FT Chronic Pain Solicitors

Privacy Policy & How we assess risk

Our website uses cookies. A full copy of our privacy policy is available in hard copy, so, please contact us to request a copy.

Please contact Paul Turner or Anne Felmingham of FT Chronic Pain Solicitors to discuss any questions or any concerns you may have.

Anne Felmingham is the appointed officer for FT Chronic Pain Solicitors and we are registered with the ICO reference number ZA823989 https://ico.org.uk

We can be contacted on the following number:

Telephone **0800 9991078**

In writing:
paut.turner@ftchronicpain.co.uk anne.felmingham@ftchronicpain.co.uk

We are committed to ensuring:

- the efficient and effective use of the information which we hold;
- that we handle information about clients and third parties fairly and responsibly, including in compliance with relevant legal requirements and the General Data Protection Regulation and associated domestic legislation in particular;
- that our information is kept secure.

This policy should be read in conjunction with the information security standards and acceptable use policy set out within our staff compliance manual. It sets out how we comply with the GDPR and includes signposts to clear staff standards and training requirements.

How we use personal data and the conditions relied upon under the GDPR

We are required by Article 30 of the GDPR to maintain certain records of our processing activities and these are as detailed / signposted below:

Our name and contact details:	As detailed above.
Purposes of our processing data	In order to operate as an employer and to provide legal advice and services we obtain, store and use personal information about clients, staff and others.

Categories of data subjects	In broad terms we hold information about our staff, unsuccessful job applicants, the staff of our business contractors and partners, clients, experts, counsel, Courts, government bodies and agencies, unconverted client enquiries, potential clients and other individuals connected to client case. See our information audit and data mapping exercise for further detail.
Categories of personal data	See our risk assessment below and our information audit and data mapping exercise for further detail.
Categories of third parties with whom personal data will be shared	In broad terms we may share personal data with lawyers representing others in the proceedings, official bodies with whom legal documents must be lodged such as the Courts and Land Registry, our regulatory bodies in appropriate circumstances, our contractors and consultants and their staff, those requesting references, witnesses, experts, counsel, IT service and software providers. Further information on how we ensure compliance when sharing personal data in this way is set out below.
Countries outside of the EU where data is transferred	We do store much of our information electronically but this does not involve data being moved outside of the EEA. Where this becomes necessary and for those countries which have not been specifically approved for such purposes under article 45 of the GDPR, we are nonetheless satisfied that appropriate safeguards are in place for ensuring the security of this data and for ensuring enforceable legal rights for accessing this data (article 46 of the GDPR). We inform our clients within our privacy notice of data transfers outside of the EU.
Time limits for erasing our data	See our retention policy below and information audit and data mapping exercise for further detail.
Information security	Please see the safeguards set out below.

We receive personal data in respect of our clients' legal matters and our staff. In many instances personal data is processed because this is necessary either to fulfil the terms of the contract between us and the client or employee or because it is necessary to comply with legal requirements. In order to work with our clients and staff it is necessary to obtain their data, store and use their personal information. This will include sharing it at certain points with other parties, for example, with opponents in the case of clients and tax officials in the case of employees. It may

also involve, in the case of working with clients, disclosing information where required to do so by law such as under anti-money laundering legislation and retaining a small amount of personal data after a file has been destroyed to comply with rules on conflicts of interest. We consider such processing to be necessary and permitted under the GDPR and associated legislation.

Upon receiving client enquiries we may in the future contact those individuals via a newsletter or similar provided that we have a clear opt out option upon receipt of the communication. We will provide the individual with clear information on how to opt out in the first of such communications at the latest (this is permitted under the GDPR Article 21.4).

We consider such processing to be permitted under the 'legitimate interests' condition (see recital 47). We have also had regard to the separate rules on marketing such as the 'soft opt in' requirements for email set out in the Privacy and Electronic Communications Regulations. We will balance our interests in promoting our services with those of the individuals we contact and will not rely upon the 'legitimate interests' condition where on a particular set of facts it would be unfair to the individual concerned. For example, we will not assume that minors or other more vulnerable individuals can be 'opted in' for these purposes in this manner and will obtain express consent from the appropriate person before sending any such communications.]

