Privacy Notice

DILL DILL CARR STONBRAKER & HUTCHINGS, P.C. (the "Dill 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.

The Dill Group is responsible (i.e. they are the 'Data Controllers') for the Personal Information we respectively collect about you (including through the www.dillanddill.com website).

The type of 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. If you are a current Dill Group employee, self-employed consultant or lawyer, trainee, intern, volunteer or any other employee or contractor (together "Staff") or Partner, see our Staff Privacy Notice instead.

Please note in particular that:

1. As a regulated law firm, we are required by applicable rules to undertake appropriate: (a) pre- hiring checks of our Staff and Partners; and (b) vetting of other third parties (including of our clients and related parties, and of suppliers). These checks/vetting will involve the collection of criminal and regulatory records where appropriate 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 to help us manage and improve our websites, your browsing experience, and (where you are known to us) the material/information that we send you. 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.

4. We will publish updates to the Notice on this website, with relevant changes highlighted as appropriate. Where we hold or Process your Personal Data, 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.

5. 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 Policy page.

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.

You will voluntarily provide most of your Personal Information directly to us. We will also obtain Personal Information from other sources or persons, including:

Public Information	Personal Information about you or your business which is publicly available, for example on your employers' website, public professional social networking sites, the press; and relevant electronic data sources.
Information From Third Parties	Personal Information provided to us by 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) where such Information is provided to us in connection with the relevant purposes set out in this Notice.
Information Collected Through our Websites	We use Cookies on our website and certain marketing emails which collect your IP address and certain other information from you when you visit our websites. For further details, please see the 'Marketing, cookies and profiling' 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

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 will in most cases need to collect your work details (such as your name, job title, work address, office email and telephone number). Other types of Personal Information which we will typically collect includes, for example:

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; or (b) do not currently have office/work contact details.
Your activity on our websites	Including 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, cookies and profiling' section below

Security and business continuity

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

Type of Data	Examples	Context
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.

Special categories of information

In certain circumstances we will need to collect more sensitive Personal Information, such as (unless applicable local law prevents this) diversity and health data, and details of offenses, regulatory action and related proceedings ("Sensitive Information"). Such information may be collected from you or, in those jurisdictions where it is permitted under applicable local law, from third parties.

This will typically be more relevant: (a) for new/current Staff and Partners; (b) where necessary to enable us provide you with our legal services; or (c) as part of our due diligence on third parties (including clients and related persons, and suppliers) – please see the relationship- specific sections of this Notice for further information.

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 your religion or health. Providing the name of your spouse or partner to us may also reveal your sexual orientation).

We will only request Sensitive Information where necessary and we are legally allowed to, and will put in place enhanced safeguards to protect such Sensitive Information.

Further information for clients

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 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 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 suppliers and external advisers

As a business, we are under legal and regulatory obligations to perform appropriate vetting of our suppliers and external advisers. This includes ensuring that you have appropriate compliance systems, policies and procedures on information security and data protection, and for the prevention of economic crimes (such as money laundering, tax evasion, fraud and bribery and modern slavery).

If you do not provide the required vetting information, we may not be able to engage you. We will notify you at the relevant time if this is the case.

We adopt a risk-based approach to our vetting, based on the sensitivity of the information you will have access to and the work you will undertake for us. In certain circumstances where we are legally permitted to do so, this will involve the Processing of Sensitive Information (such as allegations or findings of criminal acts, regulatory action and related proceedings) which are disclosed to us by you or your employer.

Sometimes we will need to: (a) see original documents; (b) check the information you or your employer provide; and (c) use Your Personal Information to check your identity and background through electronic data sources.

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 organizing, copying, analyzing, amending, retrieving, using, systemizing, storing, disclosing, transferring, retaining, archiving, anonymizing, erasing or destroying it by automated or non-automated means.

Further details on: (a) security and business continuity arrangements; (b) client due diligence and supplier vetting; and (c) equal opportunities monitoring and reporting, can be found in 'The types of Personal Information that we collect' section above. For further information about marketing, cookies and profiling, please see the 'Marketing, cookies and profiling' section.

General Permitted Purposes

We Process Your Personal Information for one or more of the following general Permitted Purposes. Where the Processing involves Sensitive Information, see also the second table under the heading 'Sensitive Information'.

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); 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

Legal Basis	Permitted Purpose
	appropriate client due diligence in accordance with anti-money laundering law; (b) to perform appropriate pre-hiring checks of Staff and Partners 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; for health and safety and workplace accident prevention compliance; (e) for equal opportunities monitoring and reporting purposes; 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); (f) to comply with any other obligation to which we are subject under applicable rules and law.
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; (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;

Legal Basis	Permitted Purpose
	(h) 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; (i) to organize corporate events and to carry out market research campaigns; (j) 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 when you return to the websites; (iii) to analyze how our websites and online services are performing; and (c) to present you with customized options relating to your interests;) (k) 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.
Where you provide your consent	For example: (a) to deal with your enquiries and requests for information about our firm and services; (b) to the extent applicable laws in certain jurisdictions require your consent for advertising, marketing and public relations purposes; (c) where you ask us to apply for or to renew any 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 the disclosure of your Personal Information to medical staff in the event of medical emergencies.

