Streathers Highgate LLP

Privacy Notice

25 May 2018

1. INTRODUCTION & SCOPE

1.1 This Privacy Notice (**"Notice"**) sets out how Streathers Highgate LLP (collectively referred to as **"Streathers"**, "**we**", "**us**" or "**our**") handles the Personal Data of our clients, suppliers and other third parties.

1.2 This Notice gives you information on how we collect and process your Personal Data and applies to all Personal Data we Process regardless of the media on which that Data is stored or whether it relates to past, present or prospective Data Subjects. This Notice supplements any other notices provided to you from time to time and is not intended to override them.

1.3 A list of defined data protection terms used in this document can be found at Appendix 1. References in this Notice to **"Partner"** means a member of Streathers Highgate LLP.

1.4 We reserve the right to amend this Notice at any time without notice to you so, if required, please check to ensure that you are referring to the latest copy of this Notice. We may also notify you in other ways from time to time about the Processing of your Personal Data.

2. DATA CONTROLLER

2.1 Streathers Highgate LLP of 1 Heath Street, London NW3 6TP is a Data Controller for the purposes of the GDPR and is responsible for your Personal Data.

2.2 Streathers have appointed a Data Protection Officer (**"DPO"**) to ensure ongoing compliance with the GDPR and who can fulfil the tasks as outlined in Article 39 of the GDPR. These tasks include (but are not limited to):

(a) to inform and advise the Data Controller or the Data Processor and the employees who are Processing Personal data of their obligations pursuant to the GDPR;

(b) to monitor compliance with the GDPR, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 of the GDPR;

(d) to cooperate with the supervisory authority, the Information Commissioner's Office (**"the ICO"**); and

(e) to act as the contact point for the supervisory authority on issues related to the Processing of Personal data

2.3 The post of DPO is currently held by Kevin Tarpey, 020 7431 8889, ktarpey@streathers.co.uk. Please contact the DPO with any questions about the operation of this Notice or the GDPR or if you have any concerns that this Notice is not being or has not been followed.

2.4 You have the right to make a complaint at any time to the ICO (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

3. PERSONAL DATA PROTECTION PRINCIPLES

3.1 We adhere to the principles relating to Processing of Personal Data set out in the GDPR which 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**).

(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**).

4. LAWFULNESS, FAIRNESS, & TRANSPARENCY

4.1 We may collect, use, store and transfer different kinds of Personal Data about you which we have grouped together as follows:

(a) **Identity Data** includes first name, maiden name, last name, marital status, title, date of birth, gender, occupation, national insurance number, tax reference numbers, and copies of driving licences/passports.

(b) **Contact Data** includes billing address, home address, registered office address, email address and telephone numbers.

(c) **Financial Data** includes bank account and payment card details.

(d) **Transaction Data** includes details about your instructions and the legal services received from us.

(e) **Sensitive Personal Data** includes information relating to your physical or mental health.

4.2 We collect Data from and about you through:

(a) **Direct interactions**. You may give us your Identity, Contact, Financial, Transaction, and Sensitive Personal Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This primarily includes Personal Data you provide in conjunction with your instructions for the provision of legal services; and

(b) **Third parties or publicly available sources**. We may receive Personal Data about you from various third parties and public sources including (but not limited to):

(i) Identity, Contact, Financial and Transaction Data from your agents, employees, representatives and/or family members based inside and outside the EU.

(ii) Identity and Contact Data from publicly availably sources such as Companies House, the Land Registry and other governmental registers based inside the EU.

4.3 Where we need to collect Personal Data by law, or under the terms of a contract we have with you and you fail to provide that Data when requested, we may not be able to perform the contract we have or are trying to enter into with you. In this case, we may have to cancel a contract you have with us but we will notify you if this is the case at the time.

5. THE PURPOSE OF DATA PROCESSING

5.1 The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her 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;

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

5.2 Your Personal Data may be Processed in order that we may discharge the services agreed, and for other related purposes including updating and enhancing client records, analysis for management purposes, advising you or individuals working for you about our firm and its services, crime prevention and legal and regulatory compliance.

5.3 We do not currently take any decisions about you by automated means. Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

5.4 Examples of when Sensitive Personal Data may be processed are:

(a) information about your physical or mental health where such information is pertinent to your instruction such as the completion of lasting powers of attorneys or in litigation or family proceedings;

(b) in order to comply with legal requirements and obligations to third parties.

5.5 Personal data is only Processed for the specific purposes for which it was first collected or for any other purposes specifically permitted by the GDPR. This means that Personal Data is not collected for one purpose and then used for another. If it becomes necessary to change the

purpose for which the Data is processed, you will be informed of the new purpose before any Processing occurs (in so far as it is reasonable and practical to do so).

5.6 Generally we do not rely on consent as a legal basis for Processing your Personal Data and we may Process your Personal Data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. DATA MINIMISATION

6.1 Personal Data is only collected to the extent that it is required for the specific purpose notified to you. Any Data which is not necessary for that purpose will not be collected in the first place.

