Crombie Wilkinson Solicitors LLP

Privacy Policy

We take your privacy very seriously. Please read this privacy policy carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event you have a complaint.

We collect, use and are responsible for certain personal data about you. When we do so we are subject to the UK General Data Protection Regulation (UK GDPR).

Key terms

Here is an explanation of some key terms used in this policy:

We, us, our	Crombie Wilkinson Solicitors LLP. We also use the following trading names: Crombie Wilkinson Solicitors, Crombie Wilkinson Ellis Lakin Solicitors and Your Family First.
Personal data	Any information relating to an identified or identifiable living individual
Special category personal data	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership Genetic and biometric data (when processed to uniquely identify an individual) Data concerning health, sex life or sexual orientation
Data subject	The individual who the personal data relates to

Personal data we collect about you

The table below sets out the personal data we will or may collect in the course of providing legal services:

Personal data we will collect	Personal data we may collect depending on why you have instructed us
Your name, address and telephone number Information to enable us to check and verify your identity, eg your date of birth or passport details Electronic contact details, eg your email address and mobile phone number Information relating to the matter in which you are seeking our advice or representation Your financial details so far as relevant to your instructions, eg the source of your funds if you are instructing on a	Your National Insurance and tax details Your bank and/or building society details Details of your professional online presence, eg LinkedIn profile Details of your spouse/partner and dependants or other family members, eg if you instruct us on a family matter or a will Your employment status and details including salary and benefits, eg if you instruct us on matter related to your employment or in which your employment status or income is relevant Details of your pension arrangements, eg if you instruct us on a pension matter or in relation to financial

Personal data we will collect	Personal data we may collect depending on why you have instructed us
purchase transaction Information relating to the matter in which you are seeking our advice or representation, or in relation to our provision of legal services to you generally Information about your use of our IT, communication and other systems, and other monitoring information, eg if using our secure online client portal	arrangements following breakdown of a relationship Your employment records including, where relevant, records relating to sickness and attendance, performance, disciplinary, conduct and grievances, eg if you instruct us on matter related to your employment or in which your employment records are relevant Your racial or ethnic origin, gender and sexual orientation, religious or similar beliefs, eg if you instruct us on discrimination claim Your trade union membership, eg if you instruct us on a discrimination claim or your matter is funded by a trade union Personal identifying information, such as your eye colour or your parents' names, eg if you instruct us to incorporate a company for you Your medical records, eg if we are acting for you in a family matter or employment claim

We collect and use this personal data to provide legal services to you. If you do not provide personal data we ask for, it may delay or prevent us from providing those services.

We may also collect personal data:-

- through our website at www.crombiewilkinson.co.uk including data you provide when you complete a website enquiry form or sign up to a newsletter. Here, we collect your name, postal address, email address, telephone number and any other details you choose to provide us with when you submit your enquiry form (if applicable);

- through your use of the Perfect Portal app.

How your personal data is collected

We collect most of this information from you direct, via our website or via secure online client portal**s** such as Perfect Portal**.** However, we may also collect information:

- from publicly accessible sources, eg Companies House or HM Land Registry;

- directly from a third party, eg: sanctions screening providers, credit reference agencies or client due diligence providers;

- from a third party with your consent, eg: your bank or building society, another financial institution or advisor; consultants and other professionals we may engage in relation to your matter; your employer and/or trade union, professional body or pension administrators; your doctors, medical and occupational health professionals;

- via our website—we use cookies on our website (for more information on cookies, please see our cookies policy on our website at www.crombiewilkinson.co.uk

- via our information technology (IT) systems, eg: via our case management, document management and time recording systems; from door entry systems and reception logs; through automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, email and instant messaging systems;

How and why we use your personal data

Under data protection law, we can only use your personal data if we have a proper reason, eg:

- where you have given consent;

- to comply with our legal and regulatory obligations;

- for the performance of a contract with you or to take steps at your request before entering into a contract; or

- for our legitimate interests or those of a third party.

A legitimate interest is when we have a business or commercial reason to use your personal data, so long as this is not overridden by your own rights and interests. We will carry out an assessment when relying on legitimate interests, to balance our interests against your own.

