Lincolns Family Law – Information Notice on the General Data Protection Regulation (GDPR)

This Notice sets out the obligations of Lincolns Family Law regarding data protection and the rights of clients ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

Does the GDPR still apply?

The EU GDPR is an EU Regulation and it no longer applies to the UK. The applicable law is now the Data Protection Act 2018 (DPA 2018).

However, the provisions of the EU GDPR have been incorporated directly into UK law as the "UK GDPR". In practice, there is little change to the core data protection principles, rights and obligations.

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

In the context of this notice the "data subject" will be any client of Lincolns Family Law.

This Notice sets out our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. Richard Shaw is the data controller and data protection officer of Lincolns Family Law and he is registered with the Information Commissioners Office.

The GDPR in summary:

The Data Protection Principles: the GDPR sets out the following 6 principles with which any party handling personal data must comply. All personal data must be processed in ways that are:

1. Lawful, fair and transparent to the data subject. For example, you must be notified within 1 month, when we acquire personal data which you have not provided
2. Limited to its purpose of pursuing your matter on your behalf in accordance with your instructions and the terms of your retainer. Your data will not be processed in ways that are outside the scope of your case or in ways that are incompatible with the purposes for which you have instructed this firm
3. adequate and necessary in relation to the purposes for which it is processed
4. accurate (and your information must be kept up to date)
5. not kept longer than needed for the pursuance of your case on your behalf although it can be kept longer providing your personal data is only processed for archiving. In addition your data may also be kept when responding to a complaint in respect of our services**.**
6. Confidential. Your data should be stored securely and in a manner which ensures that unauthorised or unlawful processing cannot occur.

The Lawful basis of our data processing

The GDPR states that processing of personal data shall be lawful if at least one of the following conditions applies:

1. The consent of the data subject.
2. To prepare for or to fulfil a contract – this would include not only a situation where you have signed your terms of business and a client care letter but also in a situation where you have a fixed fee initial interview where written terms of business have not been produced or signed.
3. There is a legal obligation other than a contract such as a court order or any other statutory obligation that the law imposes on this firm. For example anti money laundering legislation.
4. In order to protect the vital interest of a data subject such as preservation of their life
5. A public function in the public interest
6. Another legitimate interest when data processing is necessary (subject to a legitimate interests assessment) such as marketing to you except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data,

We will primarily be relying on the condition of "preparing for or fulfilling a contract" in order to lawfully process your data although we may rely on additional conditions where appropriate.

The Rights of Data subjects.

1. The right to be informed

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and where personal data is obtained from a third party, you will be informed of its purpose

2. The right of access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data that we hold about them, what we do with that personal data, and why. SARs should be made in writing to the Data Protection Officer at Lincolns Family Law, the Afon Building Worthing Road Horsham West Sussex RH12 1TL. Responses to SARs will normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complicated and/or numerous requests are made. We do not charge a fee for the handling of normal SARs

3. The right to rectification

Data subjects have the right to require us to rectify any of their personal data that is inaccurate or incomplete. We will rectify your personal data in question, and notify you of that rectification, within one month of you informing us of the issue. This period can be extended by up to two months in the case of complex requests.

4. The right to erasure (otherwise known as the 'right to be forgotten')

Data subjects have the right to request that we erase the personal data we hold about them in the following circumstances:

(i) It is no longer necessary for us to hold your personal data with respect to the purpose(s) for which it was originally collected

(ii) You object to us holding and processing your personal data (and there is no overriding legitimate interest to allow us to continue doing so or contractual basis for us to hold it)

(iii) Your personal data needs to be erased in order to comply with a particular legal obligation.

Unless we have reasonable grounds to refuse to erase personal data, all requests for erasure will be complied with, and you will be informed of the erasure, within one month of receipt of your request. The period can be extended by up to two months in the case of complicated requests. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

5. The right to restrict processing

Data subjects may request that we cease processing the personal data we hold about them. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

6. The right to data portability

Where we rely on your consent or need to process your personal data in connection with a contract we've entered into with you, as the legal basis for processing your personal information, you may ask us to provide you with a copy of that information. We will provide this to you electronically in a commonly used and machine readable form. You may also ask us to transmit your personal data to a different data controller for example a different solicitor.