7. ACCURACY

7.1 Personal Data should be accurate and, where necessary, kept up to date. If necessary, steps will be taken to check the accuracy of any Personal Data at the point of collection and at reasonable intervals afterwards.

7.2 Please keep us informed if your Personal Data changes during your working relationship with us.

8. STORAGE LIMITATION

8.1 We will only retain your Personal Data for as long as reasonably required to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Personal Data will be securely destroyed or erased from our systems when it is no longer required.

8.2 To determine the appropriate retention period for Personal Data, we consider the amount, nature, and sensitivity of the Personal Data, the potential risk of harm from unauthorised use or disclosure of your Personal Data, the purposes for which we Process your Personal Data and whether we can achieve those purposes through other means, and the applicable legal requirements.

9. SECURITY, INTEGRITY AND CONFIDENTIALITY

9.1 The GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. We ensure that reasonable security measures are taken against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

9.2 Maintaining data security means guaranteeing 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 should be accurate and suitable for the purpose for which it is Processed.

(c) **Availability** means that authorised users should be able to access the Data if they need it for authorised purposes.

9.3 If you have any questions about our current organisational and technical security procedures, please contact the DPO or one of the Partners.

9.4 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject. We will notify Data Subjects or any applicable regulator where we are legally required to do so.

10. DATA SHARING & TRANSFERRING INFORMATION OUTSIDE THE EU

10.1 We may have to share your Data with third parties. We will only share your Personal Data with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. "Third parties" includes your other representatives in relation to an instruction, the representatives of other parties to a relevant instruction and third party experts such as counsel.

10.2 Such third parties in the United Kingdom and the EU are subject to the provisions of the GDPR or similar regulations in relation to your Personal Data. We do not authorise third parties to use your Personal Data for their own purposes.

10.3 We may also be required to transfer your Personal Data outside the EU. 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. We transfer Personal Data originating in one country across borders when we transmit, send, view or access that data in or to a different country.

10.4 We may transfer Personal Data outside the EEA only if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;

(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 including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

11. DATA SUBJECT'S RIGHTS & REQUESTS

11.1 You have rights when it comes to how we handle your Personal Data. These include rights to:

(a) **Request access** to your Personal Data (commonly known as a "data subject access request"). This enables you to receive certain information about our Processing activities and a copy of the Personal Data we hold about you to check that we are lawfully processing it.

(b) **Request correction** of the Personal Data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

(c) **Request erasure** of your Personal Data. This enables you to ask us to delete or remove Personal Data where there is no good reason for us continuing to Process it. You also have the right to ask us to delete or remove your Personal Data where you have exercised your right to object to Processing (see below).

(d) **Object to Processing** of your Personal Data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your Personal Data for direct marketing purposes.

(e) **Request the restriction of processing** of your Personal Data. This enables you to ask us to suspend the Processing of Personal Data about you, for example if you want us to establish its accuracy or the reason for Processing it.

(f) **Request a copy of any agreement** under which Personal Data is transferred outside of the EEA;

(g) **Request the transfer** of your Personal Data to another party.

11.2 If you want to review, verify, correct or request erasure of your Personal Data, object to the Processing of your Personal Data, or request that we transfer a copy of your Personal Data to another party, please contact the DPO or a Partner in writing.

11.3 In the limited circumstances where you may have provided your consent to the collection, Processing and transfer of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific Processing at any time. To withdraw your consent, please contact your solicitor of the DPO. Once we have received notification that you have withdrawn your consent, we will no longer Process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

11.4 You will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, we will charge a reasonable fee if your request for access is unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

11.5 We may need to request specific information from you to help us confirm your identity and ensure your right to access any information requested (or to exercise any of your other rights). This is an appropriate security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it.

APPENDIX 1

1. DEFINITION OF DATA PROTECTION TERMS

1.1 **Consent**: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

1.2 **Data:** information which is stored electronically, on a computer, or in certain paper-based filing systems.

1.3 **Data Controller**: 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. Streathers are the Data Controller of all Personal Data relating to our clients, employees, workers, contractors, agency workers, consultants, members and others and Personal Data used in our business for our own commercial purposes.

1.4 **Data Processor(s):** any person who processes Personal Data on behalf of a Data Controller. Employees of Data Controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

1.5 **Data Subject**: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

1.6 **EEA**: the countries in the EU, and Iceland, Liechtenstein and Norway.

1.7 **Explicit Consent**: consent which requires a very clear and specific statement (that is, not just action).

1.8 **General Data Protection Regulation (GDPR)**: the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

1.9 **Personal Data**: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive 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.

1.10 **Personal Data Breach**: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or 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.

1.11 **Processing or Process**: 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, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

1.12 **Sensitive Personal Data**: 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.