORMATION

We will only keep your Personal Information in an accessible form which can identify you for as long as we need to for the Permitted Purposes.

As retention periods can vary significantly depending on the Permitted Purpose and the relevant jurisdictions concerned, it is not possible for us to commit to an overall retention period for all of your Personal Information held by us.

As a result, we use certain categories and criteria to determine how long we keep certain of your Personal Information, and these are set out below. Where your Personal Information is used for more than one Permitted Purpose (and/or in more than one jurisdiction), there will be overlapping retention periods in respect of that Information. In such cases, we will retain your Personal Information for the longer of those overlapping retention periods. We will also transfer paper files into, and store them in, electronic format where appropriate.

If you are a client, after the expiry of the retention period, we may dispose of your matter files (including your Personal Information) without further notice to you, except for any documents or deeds that we have agreed in writing to hold for safe keeping.

Type of Personal Information	**Retention Period**
Personal Information Processed in connection with client matters	Up to 15 years after the date of our final bill for the relevant matter, unless: (a) otherwise required by applicable law; (b) where required for regulatory, compliance or insurance purposes; (c) where a longer limitation period applies in respect of specific types of actions/documents; and/or in the event of a dispute which requires it to be kept for longer; (d) where you ask that we retain some of your original documents (such as wills and trust documents) on your behalf for safekeeping - in such circumstances, we will retain the documents for such period (and on such terms) as agreed between us; or (e) there is another legitimate reason which requires it to be kept for longer.

Type of Personal Information	Retention Period
Personal Information Processed in connection with your application for a role	Unsuccessful applicants - up to 2 years after the date of notification that their application has not been successful, unless: (a) otherwise required by applicable law; (b) you consent to us storing it for longer (for example to consider you for future roles); or (c) in the event of a dispute or other legitimate reason which requires is to be kept for longer.
Personal Information relating to suppliers and the services they provide to us	Up to 13 years following the end of our business relationship, unless: (a) otherwise required by applicable law; (b) you consent to us storing it for longer; (c) the Personal Information forms part of files which are required to be kept for longer (for example where you were involved in one of our client matters); or (d) where a longer limitation period applies in respect of specific types of actions/documents; and/or in the event of a dispute or other legitimate reason which requires it to be kept for longer.
Personal Information used for marketing purposes	For as long as you have not opted out of our marketing. If you ask us to no longer use your Personal Information for marketing purposes, we will need to retain certain of your details in our database to ensure that we do not accidentally send you marketing material.
Personal Information held in our electronic backups	Our electronic back-ups are retained for varying lengths of time dependent upon system for business continuity reasons, following which they are deleted

Where we no longer require your Personal Information, we will take steps to delete or anonymize it. There will be circumstances where certain Personal Information cannot be permanently deleted or anonymized, for example because it is stored in our back-ups for business continuity purposes.

In such cases, we will take appropriate steps to minimize (and pseudonymize where technically practicable) the Personal Information that we hold, and to ensure that it is: (a) not used in connection with any decision involving you; (b) not shared with anyone, except where we are legally required to do so (e.g. following a court order); (c) kept secure and virtually inaccessible; and (d) permanently deleted if, or when, this becomes technically possible.

YOUR RIGHTS

You may have certain rights regarding your Personal Information and Sensitive Information. The rights available to you depend on our reason for processing your Personal Information and the requirements of applicable law (i.e., your rights will vary depending on whether you are located in, for example, California, the EU, the UK, Asia or the Middle East). Specifically, you may have the following rights. Further information can be sought from our privacy contacts. In the event of any inconsistency, the applicable local legislation will prevail.

