

privacy notice.



Thompson Gill Family Law takes its responsibility for protecting your data very seriously. This notice is designed to help you understand everything you need to know about the way Thompson Gill Family Law collects, uses, protects and shares your personal information, what your legal rights are and how to exercise them.

We encourage you to read this whole notice to confirm that you are clear on our practices and processes. We have tried to avoid jargon and to keep this as simple as possible. If, however, there is anything you do not understand, or if you have any questions, please do contact us.

This notice may be updated from time to time. We will use our best efforts to keep you informed if there are any changes to the way we process your personal data in future.

1. Who we are

Thompson Gill Family Law, whose registered office is at Arkwright House, Parsonage Gardens, Manchester M3 2LF, is the "Data Controller" of your personal information. This means that we decide how and why your data is processed and are responsible for ensuring that we comply with relevant data protection laws when processing your personal information. We are registered with the Information Commissioner's Office (ICO) under registration number ZC154413.

2. What is personal information?

Personal information is data that allows us to identify you or that relates to you. This includes your name, address, telephone number but also less obvious things such as analysis of your use of our website or your attendance at a webinar or marketing event.

Personal information that is considered sensitive in nature is given additional protection under data protection laws. This "special category" data includes information about your health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, your genetic and biometric data and information concerning your sex life or sexual orientation.

3. The information we collect

We only collect personal information about you in connection with providing our services and running our business. We may collect, use, store and transfer different types of personal information about you, either directly from you or from other sources, to achieve those purposes. The types of information we process about you may include:

Type of personal information

Examples

Identification details	Name, any previous names, username or similar identifier, title, marital status, date and place of birth, gender, nationality, employer, job title and employment history, family details and relationships (including information relating to children), facial images, video recordings and call recordings that may identify you, identification numbers and documents issued by government bodies or agencies (such as your national insurance number, passport number, tax identification number and driving licence number) and utility bills
Contact details	Billing address (including proof of address), delivery address, email address and telephone numbers
Financial information	Bank details, bank account or payment card details and information regarding your assets, income and source of funds
Case details	Details about payments to and from you, information about you which is relevant to a matter on which we are advising you or another client, marriage details, country of birth, other details of services you have purchased from us and your feedback
KYC, credit, anti-fraud and sanctions data	Credit history, credit score and information received from various anti-fraud and sanctions databases relating to you
Special category data	Information about your health, racial or ethnic origin, your genetic and biometric data, information about your sex life or sexual orientation, religious or philosophical beliefs
Criminal convictions information	Information relating to your criminal convictions and offences
Marketing and communications data	Communications and marketing preferences
Technical identifying data	Date time and duration of any call with us or our specialist third-party telephony and call-handling provider. Information which can be traced back to you including your internet protocol (IP) address, your login data, information about how you interact with and use our website and services, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, device ID and other technology on the devices you use to access our website

4. Why we collect your personal information

The law requires us to have a “lawful basis” for processing your data. The main reasons we use your personal information is to:

- 1. Perform and fulfil our contractual obligations:** This is the main purpose for holding your data. The law allows us to process your data for the purposes of performing a contract or for the steps necessary to enter a contract, for example our engagement letter with you. We cannot provide legal advice or represent you in court without it;
- 2. Comply with a legal obligation:** If the law requires us to, we may need to collect and process your personal information to comply with our legal obligations. For example, to carry out anti-money laundering checks, to comply with our regulatory requirements, to detect and prevent fraud or to pass on details of people involved in fraud

3. Legitimate interests: In specific situations, we require your personal information to pursue our legitimate interests in a way which might reasonably be expected as part of running our business, and which does not materially impact your rights, freedom or interests. For example, as a regulated law firm, we have a legitimate interest in using your information where this is necessary or appropriate to provide legal advice to our clients, to manage our relationship with prospective clients, hosting you and others at our offices or at virtual or in-person events, to contact and deal with individuals providing services to the firm, in keeping you informed if you have requested that, ensuring appropriate standards and compliance with our policies, controls, practices or procedures or to satisfy our external auditors or regulators or other third parties where necessary; and

4. Consent: In some circumstances, we can collect and process your personal information with your consent for a specified purpose or service. For example, for referring clients to other firms or when you tick a box to receive email newsletters or updates or other future marketing purposes.