In scenarios other than those set out above, we will generally speaking obtain express affirmative client consent to any data processing. This will typically involve explaining to the client within a privacy notice in our engagement documents how their information will be used and obtaining their instructions to proceed on that basis. We will not obscure consents by placing this within a detailed set of terms without specifically flagging the issue up. We do reserve the right to obtain consent verbally and retain a very clear record of what the relevant individual was told and agreed to and when. We will not necessarily obtain a fresh consent however where the modified use which we wish to make of client information is so closely linked to our original instructions that it will not come as any surprise to the client that their information is being used in this way. For example, if in our privacy notice to clients we have stated that we use a particular outsourcer or cloud provider we will not ordinarily need to seek express consent to switch to a comparable provider as a business where no material risks are posed to the client's information or rights. Whereas if we have never informed the client about outsourcing and we decide to outsource legal work on their file overseas we should seek their express consent. This because outsourcing core work overseas is not a necessary method of delivering our services to the client and so separate consent should be sought. We will retain records of client consents on the file and staff consents on the personnel file i.e. the retainer and contract / staff handbook sign off. We will exercise particular caution in obtaining consent for new uses of any sensitive personal data (i.e. race or ethnicity, political opinions and trade union membership, religious beliefs, health, sex life and genetic or biometric data) which we hold (there are greater restrictions on handling such information).

We do sometimes work with sensitive personal data (i.e. race or ethnicity, political opinions and trade union membership, religious beliefs, health, sex life and genetic or biometric data) which we hold. There are greater restrictions on handling such information. For clients, working with this information will often be necessary in order to pursue or defend their legal matter. In personal injury cases details of health must be processed for example. For staff this will typically be in order to comply with employment or equality legislation, namely around making reasonable adjustments and monitoring absences. Using sensitive information to pursue legal claims or comply with employment legislation is permitted under GDPR. However in order to be prudent and ensure best practice we are nonetheless transparent with staff and clients about how such information is used and seek agreement to information being used in this way in the respective contracts.

Risk assessment

In accordance with ICO guidance we have made an assessment of the risks posed to the information which we hold. This has been done to inform our policies and procedures on ensuring compliance and security of information in practice. In particular, we have assessed our information's sensitivity, financial value and what damage or distress could be caused if there was a security breach (e.g. if the information was destroyed, corrupted or improperly accessed by a third party). We have also considered the nature of our business and our working environment. Having done so, we have assessed the work across our firm as posing a moderate risk. The reasons for this are as follows[1]:

- as a law firm we recognise that our operations automatically carry a certain level of risk in that we will handle personal and business affairs on a confidential basis;
- We will hold data in relation to the pursuance of personal injury claims including medical records, personal information required to pursue a claim including private details from you or any party to a case/claim.
- Information held from a clients medical history or medical records is considered sensitive and we have assessed how this information is stored and processed.
- The members of staff involved are senior with considerable experience with paper light/paperless working practices.
- The manner in which data is shared will be encrypted, or where posted securely via couriers or guaranteed delivery

Our approach to managing risk and ensuring GDPR compliance

The outcome of our risk assessment above has informed the policies and procedures developed by our firm and the training provided to staff.

We have named an Information Officer to oversee compliance and best practice in this area[2]. The Information Officer duties will include the following:

- promote good data protection knowledge and best practice in the business including ensuring that there is appropriate training;
- monitor compliance in practice including periodic audits;
- provide advice on data protection impact assessments (see below) and monitor performance in practice in this respect;
- act as a point of contact for the ICO.

In terms of ensuring that our staff manage information safely and in accordance with the requirements of the GDPR, we:

- have set out in our office manual a clear policy for staff on the standards expected when working with business information, including in the context of:
    - client confidentiality and data protection, including guidance on the data protection principles including use of information for specified purposes only and keeping information up to date and also a procedure for processing subject access requests and the exercise of other rights under the GDPR;
    - information security and acceptable use policies, including standards on keeping information safe in the office, on the go and when working at home;
    - publicity policies, including a policy covering use of email, social media and adding content to our website;
    - bogus law firm and fraud risks, including the need to verify the identity of solicitors we work with and exercising great caution in the context of banking information;
    - file retention and destruction;
- train all staff on confidentiality, how to keep information safe and the requirements of the General Data Protection Regulation[3] ('GDPR') as far as this is relevant to their role. There is induction training for all new staff and rolling refresher training every 2 years. See our learning and development standards for further information.

