THOMAS FLAVELL + SONS SOLICITORS

Document title:	**Data Protection policy**

Issue date:	**June 2019**	**Review date:**	**June 2024**

Version:	1	**Issued by:**	Lindsey Dewart

Scope:	Clients

Associated documentation:	Subject Access Request Form
Appendices:	None
Approved by:	Directors
Date:	Issued June 2019

Review and consultation process:	Annual review from issue date. We reserve the right to amend the policy without notice.
Responsibility for Implementation & Training:	Day to day responsibility for implementation: Compliance officers Day to day responsibility for training: Compliance officers

---

Revisions History:		
Date:	**Author:**	**Description:**
June 2023	Lindsey Dewart	Subject Data Access Request form removed and created as stand alone fillable PDF.

Distribution	Document to be stored on the website If you have any suggested changes to this document, then please notify the Practice Manager. The current version of this document is stored on the website. Any copies that are printed will be deemed to be invalid within 24 hours of printing.

1. Data protection principles

TFS is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

a. This policy applies to all personal data processed by the firm.
b. The Responsible Person shall take responsibility for the firm's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The firm shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, TFS shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Clients have the right to access their personal data and any such requests made to TFS shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the firm must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The firm shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the firms systems.

5. Data minimisation

a. The firm shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The firm shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the firm has put in place a Data Retention & Destruction Policy for each area in which personal data is processed and review this process annually.

b. The Data Retention & Destruction Policy shall consider what data should/must be retained, for how long, and why. Details of which are contained in the firms Terms and Conditions.

8. Security

a. The firm shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the firm shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

10. Your rights in relation to your Data

This policy outlines the rights that data subjects have, under the General Data Protection Regulation (GDPR), in relation to the data about them that we hold. Data subjects, for the purposes of this policy, includes clients and third parties.

11. The right to be informed

In order to keep you informed about how we use your data, we have a privacy notice for clients. You can obtain a copy of the privacy notice from our website.

Our privacy notices set out:

a) the types of data we hold and the reason for processing the data;
b) our legitimate interest for processing it;
c) details of who your data is disclosed to and why, including transfers to other countries. Where data is transferred to other counties, the safeguards used to keep your data secure are explained;
d) how long we keep your data for, or how we determine how long to keep your data for;
e) where your data comes from;
f) your rights as a data subject;
g) your absolute right to withdraw consent for processing data where consent has been provided and no other lawful reason for processing your data applies;
h) your right to make a complaint to the Information Commissioner if you think your rights have been breached;
i) whether we use automated decision making and if so, how the decisions are made, what this means for you and what could happen as a result of the process;
j) the name and contact details of our data protection officer.

12. The right of access

You have the right to access your personal data which is held by us. You can find out more about how to request access to your data by reading our Subject Access Request section.

13. The right to correction

If you discover that the data we hold about you is incorrect or incomplete, you have the right to have the data corrected. If you wish to have your data corrected, you should contact Lindsey Dewart our Practice Manager.

Usually, we will comply with a request to rectify data within one month unless the request is particularly complex in which case we may write to you to inform you we require an extension to the normal timescale. The maximum extension period is two months.

You will be informed if we decide not to take any action as a result of the request. In these circumstances, you are able to complain to the Information Commissioner and have access to a judicial remedy.

Third parties to whom the data was disclosed will be informed of the rectification.

14. The right of erasure

In certain circumstances, we are required to delete the data we hold on you. Those circumstances are:

a) where it is no longer necessary for us to keep the data;
b) where we relied on your consent to process the data and you subsequently withdraw that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data;
c) where you object to the processing (see below) and the Company has no overriding legitimate interest to continue the processing;
d) where we have unlawfully processed your data;
e) where we are required by law to erase the data.

If you wish to make a request for data deletion, you should contact Lindsey Dewart, the Practice Manager.

We will consider each request individually, however, you must be aware that processing may continue under one of the permissible reasons. Where this happens, you will be informed of the continued use of your data and the reason for this.

Third parties to whom the data was disclosed will be informed of the erasure where possible unless to do so will cause a disproportionate effect on us.

15. The right of restriction

You have the right to restrict the processing of your data in certain circumstances.

We will be required to restrict the processing of your personal data in the following circumstances:

a) where you tell us that the data we hold on you is not accurate. Where this is the case, we will stop processing the data until we have taken steps to ensure that the data is accurate;
b) where the data is processed for the performance of a public interest task or because of our legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether our legitimate interests mean it is appropriate to continue to process it;
c) when the data has been processed unlawfully;
d) where we no longer need to process the data but you need the data in relation to a legal claim.

If you wish to make a request for data restriction, you should contact Lindsey Dewart, the Practice Manager.

Where data processing is restricted, we will continue to hold the data but will not process it unless you consent to the processing or processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible unless to do so will cause a disproportionate effect on us.

You will be informed before any restriction is lifted.

16. The right to data portability

You have the right to obtain the data that we process on you and transfer it to another party. Where our technology permits, we will transfer the data directly to the other party.

Data which may be transferred is data which:

a) you have provided to us; and
b) is processed because you have provided your consent or because it is needed to perform the contract between us; and
c) is processed by automated means.