Where the processing of “special category” data is necessary, this requires an additional justification to those lawful bases set out above. Processing this special category data is necessary for the establishment, exercise or defence of legal claims, for preventing or detecting unlawful acts or for statutory or government purposes; otherwise, we will only process this special category data with your explicit consent.

For ease, the specific purposes for which we will use your personal information have been summarised in the table below:

Purpose/Use	Type of Data	Lawful basis	Special Category Condition (if applicable)
Call recording and telephony data – when you contact us via our main telephone lines, you may get put through to our specialist third-party telephony and call handling service provider, who will take basic contact details but may record the conversation and collect associated metadata.	Identification details, contact details, brief nature of the matter, any financial or special category data that you choose to disclose during the conversation, technical identifying data	Legitimate Interests – for for training, quality assurance, establishing an accurate record of the request and contact details provided by you to enable a member of our firm to respond to you and compliance with a legal obligation of being able to run suitable conflict checks to establish if our firm is able to assist you.	We do not generally look to collect special categories of personal data for this purpose. Where you volunteer special category personal data – consent and/ or the establishment, exercise or defence of legal claims .
Initial enquiry or complaint – responding to your request for information or an initial meeting either by phone, email or the online enquiry form on our website and responding to a complaint made to us.	Identification details, contact details, brief nature of the matter/information submitted as part of the complaint.	Legitimate Interests – to to provide information requested by a potential client or to respond to a complaint made by a client or third party. We will only use this information for the purpose for which it has been provided by you. In all other cases, we will process this information with consent .	N/A

Table continued.

Client onboarding, risk management, and other legal obligations – we obtain information about our clients/potential clients and their representatives and beneficial owners to check whether we can act for them as a new or existing client and to carry out all of our regulatory compliance requirements and comply with legislation, including conflicts of interest, background screening, money laundering, terrorist financing, fraud and sanctions. We may also process such information for the purposes of risk management. These procedures may include a digital identity, verification and facial similarity check through our third-party service provider. We and they may process your biometric data taken from a screenshot of your photo identification document and a short video of you to verify your identity. We may also collect and disclose personal information under legislation and orders from regulators and the courts. We would disclose only to those people and bodies who are entitled to receive the information.	Identification details, contact details, financial information, case details, KYC, credit, anti-fraud and sanctions data, special category data, criminal convictions information.	For all information - compliance with a legal obligation or legitimate interest. As a regulated law firm, we have a legitimate interest in conducting appropriate risk management practices and procedures and to perform the services in our engagement letter. For AML and identification and verification checks, we have a legal obligation to comply with regulations and legislation (e.g. the Money Laundering Regulations).	For biometric special category data processed as part of identity verification and facial recognition checks – consent / explicit consent. For all other special category and criminal data – preventing or detecting unlawful acts, regulatory requirements, suspicion of terrorist financing or money laundering.
Direct legal services and contentious and non-contentious legal advice – we obtain information about you where it is necessary or appropriate to deliver our services to you, advise you on your legal position, structure your agreements and represent you in contentious matters and proceedings as well as engaging service providers, managing payments, fees and charging and collecting and recovering money owed to the firm.	Identification details, contact details, financial information, case details, special category data, criminal convictions information, marketing and communications data	For all information – legitimate interests or contractual obligation. As a regulated law firm, we have a legitimate interest in using your information where this is necessary or appropriate to provide you or our clients legal advice, and to perform the services in our engagement letter.	For all special category and criminal data – the establishment, exercise or defence of legal claims

Table continued.