The table below explains what we use your personal data for and why:-

What we use your personal data for	Our reasons
Providing legal services to you	To perform our contract with you or to take steps at your request before entering into a contract
Preventing and detecting fraud against you or us	For our legitimate interest, ie to minimise fraud that could be damaging for you and/or us
Conducting checks to identify our clients and verify their identity Screening for financial and other sanctions or embargoes Other activities necessary to comply with professional, legal and regulatory obligations that apply to our business, eg under health and safety law or rules issued by our professional regulator	To comply with our legal and regulatory obligations
To enforce legal rights or defend or undertake legal proceedings	Depending on the circumstances: —to comply with our legal and regulatory obligations;

What we use your personal data for	Our reasons
	—in other cases, for our legitimate interests, i.e. to protect our business, interests and rights
Gathering and providing information required by or relating to audits, enquiries or investigations by regulatory bodies	To comply with our legal and regulatory obligations
Ensuring business policies are adhered to, eg policies covering security and internet use	For our legitimate interests, i.e. to make sure we are following our own internal procedures so we can deliver the best service to you
Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests, i.e. to be as efficient as we can so we can deliver the best service to you at the best price
Ensuring the confidentiality of commercially sensitive information	For our legitimate interests, i.e. to protect trade secrets and other commercially valuable information; and to comply with our legal and regulatory obligations
Statistical analysis to help us manage our business, eg in relation to our financial performance, client base, services range or other efficiency measures	For our legitimate interests, ie to be as efficient as we can so we can deliver the best service to you at the best price
Preventing unauthorised access and modifications to systems	For our legitimate interests, ie to prevent and detect criminal activity that could be damaging for you and/or us; and to comply with our legal and regulatory obligations
Protecting the security of systems and data used to provide services	To comply with our legal and regulatory obligations We may also use your personal data to ensure the security of systems and data to a standard that goes beyond our legal obligations, and in those cases our reasons are for our legitimate interests, ie to protect systems and data and to prevent and detect criminal activity that could be damaging for you and/or us
Updating and enhancing client records	To perform our contract with you or to take steps at your request before entering into a contract. To comply with our legal and regulatory obligations; For our legitimate interests, e.g. making sure we can keep in touch with our clients about existing

What we use your personal data for	Our reasons
	and new services
Statutory returns	To comply with our legal and regulatory obligations
Ensuring safe working practices, staff administration and assessments	To comply with our legal and regulatory obligations; and for our legitimate interests, e.g. to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you
Marketing our services to: —existing and former clients; —third parties who have previously expressed an interest in our services; —third parties with whom we have had no previous dealings (including visitors to our website);	For our legitimate interests, i.e. to promote our business to existing and former clients
External audits and quality checks, eg for Lexcel or Investors in People accreditation and the audit of our accounts (*to the extent not covered by 'activities necessary to comply with legal and regulatory obligations' above)*	For our legitimate interests, i.e. to maintain our accreditations so we can demonstrate we operate at the highest standards; and to comply with our legal and regulatory obligations
To share your personal data with members of our group and third parties that will or may take control or ownership of some or all of our business (and professional advisors acting on our or their behalf) in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale or in the event of our insolvency In such cases information will be anonymised where possible and only shared where necessary	Depending on the circumstances: —to comply with our legal and regulatory obligations; —in other cases, for our legitimate interests, ie to protect, realise or grow the value in our business and assets

How and why we use your personal data—Special category personal data

Certain personal data we collect is treated as a special category to which additional protections apply under data protection law:

- *personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership*;
- *genetic data*;

- *biometric data (when used to uniquely identify an individual)*;
- *data concerning health, sex life or sexual orientation*.

Where we process special category personal data, we will also ensure we are permitted to do so under data protection laws, eg:

- we have your explicit consent;
- the processing is necessary to protect your (or someone else's) vital interests where you are physically or legally incapable of giving consent; or
- the processing is necessary to establish, exercise or defend legal claims.

How and why we use your personal data—sharing

See '**Who we share your personal data with**' for more information on the steps we will take to protect your personal data where we need to share it with others.

Marketing

We may use your personal data to send you updates (by email, text message or post) about our services, including exclusive offers, promotions or new services.

We have a legitimate interest in using your personal data for marketing purposes (see above '**How and why we use your personal data**'). This means we do not usually need your consent to send you marketing information. If we change our marketing approach in the future, or there are instances where consent is needed, we will ask for this separately and clearly.

You have the right to opt out of receiving marketing communications at any time by:

- contacting our Marketing team based in our York office (Telephone: 01904 624185 or Email: s.edwards@crombiewilkinson.co.uk)
- using the 'unsubscribe' link in emails or 'STOP' number in texts

We may ask you to confirm or update your marketing preferences if you ask us to provide further services in the future, or if there are changes in the law, regulation, or the structure of our business.

We will always treat your personal data with the utmost respect and never sell or share it with other organisations for marketing purposes.