7. The right to object

Data subjects have the right to object to our processing their personal data based on legitimate interests and direct marketing. Where you object to us processing your personal data based on our legitimate interests, we shall cease such processing immediately, unless it can be demonstrated that our legitimate grounds for such processing override your interests, rights, and freedoms, or that the processing is necessary for the management of queries, complaints or the conduct of legal claims. If you object to us contacting you for marketing purposes we will cease that activity forthwith.

8. Data subjects also have the right to request information in respect to automated decision-making (currently we do not engage in automated decision making).

Special categories of data

There is a general prohibition on processing special categories of data including the following types of information: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data concerning a persons sex life or sexual orientation. This is subject to the exemptions listed at section 9(2) of the GDPR, which for example includes your explicit consent or you manifestly making such information public.

How we collect your personal information

This is information about you that you give to us by directly whether in person, corresponding with us by phone, email or via hardcopies of documentation or letters you send to us, and is provided entirely voluntarily.

Personal information we may receive from other sources.:

We may receive information from third parties in the course of pursuing your case. This may include your opponent, the court, reports from professionals that you or we instruct on your behalf. We may be required to share such information with third parties when appropriate in the course of pursuing your case.

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by Lincolns Family Law: records of telephone conversations, records of work carried out and time spent on your matter, documentation generated either by you, by us, your opponents, the courts and any other professionals we engage upon your instructions whilst pursuing your matter, invoices sent to you and invoices for disbursements and corresponding financial records.

The basic personal information we may ask for, or you may choose to give us, includes evidence in respect of your identity, your name, your address, email address and phone number. We may retain details of any enquiry you make to us and records of any correspondence with us.

Our suppliers and service providers may receive or have access to your personal information. We may disclose your information to our third party service providers, agents, subcontractors and other organisations for the purposes of providing services to us in order to allow us to act on your behalf.

Such third parties may include cloud service providers; hosting, email providers, providers engaged in legal accounting, providers of outsourced transcription, experts whom we instruct with your permission including Barristers, payment processing companies (who will process your debit/credit card securely if you purchase services from us).

When we use third party service providers, we only disclose to them any personal information that is necessary for them to provide their service and we have a contract in place that requires them to keep your information secure and not to use it other than in accordance with our specific instructions.

We will disclose your personal data to our insurers in the event that you make a complaint

against us.

We may disclose information to the Court and other statutory bodies where a legal obligation exists.

Data anonymity and use of aggregated information

Your information may be converted into statistical or aggregated data in such a way as to ensure that you are not identified or identifiable from it. Aggregated data cannot be linked back to you as a natural person. We may use this data for analytical purposes or for communicating with our regulator or insurers.

Data Protection Impact Assessments

We will carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage) under the GDPR.

Accountability and Record-Keeping

(i) The Data Protection Officer is Richard Shaw of the Afon Building, Worthing Road, Horsham, West Sussex RH12 1TL.

(ii) The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy.

(iii) We will keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

(a) The name and details of the firm, its Data Protection Officer, and any applicable third-party data processors;

(b) The purposes for which the firm collects, holds, and processes personal data;

(c) Details of the categories of personal data collected, held, and processed by the firm,

(d) Details of how long personal data will be retained by the firm

(e) Descriptions of all technical and organisational measures taken by the Firm to ensure the security of personal data.

Data Security

We will ensure that the following measures are taken with respect to the storage and use of personal data:

(i) Electronic copies of personal data will be securely stored at data centres located in the EU. Lincolns Family Law has a case management system in place and it is ISO27001 accredited and the provider stores data at data centres located in England and Wales.

(ii) No personal data should be transferred to any device personally belonging to an employee

(iii) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer;

(iv) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

(v) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

(vi) All passwords used to protect personal data will be changed regularly and will not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, and numbers,

(vii) Only employees, agents, sub-contractors, or other parties working on behalf of ourselves that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by us;

(viii) All agents, contractors, or other parties working on our behalf handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions arising out of the GDPR;

(ix) All personal data we hold shall be reviewed periodically

(x) When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

Data Breach Notification

1. All personal data breaches must be reported immediately to the Data Protection Officer.

2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

3. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

4. Data breach notifications shall include the following information:

    (a) The categories and approximate number of data subjects concerned;

    (b) The categories and approximate number of personal data

records concerned;

(c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

(d) The likely consequences of the breach;

(e) Details of the measures taken, or proposed to be taken, by us to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of this Policy

This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retrospective effect and shall thus apply only to matters occurring on or after this date.

We may review this policy from time to time and any changes will be notified to you by posting an updated version on our website.

LINCOLNS FAMILY LAW