Case management –to provide you with legal services, we share your data with external experts including barristers, courts or other experts	Identification details, contact details, financial information, case details, special category data, criminal convictions information	For all information – legitimate interests or contractual obligation. As a regulated law firm, we have a legitimate interest in using your information where this is necessary or appropriate to provide you or our clients legal advice, and to perform the services in our engagement letter.	For all special category and criminal data (and any data related to children) – the establishment, exercise or defence of legal claims
Practice management – we may need to share information with third party organisations when requested, audited or investigated by our auditors, the Solicitors Regulation Authority, other regulators or government bodies or our insurers. We may also need to share information to administer and protect our business and our website, including troubleshooting, data analysis, testing, system maintenance, support and reporting and hosting of data. We may also request reviews or feedback on the services we provide.	Identification details, contact details, financial information, case details, special category data, criminal convictions information, technical identifying data.	For all information shared with government, financial or regulatory bodies – compliance with legal obligation, including our regulatory and legislative requirements. For information to protect our business and our website– legitimate interest in the provision and administration of a secure website for use by clients and other third parties. We also have a legitimate interest in seeking reviews or feedback to improve the quality of services offered and to better understand clients’ needs.	For all special category and criminal data – statutory and government purposes
Service providers – we may collect information about service providers with their provision of services to us either directly or as a representative of a provider of services to us.	Identification details, contact details, financial information, KYC, credit, anti-fraud and sanctions data, special category data, criminal convictions information	We have a legitimate interest in contacting and dealing with individuals involved in providing services to the firm.	We do not generally look to collect special categories of personal data and criminal convictions information for this purpose, other than where we are required to do so to meet our legal obligations – see risk management, and other legal obligations above.

Table continued.

Marketing, events, legal updates and seminars – as part of our marketing analysis, we may track how you interact with our marketing activities, materials or links. We may use this data analytics to help improve our website and services, our marketing and customer experiences. We are able to record this information against your email address by placing 'cookies' on your device. You can control cookies through the preferences on your browser or dedicated browser add-ons. We may ask you to provide a limited amount of personal information if you wish to attend any events we host or receive any updates or firm news. We use this information to communicate with you about these events to ensure you are an appropriate audience and to conduct analysis for marketing. If there are professional photographers and videographers at our event, the footage may identify individuals which could be used for promotional and marketing purposes. Please let us know if you do not want your image to be used in this way.	Identification details, contact details, marketing and communications data, technical identifying data	We have a legitimate interest in keeping you informed about events and updates that may be of interest. For all other purposes – consent, for example where you have opted-in to receive communications. You may opt out of receiving marketing communications from us at any time.	N/A
Staff recruitment – at the appropriate time, we ask job applicants to provide personal information including for the purposes of making reasonable adjustments. We will also conduct checks to verify your identity, the information in your application and obtain further information about your suitability for a role within our firm. In some cases, this may include special category data and criminal convictions information. Our background checks may include right to work checks through a third-party provider, which may include processing biometric data from a photo of you.	Identification details, contact details, financial information, KYC, credit, anti-fraud and sanctions data, special category data, criminal convictions information	We have a legitimate interest in processing and retaining all information related to recruitment, to ensure we employ (now and in future) the appropriate staff to comply with our legal, regulatory and ethical duties and in monitoring to ensure our practices are fair and inclusive.	For special category data and criminal information – employment protection or regulatory requirements.

5. Where we collect your personal information from

We collect your personal information in various ways and from various sources.

In some circumstances, we can collect and process your personal information when you provide it to us (for example by completing an online form or providing it either to our specialist third-party telephony and call handling service provider or directly to a representative of the firm before, during or after your matter) or when it is provided to us by others (your opponent's solicitors or your representative, for example).

Other sources include our service providers and third parties such as experts, witnesses, solicitors, barristers, investigators, anti-fraud and anti-money laundering databases, sanctions lists, government agencies and publicly accessible registers or sources of information including Companies House and company websites and other public sources, credit reference agencies, recruitment agencies and referees, professional networking sites and social media.