If you wish to exercise this right, please speak to the person acting on your matter.

We will respond to a portability request without undue delay, and within one month at the latest unless the request is complex or we receive a number of requests in which case we may write to you to inform you that we require an extension and reasons for this. The maximum extension period is two months.

We will not charge you for access to your data for this purpose.

You will be informed if we decide not to take any action as a result of the request, for example, because the data you wish to transfer does not meet the above criteria. In these circumstances, you are able to complain to the Information Commissioner and have access to a judicial remedy.

The right to data portability relates only to data defined as above. You should be aware that this differs from the data which is accessible via a Subject Access Request.

17. The right to object

You have a right to require us to stop processing your data; this is known as data objection.

You may object to processing where it is carried out:

a) in relation to the Company's legitimate interests;
b) for the performance of a task in the public interest;
c) in the exercise of official authority; or
d) for profiling purposes.

If you wish to object, you should do so by contacting the person handling your case.

In some circumstances we will continue to process the data you have objected to. This may occur when:

a) we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights; or
b) the processing is required in relation to legal claims made by, or against, us.

If the response to your request is that we will take no action, you will be informed of the reasons.

18. Right not to have automated decisions made about you

You have the right not to have decisions made about you solely on the basis of automated decision-making processes where there is no human intervention, where such decisions will have a significant effect on you.

However, we may carry out automated decision making with no human intervention in the following circumstances:

a) when it is needed for entering into or the carrying out of a contract with you;
b) when the process is permitted by law;
c) when you have given explicit consent.

19. Subject Access Request

You have a right, under the General Data Protection Regulation, to access the personal data we hold on you. To do so, you should make a subject access request, and this policy sets out how you should make a request, and our actions upon receiving the request.

20. Definitions

“Personal data” is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including your name.

“Special categories of personal data” includes information relating to:

a) race

b) ethnic origin

c) politics

d) religion

e) trade union membership

f) genetics

g) biometrics (where used for ID purposes)

h) health

i) sex life or

j) sexual orientation.

21. Making a request

Although subject access requests may be made verbally, we would advise that a request may be dealt with more efficiently and effectively if it is made in writing. If you wish to make a request, please use the Subject Access Request form.

Requests that are made directly by you should be accompanied by evidence of your identity. If this is not provided, we may contact you to ask that such evidence be forwarded before we comply with the request.

Requests made in relation to your data from a third party should be accompanied by evidence that the third party is able to act on your behalf. If this is not provided, we may contact the third party to ask that such evidence be forwarded before we comply with the request.

22. Timescales

Usually, we will comply with your request without delay and at the latest within one month. Where requests are complex or numerous, we may contact you to inform you that an extension of time is required. The maximum extension period is two months.

23. Fee

We will normally comply with your request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact you requesting a fee. This fee must be paid in order for us to comply with the request. The fee will be determined at the relevant time and will be set at a level which is reasonable in the circumstances.

In addition, we may also charge a reasonable fee if you request further copies of the same information.

24. Information you will receive

When you make a subject access request, you will be informed of:

a) whether or not your data is processed and the reasons for the processing of your data;

b) the categories of personal data concerning you;

c) where your data has been collected from if it was not collected from you;

d) anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards utilised to ensure data security;

e) how long your data is kept for (or how that period is decided);

f) your rights in relation to data rectification, erasure, restriction of and objection to processing;

g) your right to complain to the Information Commissioner if you are of the opinion that your rights have been infringed;

h) the reasoning behind any automated decisions taken about you.

25. Circumstances in which your request may be refused

We may refuse to deal with your subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse your request, we will contact you without undue delay, and at the latest within one month of receipt, to inform you of this and to provide an explanation. You will be informed of your right to complain to the Information Commissioner and to a judicial remedy.

We may also refuse to deal with your request, or part of it, because of the types of information requested. For example, information which is subject to legal privilege. Where this is the case, we will inform you that your request cannot be complied with and an explanation of the reason will be provided.

26. Data breach notification

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches:

a) access by an unauthorised third party;

b) deliberate or accidental action (or inaction) by a data controller or data processor;

c) sending personal data to an incorrect recipient;

d) computing devices containing personal data being lost or stolen;

e) alteration of personal data without permission;

f) loss of availability of personal data.

Breach detection measures

We have implemented internal measures to assist us in detecting a personal data breach, these include, but are not limited to, using Multi-factor authentication to access our technology, destroying documents securely, 90 day password changes, Network cyber security hardware and software is installed to provide extra protection and ongoing training in identifying malicious intent is carried out with staff.

Investigation into suspected breach

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by Lindsey Dewart, Practice Manager who will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

When a breach will be notified to the Information Commissioner

In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

a) a description of the nature of the personal data breach including, where possible:

   i. the categories and approximate number of individuals concerned; and

   ii. the categories and approximate number of personal data records concerned

b) the name and contact details of the appointed officer where more information can be obtained;

c) a description of the likely consequences of the personal data breach; and

d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

When a breach will be notified to the individual

In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

a) a description of the nature of the breach

b) the name and contact details of the appointed compliance officer where more information can be obtained

c) a description of the likely consequences of the personal data breach and

d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Record of breaches

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.