Right to be informed	You can ask us to provide you with privacy information about how we Process your Personal Information. That information is set out in this Notice, together with any other specific notices which are provided to you at the time of collection of your Information.
Right of access	You can request us to confirm whether we Process your Personal Information. You can also ask us to access your Personal Information.
Right to rectification (correction) and erasure (deletion)	In the event that we hold inaccurate or incomplete Personal Information, you can ask us to rectify or correct that Information. You can also ask us to erase/delete your Personal Information. This right is not absolute and only applies in certain circumstances.
Right to restrict processing	You can ask us to restrict the Processing of your Personal Information (or to suppress it) for a certain period of time. This right is not absolute and only applies in certain circumstances. Where applicable, the respective Personal Information will be marked accordingly and may only be processed by us for certain purposes.
Right of data portability	You can ask us to move, copy or transfer your Personal Information back to you or to another person under certain circumstances. This right only applies: (a) to Personal Information you have provided to us as a Data Controller; (b) where the Processing is based on your consent or for the performance of a contract; and (c) when processing is carried out by automated means.
Right to object	You can ask us at any time to stop Processing your Personal Information for marketing purposes. Where there are legitimate grounds to do so, you can also object to us Processing your Personal Information on the basis of our legitimate

	interests and in certain other situations.
Right to withdraw consent	Where we are Processing your Personal Information on the basis of your consent, you can withdraw that consent at any time.
Right to opt out of the sale or sharing of Personal Information	We do not currently, nor have we in the preceding 12 months, sold or shared (in this context, share means use of your Personal Information for cross-contextual behavioural advertising) your Personal Information.
Right of non-discrimination/retaliation	We do not discriminate against individuals who exercise any of their rights described in this Notice, nor do we retaliate against individuals who exercise these rights.
Right to opt out of the use of Sensitive Information	You have the right to opt out of certain uses and disclosures of Sensitive Information. However, we do not use or disclose Sensitive Information for purposes other than those which cannot be limited under California law.

Please note that many of the above rights are subject to exceptions and limitations. Your rights and our responses will vary based on the circumstances of the request. If you choose to assert any of these rights under applicable law, we will respond within the time period prescribed by such law. We will not be able to comply with your request in certain circumstances, for example where your request is manifestly unfounded or excessive.

When you Request access to your Personal Information, there will be some Personal Information, which we are not able to disclose to you, such as documents which include confidential or personal information about another entity or person; documentation relating to management forecasting or planning; legally privileged documents; and copies of references.

For further details about these privacy rights under EU and UK GDPR (including their limitations), please see the European Commission's website.

To exercise your rights, please send a written and dated request (a "Request") to privacy@bclplaw.com, or speak to the relevant contact. Please note that we will need to verify your identity in order to be able to comply with certain of your Requests.

We hope to address any enquiry or Request to your satisfaction, but if we do not, you have the right to lodge a complaint with the relevant data protection regulator in the country where you normally live or work, or where an alleged breach of data protection is said to have occurred (such as the Information Commissioners' Office in England).

California Residents

If you are located in the State of California in the United States, a person authorized to act on your behalf may make a verifiable request related to your Personal Information. If you designate an authorized person to submit requests to exercise certain privacy rights on your behalf, we will require verification that you provided the authorized agent permission to make a request on your behalf.

Please address written requests and questions about your rights as a California resident to privacy@bclplaw.com or call us at toll free number: 1-833-948-1182.

CONTACTS AND OTHER IMPORTANT PRIVACY INFORMATION

The identity of the BCLP Firm which is the Data Controller for each of our offices is on our website legal notices. For contact details, please see Our Locations.

We have appointed a Compliance Officer for Data Protection for the BCLP Group, supported by our Regional Privacy Officers. Where required by local law, we have also appointed statutory Data Protection Officers for certain of our offices. Their details are as follows:

	Location	**Offices Responsible for**
The Compliance Officer for Data Protection / Regional Privacy Officer for Europe and the Middle East	London office	UK, Brussels, Paris, United Arab Emirates and Saudi Arabia
The Data Protection Officer, Bryan Cave Leighton Paisner LLP (Germany)	Berlin office	Germany
The Data Protection Officer, Singapore / Regional Privacy Officer for Asia and Australia	Singapore office	Singapore, Hong Kong SAR, Australia
The Regional Privacy Officer for the United States	San Francisco office	US

If you have any queries regarding this Privacy Notice or our processing of your Personal Information, please email us at privacy@bclplaw.com. You may also:

- Write a letter to the 'Privacy Officer' (or the 'Data Protection Officer' where applicable) at the relevant office; or
- Speak directly to the Compliance Officer for Data Protection in our London office.