We may also actively gather your personal information such as technical identifying data or metadata of your call, for example through automated technologies or interactions with our website where our systems and cookies may gather data from your computer equipment or via our third-party telephony and call handling service provider.

6. How we share your personal information

We do not sell you information or make it generally available to others. We may, however, have to share your personal information with trusted third parties. These third parties include:

- barristers, experts, courts and accountants;
- the counterparty and their legal representatives;
- regulators or government institutions or authorities;
- referral firms and recruiters; and
- organisations and services providers where it is necessary to provide or receive services to achieve our business purposes, for example identification and e-verification providers, case management system providers, accounting software providers etc.

We only do this where we are legally required to do so, where it is necessary to provide you with legal services or for the effective operation of our legal practice. We provide only the information required for the third party to perform their services and specify in their contract the purpose for which it can be used. If we stop using their services, any of your personal information held by them will either be deleted or anonymised.

The third parties with whom we share your information will either process it in their capacity as a "controller" or as our "processor". Where they process your personal information on our behalf as a processor (for example our cloud storage or IT provider), we remain primarily responsible to you for ensuring they keep your information safe and secure. Where they process your personal information as a controller (for example, opposing counsel or a regulator), they are legally responsible to you for how they process your information.

7. How long we keep your personal information

We only keep your personal information for as long as is necessary for the purpose(s) for which it was provided. This includes the purposes of complying with any legal, regulatory, accounting and reporting requirements or obligations to retain the information for a minimum period, to conduct legal work, limitation periods for taking legal action including for the establishment and defence of legal claims (i.e. respond to any future legal claims), the need to comply with government and regulatory investigations, to comply with our professional indemnity insurance requirements, good practice and our business purposes.

Generally, we retain client files for seven years following conclusion of the matter. This may be longer in certain circumstances, for example twelve if executed as a deed or until a child reaches the age of 18 if it is a children matter. This is to enable us to meet the obligations set out above. Calls to members of staff within our firm are not recorded. However, were recordings to be made of calls between you and our specialist third-party telephony and call handling service provider, they would be retained by them for a standard period of 90 days from the date of the call (during which time they would only be accessible via an encrypted connection).

8. Protecting your personal information

We take our responsibility for protecting your data very seriously.

The information you provide us is confidential and often extremely sensitive and may be subject to legal professional privilege. We treat your data with the upmost care. We take appropriate steps to help maintain the security of our information systems and processes and to prevent the accidental loss, destruction or unauthorised disclosure of the personal information we process.

Where information is privileged, we have a strict legal duty to keep it confidential. We will not disclose privileged material to any third party unless we are legally compelled to do so or you provide express permission. While we use IT providers and cloud storage, they are “processors” for data protection purposes and bound by strict confidentiality agreements that do not waive your privilege.

Please note, our website may contain links to other websites. Once you have used these links to leave our site, please note that we do not have any control over those other websites and nor are they governed by this Privacy Notice. We cannot, therefore, be responsible for the protection and privacy of any information you provide whilst visiting such sites. Please exercise caution and look at the privacy statement or policy applicable to the website in question.

9. Your legal rights

Under data protection laws, you have rights regarding your personal information. However, these rights are not absolute and may be limited by our professional obligations and legal professional privilege.

Under certain conditions, you may have the right to:

a) Access – request a copy of the personal information we hold about you (commonly known as a “subject access request”). Please note that we generally cannot disclose information that would reveal personal data about another person (e.g. your spouse) unless they consent;

b) Correction – ask us to correct any inaccurate or incomplete information we hold about you;



c) Erasure – ask us to erase your personal information where we no longer have a lawful ground or good reason for continuing to process it. Please note, however, that we may not always be able to comply with your request for specific legal reasons, including that we are usually required by the Solicitors Regulation Authority and our professional indemnity insurers to retain client files for a minimum of six years (and sometimes longer in cases involving children and pension sharing orders). Another reason for being unable to erase all data is if the data is still required for legal claims or regulatory compliance;