Who we share your personal data with

We routinely share personal data with:

- professional advisors who we instruct on your behalf or refer you to, eg barristers, medical professionals, accountants, tax advisors, financial advisors or other experts;
- third parties where necessary to carry out your instructions, eg your mortgage provider, HM Land Registry in the case of property transactions, HM Courts & Tribunals Service or Companies House;

- third parties and external service suppliers, representatives and agents that we use to help deliver our services to you and make our business more efficient, eg payment service providers, office services;
- other third parties we use to help us run our business, eg marketing agencies or website hosts;
- third parties approved by you, eg social media sites you choose to link your account to or third party payment providers;
- our insurers and brokers;
- external auditors, eg in relation to Lexcel accreditation and the audit of our accounts;
- our banks;
- third party mailing database software providers (eg Mailchimp) where we are permitted to add you to or you have opted in to joining our marketing communications mailing list;

We only allow those organisations to handle your personal data if we are satisfied they take appropriate measures to protect your personal data.

We or the third parties mentioned above occasionally also share personal data with:

- our and their external auditors, eg in relation to the audit of our or their accounts, in which case the recipient of the information will be bound by confidentiality obligations;
- our and their professional advisors (such as lawyers and other advisors), in which case the recipient of the information will be bound by confidentiality obligations;
- law enforcement agencies, courts, tribunals and regulatory bodies to comply with our legal and regulatory obligations;
- other parties that have or may acquire control or ownership of our business (and our or their professional advisers) in connection with a significant corporate transaction or restructuring, including a merger, acquisition or asset sale or in the event of our insolvency—usually, information will be anonymised but this may not always be possible. The recipient of any of your personal data will be bound by confidentiality obligations

Who we share your personal data with—further information

If you would like more information about who we share our data with and why, please contact us (see '**How to contact us**' below).

MailChimp

MailChimp process your data in accordance with their Data Processing Addendum which can be found at https://mailchimp.com/en-gb/legal/data-processing-addendum/#6._International_Transfers. Mailchimp also have a GDPR compliance statement which can be found at https://mailchimp.com/en-gb/help/about-the-general-data-protection-regulation/

MailChimp automatically place single pixel gifs, also known as web beacons, in every email they send for us. These are tiny graphic files that contain unique identifiers that enable MailChimp to recognize when you have opened an email or clicked certain links. These technologies record your email address, IP address, date, and time associated with each open and click for a campaign. MailChimp use this data to create reports for us about how an email campaign performed and what actions you took.

Where we elect to use certain Mailchimp add-ons or features, the use of those may permit or require additional cookies or tracking technologies to be employed. Where we connect our website(s) to a Mailchimp account, Mailchimp installs a JavaScript tracking snippet ("Snippet") on our website. This Snippet will allow cookies, pixels, and other technologies to be set on our website to facilitate the use of certain automations, features and functionality offered by Mailchimp through the Service. The specific cookies, pixels, or other technologies that will be set on our website depend on the particular add-ons or features that we may choose to use as part of the Service. You should therefore review this privacy notice and our cookie disclosures for further information about the specific types of cookies and other tracking technologies used on our websites. These optional add-ons and features may include Popup forms. This is where the Snippet will allow our website to deploy a Mailchimp cookie that recognizes whether you have previously viewed a popup form and ensures you do not see the form again for a period of up to one year.

Where your personal data is held

Personal data may be held at our offices and those of our third party agencies, service providers, representatives and agents as described above (see '**Who we share your personal data with**').

Some of these third parties may be based outside the European Economic Area. For more information, including on how we safeguard your personal data when this occurs, see below: '**Transferring your personal data out of the UK and EEA**'.

How long your personal data will be kept

We will not keep your personal data for longer than we need it for the purpose for which it is used. We will however keep your personal data after we have finished providing legal services to you, in line with our published file retention/destruction policy, so that we may:

- respond to any questions, complaints or claims made by you or on your behalf;
- show that we treated you fairly;
- keep records required by law.

As a general rule, if we are no longer providing services to you, we will delete or anonymise your account data after six years. However, different retention periods apply for different services. Further details on this are available within our Terms of Business which are provided to you at the outset of your matter.

Following the end of the of the relevant retention period, we will delete or anonymise your personal data.

Where you have opted in to receiving or we are permitted to send you marketing communications, your personal data will be stored by MailChimp until such time as you unsubscribe.

Transferring your personal data out of the UK and EEA

Countries outside the EEA and the UK have differing data protection laws, some of which may provide lower levels of protection of privacy.

It is sometimes necessary for us to transfer your personal data to countries outside the UK and EEA, for example to our service providers located outside the UK/EEA or if you are based outside the UK/EEA. In those cases we will comply with applicable UK and EEA laws designed to ensure the privacy of your personal data.

Under data protection laws, we can only transfer your personal data to a country outside the UK/EEA where:

- in the case of transfers subject to UK data protection law, the UK government has decided the particular country ensures an adequate level of protection of personal data (known as an '**adequacy regulation**') further to Article 45 of the UK GDPR. A list of countries the UK currently has adequacy regulations in relation to is available here.

