Acorn Family Law Privacy Notice

This notice explains what personal data we obtain and why; how we use and store this data, who we share it with and how we keep it secure. Persons who have dealings with us are entitled to this information under data protection law[1].

Our details

We are Acorn Family Law LLP of Acorn House, 361 Midsummer Boulevard, Central Milton Keynes MK9 3HP. Your main point of contact for GDPR is Ms Leonora Marchant who is our Data Protection Officer.

Our contact details are general email: admin@acornfamilylaw.co.uk. Tel: 01908 410301 Web: www.acornfamilylaw.co.uk

What type of information we collect

The nature of our work requires us to collect personal data from all our clients as well as other parties directly involved in their cases. We will routinely collect full names, addresses, contact details, dates of birth and children's details. Depending on what work we have been instructed to do we may be required to obtain other and more sensitive data.

For financial cases we will usually need to collect and retain personal data and paperwork such as bank statements, pension statements, property valuations, mortgage statements, wage slips, tax returns, business accounts, etc.

For children cases we may be required to obtain and keep on file sensitive information relating to the relevant issues which can include paternity, drug and alcohol testing, medical reports or records, police records, witness statements, reports from other organisations such as CAFASS or a local authority.

How we get the information and why we have it

We obtain data from many sources but more specifically:

- Directly from our clients following face to face meetings, by post, over the telephone or by email

[1] General Data Protection Regulation (GDPR) under EU Law

- From other organisations such as the family courts, barristers, CAFCASS, local authorities, medical professionals, mediators, other solicitors, the other party, testing agencies, the police, or other relevant source.

We can do this lawfully in our contractual role as solicitors engaging in casework on our client's behalf. The full nature and extent of such data will depend on the type of case and whether we are actually instructed to engage in work on a client's behalf or simply providing information and support at a fixed fee appointment.

What we do with the information and who we share it with

We need to collect relevant data to verify client's ID, for money laundering purposes, to communicate with clients and other parties, to establish the facts of each case; and enable us to effectively manage and progress legal work on behalf of our clients.

Once we collect the information we will store this on physical files and electronically, and use it to correspond with our clients and relevant third parties, prepare legal documents, issue and conduct court proceedings, etc.

We will only share this information with other parties if it is necessary for us to do so for the proper conduct of our casework. This may include, but is not limited to: the family courts, barristers we instruct, CAFCASS, local authorities, medical professionals, mediators, the other party or their solicitor. Clients will be fully informed about this during the conduct of their case.

In very exceptional cases we may be obliged to divulge data by law or regulation for the prevention of crime or terrorism.

How we store and protect information

The data we obtain is kept in both paper and electronic form.

All paper files for our clients are retained on site at our offices and kept locked in filing cabinets when not in use. Sometimes client's files are taken to court for hearings when they are kept in the possession of the fee earner with conduct at all times. On other occasions client files may be taken to a partner's home address to work on, where they are retained in a lockable case when not in use. Client files are never left unattended in vehicles.

Data concerning all our clients and relevant third parties is stored on our cloud-based case management system, Osprey. Additionally data is kept on the individual PCs of all staff members in the firm and on the partners laptops. All hard drives are encrypted and subject to individual password protection. Access to Osprey is also password protected.

Concerning internet security, we do not have a shared connection and our individual internet provider has stringent security measures including encryption and firewalls to prevent unauthorised access to information we sent and receive electronically.

Who has access and how long we keep information

Only the partners and members of staff, or contractors such as bookkeepers have access to data on the devices we use to conduct our work, or the information we retain in paper form. All personnel working within the firm are aware of data compliance issues and have had training to understand the importance of confidentiality and of minimising the risk of any data protection breach.

Once a case is finished and the client's file archived we are, under legislation, obliged to retain it for at least 6 years. After that time both the physical file and electronic files will be destroyed.

Your data protection rights

By law, you are entitled to access your personal data. If you wish to make a request for the data we hold concerning you, please do so in writing addressed to our Data Protection Officer Leonora Marchant; or contact the person dealing with your matter.

This means you are entitled to a copy of the data we hold – such as your name, address, contact details, date of birth, information about your finances and so on, but it does not mean you are entitled to the documents that contain this data.

Under certain circumstances, you also have the following rights:

1. The right to be informed: fulfilled by way of this privacy notice and our clear explanation as to how we use personal data

2. The right to rectification: if your personal data is inaccurate or incomplete

3. The right to erasure / 'right to be forgotten': you can ask for the deletion or removal of your personal data where there is no compelling reason for its continued processing. This only applies in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was originally collected
- Where consent is relied upon as the lawful basis for holding your data and you withdraw your consent
- Where you object to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- Where you object to the processing for direct marketing purposes

4. The right to object: you have the right to object to processing based on legitimate interests where you have sufficient grounds to do so; such as for direct marketing.

If you elect to use your right to object, we must stop processing your personal data unless:

- we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms; or

- the processing is for the establishment, exercise or defence of legal claims.

5. The right to restrict processing: you have the right to request the restriction or suppression of your data. When processing is restricted, we can store the data but not use it. This right only applies in the following circumstances:

- Where you contest the accuracy of the personal data – we should restrict the processing until we have verified the accuracy of that data
- Where you object to the processing (where it was necessary for the performance of a public interest or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override your right
- Where processing is unlawful and you request restriction
- If we no longer need the personal data but you require the data to establish, exercise or defend a legal claim

6. **Your right to data portability** - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

How to complain

If you wish to raise a complaint on how we have handled your personal data, you should contact our Data Protection Officer Leonora Marchant, by telephone on 01908 410303, or email: lm@acornfamilylaw.co.uk

If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law, you can complain to the Information Commissioner's Office (ICO).

Their contact details are as follows:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Helpline number: 0303 123 1113