Security measures

In addition, we work hard to make sure that our infrastructure and processes as a business maintain the security of our information. We have obtained expert input from our IT support who is adept in risk management and security measures in ensuring best practice in the following areas:

1) Encryption of devices such as laptops;

2) Anti-virus and anti-malware software;

3) Firewalls;

4) Disaster recovery systems and backups;

5) Software updates / patching;

6) Secure remote connections i.e. a VPN (virtual private network).

Patches / software updates will be deployed without delay and if IT assets need to be disposed of we will make use of a reputable contractor for this purpose who are ISO27001 or equivalent certified.

Guidance and training is provided to staff to ensure that they do not inadvertently do anything which could undermine our infrastructure. More detail is set out in our acceptable use standards for staff.

Our staff manual includes a requirement to inform our Information Officer of proposed contracts to share information with third parties in order to ensure that the contract contains the paragraphs required by the SRA in terms of outsourcing and the GDPR. More detail is set out in our Outsourcing Policy.

Privacy notices

We are registered with the ICO and provide a privacy notice to every client within our standard terms and conditions to explain how we use their information. We make use of template privacy notices for this purpose which detail the following information in as clear and transparent a manner as possible:

- who we are;
- the contact details for our information officer;
- how we propose to process the information we are gathering (including identifying the third parties with whom we typically will be sharing information);
- why we are proposing to use it in this way;
- what condition or conditions we are relying upon to use information in this way (see above for the common conditions we rely upon). Where we rely upon consent we will highlight the right to withdraw consent. Where we need the information to comply with the law or to deliver the contract for services to the client we will explain that we may not be able to act in the matter without receiving the necessary information. For marketing which relies upon the 'legitimate interests' condition we specifically explain that we make use of established relationships to raise awareness of changes and services which we feel may be of interest;

- whether information is to be transferred outside of the EU and, if so, upon what safeguards or other grounds we rely in order to do this (see above);
- how long their information will be stored for, including our right to retain papers in order to exercise a lien and to demonstrate a legally admissible record at a later date of the work we have performed should it be necessary to do so;
- a reminder of the rights to access information, have it rectified or erased and where applicable to have it delivered in a 'portable' format such as a CSV file;
- the right to lodge a complaint with the Information Commissioner's Office ('ICO') about how personal data has been handled;
- details of any automated decision making processes (including profiling) which we make use of (which we do not anticipate currently).

While we acknowledge that under the GDPR privacy notices should also be given to individuals whose personal data we hold because it has been given to us by someone else, generally speaking such information is held confidentially and is privileged. For example, a client may give us information about other individuals connected to their legal matter but this will typically be confidential and privileged. As such we would not be required to provide such a privacy notice under the GDPR (Article 14.5(d)). In other cases we will however take steps to provide the necessary information about how we handle personal data to other individuals within a reasonable time period of receiving it and in any event within one month (Article 14.3).

Our website

We take care to ensure that our website is secure (see above), up to date, does not infringe copyright and is compliant with SRA requirements and applicable accessibility standards. Our office manual sets out a procedure for approving web content and the standards expected in this respect.

Our website provides appropriate information to users on privacy and cookies.

Identity theft and bogus law firms

We have set out in our office manual:

- a requirement to verify the authenticity of unknown law firms which we work with (together with clear guidance on how to do so);
- guidance on the warning signs of bogus law firms; and
- set out a procedure of oversight by our COLP where issues arise.

Our COLP has taken responsibility for considering SRA guidance on bogus law firms[4] and fraud in the context of our business and staying up to date with scam alerts and trends. Trends or alerts which pose a particular risk to us will be shared

by our COLP with colleagues in a particular department or throughout the firm as appropriate.

In order to minimise the risks of identity theft a member of staff periodically:

- conducts internet searches against the name of our firm and our senior lawyers to check whether our identity is being misused; and
- checks our authorisation on the Law Society Find a Solicitor web service to ensure that the details remain accurate and up to date;
- keeps a record of these checks.

Policy up to date and live from January 2021