- in the case of transfers subject to EEA data protection laws, the European Commission has decided that the particular country ensures an adequate level of protection of personal data (known as an '**adequacy decision**') further to Article 45 of the EU GDPR. A list of countries the European Commission has currently made adequacy decisions in relation to is available here.

- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for you; or

- a specific exception applies under relevant data protection law.

Where we transfer your personal data outside the UK, we do so on the basis of an adequacy regulation or where this is not available, *legally-approved standard data protection clauses recognised or issued further to Article 46(2) of the UK GDPR*. In the event we cannot or choose not to continue to rely on either of those mechanisms at any time, we will not transfer your personal data outside the UK unless we can do so on the basis of an alternative mechanism or exception provided by UK data protection law and reflected in an update to this policy.

Where we transfer your personal data outside the EEA we do so on the basis of an adequacy decision or where this is not available, *legally-approved standard data protection clauses issued further to Article 46(2) of the EU GDPR*. In the event we cannot or choose not to continue to rely on either of those mechanisms at any time, we will not transfer your personal data outside the EEA unless we can do so on the basis of an alternative mechanism or exception provided by applicable data protection law and reflected in an update to this policy.

Please note that MailChimp use secure servers based in the United States of America and we rely upon standard contractual clauses in making any transfers outside of the UK.

Any changes to the destinations to which we send personal data or in the transfer mechanisms we rely on to transfer personal data internationally will be notified to you in accordance with the section on '**Changes to this privacy policy**' below.

Transferring your personal data out of the UK and EEA — further information

If you would like further information about data transferred outside the UK/EEA, please contact us (see '**How to contact us**' below).

Your rights

You have the following rights, which you can exercise free of charge:

Access	The right to be provided with a copy of your personal data and any supplementary information about the processing of your personal data
Rectification	The right to require us to correct any mistakes in your personal data
Erasure (also known as the right to be forgotten)	The right to require us to delete your personal data—in certain situations
Restriction of processing	The right to require us to restrict processing of your personal data—in certain situations, eg if you contest the accuracy of the data
Data portability	The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations
To object	The right to object: —at any time to your personal data being processed for direct marketing (including profiling); —in certain other situations to our continued processing of your personal data, eg processing carried out for the purpose of our legitimate interests unless there are compelling legitimate grounds for the processing to continue or the processing is required for the establishment, exercise or defence of legal claims.
Not to be subject to automated individual decision making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you
The right to withdraw consent	If you have provided us with a consent to use your personal data you have a right to withdraw that consent easily at any time You may withdraw consents by contacting us using the details in the '**How to Contact Us'** section of this policy. Withdrawing a consent will not affect the lawfulness of our use of your personal data in reliance on that consent before it was withdrawn

For more information on each of those rights, including the circumstances in which they apply, please contact us (see '**How to contact us**' below) or see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights under the General Data Protection Regulation.

If you would like to exercise any of those rights, please:

- email, call or write to us—see below: '**How to contact us**'; and

- provide enough information to identify yourself *(eg your full name, address and client or matter reference number)* and any additional identity information we may reasonably request from you (eg a copy of your driving licence or passport and a recent utility bill); and

- let us know what right you want to exercise and the information to which your request relates.

Keeping your personal data secure

We have appropriate security measures to prevent personal data from being accidentally lost, or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access it. Those processing your personal data will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

If you want detailed information from Get Safe Online on how to protect your personal data and other information and your computers and devices against fraud, identity theft, viruses and many other online problems, please visit www.getsafeonline.org. Get Safe Online is supported by HM Government and leading businesses.

How to complain

Please contact us if you have any queries or concerns about our use of your personal data (see below '**How to contact us**'). We hope we will be able to resolve any issues you may have.

You also have the right to lodge a complaint with:

- the Information Commissioner in the UK;

- a relevant data protection supervisory authority in the EEA state of your habitual residence, place of work or of an alleged infringement of data protection laws in the EEA.

The UK's Information Commissioner may be contacted using the details at https://ico.org.uk/make-a-complaint or by telephone: 0303 123 1113.

For a list of EEA data protection supervisory authorities and their contact details see here.

Changes to this privacy policy

This privacy policy was published on 1 August 2023 and last updated on the same date.

We may change this privacy policy from time to time, and when we do the updated version will be displayed on our website.

How to contact us

You can contact us by post, email or telephone if you have any questions about this privacy policy or the information we hold about you, to exercise a right under data protection law or to make a complaint.

Our contact details are shown below:

Our contact details	Duncan Morter, Director in charge of Data Protection
Address: Email: Telephone:	19 Clifford Street, York, YO1 9RJ d.morter@crombiewilkinson.co.uk 01904 624185

Do you need extra help?

If you would like this policy in another format (for example audio, large print, braille) please contact us (see 'How to contact us' above).

Updated August 2023