Sensitive Information

Where we are legally permitted to do so and one of the general Permitted Purposes apply, we will Process Sensitive Information for one or more of the following additional Permitted Purposes:

Legal Basis	Permitted Purpose
Where it is necessary for reasons of substantial public interest, on the basis of applicable law	For example: a) for the prevention or detection of fraud and other unlawful acts; b) to comply with our money laundering and terrorist financing reporting requirements; and/or c) to protect the public against dishonesty, malpractice or other seriously improper conduct; unfitness or incompetence; mismanagement or failures in services. d) In certain 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. e) Processing which is necessary for any other valid public interest reason.
Where the processing is necessary for the establishment, exercise or defense of legal or regulatory claims	For example, in certain 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; 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 LinkedIn profile, 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	For example the disclosure of your Sensitive Information to medical staff in the event of medical emergencies in circumstances where consent cannot be provided.

Legal Basis	Permitted Purpose
you/they are physically or legally incapable of giving consent	
Where you provide your explicit consent, except prevents it	For example: (a) Where you ask us to apply for or to renew any 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) 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 (d) You otherwise provide your valid explicit consent.

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 (for example in Russia) 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.

Cookies

We use Cookies on our website to make sure the site functions as it should (e.g. to ensure images display correctly, to store your preferences, and to prevent errors).

Where you agree to Cookies through our website cookies banner, and/or click on a link in a blog, legal update or other direct mailing from us (a “Mailer”), we will also use certain Cookies (“Optional Cookies”) to:

1. Analyze how our websites and online services are performing; and

2. Personalize the content that you see on our website (and, where you are known to us, that we send you), based on your previous use of the websites.

Read our full list of cookies we use

Please note that some of the Cookies on our website are third party Cookies (e.g. Google advertising cookies) which we do not control.

If you are concerned about Cookies, most web browsers allow some control of most cookies through the browser settings.

For more information about cookies and how to disable and/or delete them, please visit

www.aboutcookies.org or www.allaboutcookies.org

WHERE IS YOUR PERSONAL INFORMATION STORED

Electronic information is stored by us in our secure servers.

We will also at times need to share some of your Personal Information with select third parties, such as:

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 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. 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.

(collectively, "Select Third Parties")

SECURITY OF YOUR PERSONAL INFORMATION

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 and undertake appropriate information security and regulatory compliance due diligence on them. Where suppliers will have access to our and/or our clients' information, they are also made subject to strict contractual

provisions requiring them to ensure any Personal Information is kept secure and is only used in accordance with our instructions (or as otherwise and to the extent strictly required by law, if applicable).
All our Partners and Staff who handle Personal Information are subject to confidentiality obligations, have to comply with our internal compliance policies, and receive appropriate data protection and information security training.

Our internal data protection compliance framework includes: (a) internal data protection and information security policies, systems and procedures; (b) a Privacy Oversight Committee (comprising senior cross functional leadership of the firm) to consider and make policy decisions regarding data privacy. They are supported by experts who are responsible for IT systems and Information Security, Marketing and Human Resources.

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 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 policy before submitting any Personal Information to them.

Data Breaches

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. For example, we are under legal obligations to keep certain records for specific periods which will usually extend after the end of a contractual relationship (including minimum statutory retention periods in respect of tax, payroll records; and client due diligence documents).

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 Information for the longer of those overlapping retention periods. We will also transfer paper files into, and store them in, electronic format where appropriate.

Type of Personal Information	**Retention Period**
Personal Information Processed in connection with client matters	Up to 10 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 relating to suppliers and the services they provide to us	Up to 10 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 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 backups are retained for 24 months 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 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.

Further information for clients

YOUR RIGHTS

The following privacy rights apply although there may be circumstances where some of these rights do not apply under or are modified by local law. 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 Privacy 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 and erasure	In the event that we hold inaccurate or incomplete Personal Information, you can ask us to rectify or complete that Information. You can also ask us to erase 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.
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.
Rights in relation to	You have the right to: (a) ensure that any significant decisions affecting you are not made purely by automated means based on an online profile or other

automated decision-making	information (i.e. a person is involved in the decision-making), and (b) that you can express your views and to challenge the decision.

To exercise your rights, please send a written and dated request (a "Request") to cwork@dillanddill.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.

- 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.
- We will not be able to comply with your Request in certain circumstances, for example where your Request is manifestly unfounded or excessive.