d) Objection – where processing is based on consent, you can ask us to stop that particular processing by withdrawing your consent (for example for direct marketing purposes). You can also object to any processing based on our legitimate interests unless we have compelling legitimate grounds to do so which outweigh any prejudice to your data protection rights;

e) Restriction of Processing – ask us to restrict how we use your personal information in certain circumstances, such as if you want us to establish the data's accuracy;

f) Data Portability – ask that we transfer your personal information to you or a third party (for example another lawyer) in a structured, commonly used machine-readable format. Please note that this right only applies to information which you initially gave us or provided consent for us to use;

g) Automated Decision Making - we do not make decisions about you based solely on automated processing where those decisions produce legal effects or similarly significant effects; and

h) Withdraw Consent - where we rely on your consent to process personal data, you may withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn.

We are obliged to keep your personal information accurate and up to date. Please help us to do this by advising us of any changes.

In certain circumstances, we may need to restrict your rights to safeguard public interest (for example the detection or prevention of crime) and our interests (for example the maintenance of legal privilege).

You will not have to pay a charge for exercising your rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive or if you request further copies of the same information that has already been provided to you.

We may need to ask you for information to confirm your identity, to clarify the request, or to help us locate the relevant personal data. Where clarification is reasonably required, the period for responding may be paused until we receive the necessary clarification.

When responding to a right of access request, we are required to carry out searches that are reasonable and proportionate. We are not required to conduct searches that would be disproportionate in the circumstances.

We try to respond to all legitimate requests within one month from the later of: a) the date of your request; or b) when we receive any further information from you that we reasonably request, for example to confirm your identity or clarification to help speed up our response.

Occasionally it could take us longer if your request is particularly complex or you have made a number of requests. In this case we will notify you and keep you updated.

We may refuse to comply with a request, or charge a reasonable fee, where permitted by law, including where a request is vexatious or excessive. If we refuse a request, we will explain the reason, subject to any legal or regulatory restrictions.

10. How to contact us

If you have any questions about this Privacy Notice, how we handle your personal information or how we maintain security of our information, and to exercise your rights to access information, please contact Amy Thompson by email at amy.thompson@tgfl.co.uk, by phone on 0208 076 8484 / 0161 560 9993 or by post at Arkwright House, Parsonage Gardens, Manchester M3 2LF.

If you believe the information we hold is incorrect or out of date, please let us know so that we can update our records.

11. Your right to complain

If you are unhappy with how we use your personal information, or our response to any request by you to exercise your data protection rights, you have the right to make a data protection complaint to us by using the contact details below. A data protection complaint is a complaint about how we have processed personal data, including a complaint that we have not complied with data protection law. We request that any complaint be first brought to our attention so that we can consider your concern, investigate matters and seek to resolve the issue.

Please send data protection complaints to Amy Thompson by email at amy.thompson@tgfl.co.uk or to our contact@tgfl.co.uk email, by phone on 0208 076 8484 / 0161 560 9993 or by post at Arkwright House, Parsonage Gardens, Manchester M3 2LF.

We will acknowledge your complaint within 30 days of receipt. We will take appropriate steps to investigate and respond to your complaint. This may include reviewing the relevant processing activities, considering any relevant documents or communications, speaking to members of staff involved, and assessing whether any remedial action is required. We will inform you of the outcome of your complaint without undue delay.

You also have the right to complain to your local data protection supervisory authority. For the UK, this is the Information Commissioner’s Office (ICO). Details of the ICO can be found at:

Address: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Website: www.ico.org.uk

Helpline: 0303 123 1113

12. Version Control

Revision Date	Author	Version	Change Summary	Next Review Date
May 2026	Amy Thompson, COLP	0.0	Policy Created	May 2027
June 2026	Amy Thompson, COLP	0.1	Policy Amended to reflect changes introduced by the Data Use and Access Act 2025	May 2027