Bone & Payne Solicitors LLP

Privacy Notice

On 19 June 2025 the Data (Use and Access) Act (DUAA) became law in the UK.

The DUAA amends, but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) or the Privacy and Electronic Communications Regulations (PECR).

Phased implementation of DUAA

The DUAA changes are being phased in mainly between June 2025 and June 2026.

The first DUAA provisions came into force on 19 and 20 August 2025.

The latest set of DUAA provisions came into force on 05 February 2026.

This last set included most of the DUAA provisions with some exceptions such as the requirement for a Data Complaints Procedure which will become mandatory from the 19 June 2026.

Data Protection Complaints Procedure.

In anticipation of the above we have created a Data Protection Complaints Procedure.

You will find a Data Protection Complaints Form. on our website which will enable you to make a Data Protection Complaint (DPC)/or you may set out your Data Protection Complaint in an email to: jamie.herbert@boneandpayne.co.uk

You are not obliged to use the DPCF, but it would help us deal with your complaint more efficiently and we recommend that you use it.

This type of complaint will normally be dealt with by our Data Protection Supervisor, Jamie Herbert.

To help ensure that your DPC is dealt with promptly and to help protect confidentiality it is probably not prudent to send us a DPC via our Social Media platforms or other Portals and Platforms e.g. reviewsolicitors.

However you decide to submit your Data Protection Complaint it would be helpful if you provided us with:

1. Your ID (where appropriate)
2. Your Full name
3. Your preferred contact details (email / phone / postal address)
4. Your relationship to the firm:
    a. A current client
    b. A former client

c. An employee or former employee
d. Another affected individual

Please then describe your concern about how we have handled your personal data.

For further information on timescales etc please see Appendix 1 below.

The Information Commissioner

You also have the right to complain to the Information Commissioner's Office (ICO) at any time or if you are not satisfied with our response to your Complaint. You will find further information on the following link.

https://ico.org.uk/make-a-complaint/data-protection-complaints/

Service Complaints

Please note that a Data Protection Complaint is different from a service complaint i.e. where you are dissatisfied with any aspect of the service you have received from us. Our Service Complaints Procedure for this latter type of complaint is also found on our website. That type of complaint will normally be dealt with by our Complaints Handling Officer.

Data Subject Rights

The right to make a Data Protection complaint is separate from and additional to your rights numbered 1. to 8. set out below.

Before making a Data Protection Complaint you may wish to consider whether exercising one of more the rights below (e.g. 1. Making a data subject access request (DSAR) is more appropriate. If you are unsure as to which route to take, then please contact us and we will do what we can to assist you. The following examples of a DPC may help you choose.

Examples of circumstances where a Data Protection Complaint may be more appropriate:

- We didn't respond to your Data Subject Access Request.
- We have refused to provide the data you have requested.
- Your data was shared with someone else.
- You believe that we hold inaccurate information about you.
- You think that we have kept your data for too long.

If you are an individual, the rights you have under the UK GDPR include the following:

1. The **right to access** the personal data that we hold about you;
2. The **right to object** to us sending you information;
3. The **right to be informed** about the collection and use of your personal data;
4. The **right to rectification** of personal data we may hold about you if it is inaccurate or incomplete;

5. The **right to erasure** of your personal data in some circumstances;
6. The **right to restrict processing** your personal data where you may have a particular reason for wanting the restriction;
7. The **right to data portability** which will allow you to obtain and reuse your personal data across different services;
8. **Rights in relation to automated decision making and profiling** – please note we do not use automated decision making and profiling.

Data Subject Access Request (DSAR)

The DUAA has made some changes in this area and the ICO has published updated guidance which can be found on the ICO website https://ico.org.uk/for-the-public/

The right of access, commonly referred to as **subject access or data subject access request**, gives people the right to obtain a copy of their personal information, as well as other supplementary information.

The relevant individual has the right to obtain the following from us:

- Confirmation that we are processing their personal information.
- A copy of their personal information.
- Other supplementary information.

In most cases, we would confirm, in general terms, whether or not we are processing a person's personal information/data.

However, this will depend on the nature of the request. If the request is for a specific piece of information, we **must** confirm or deny whether we are processing this information unless an exemption applies. Whether or not an exemption applies will be decided on a case-by-case basis.

Manifestly unfounded or excessive Requests

We will take reasonable steps to respond positively and efficiently to your requests.

To protect your privacy, we will of course ask you to evidence your identity as appropriate in the circumstances.

However, we could refuse to respond to a request if it is manifestly unfounded or excessive. We will assess this on a case-by-case basis.

Alternatively, if we consider the request to be manifestly unfounded or excessive, rather than refuse the request we **could** charge a reasonable fee for dealing with the request. If we decide to charge a fee, we will notify the requester and explain why. We then do not need to take further action in response to the request until we receive the fee. The time limit for responding to the request begins to run again only once we have received the fee. We will explain how we have calculated the fee charged based on our administrative expenses.

We will explain to you why we consider your request to be manifestly unfounded or excessive.

Our Use of your Personal Data

We use your personal data to help us provide an excellent client service, which includes tailoring the information we share with you to help ensure that it's relevant, useful and timely.

We will respect your privacy and work hard to ensure we meet strict regulatory requirements.

We will not sell your personal data to third parties.

We will provide you with easy ways to manage and review your marketing choices if you receive direct marketing communications from us.

We are a firm that is authorised and regulated by the Solicitors Regulation Authority (SRA). As you might expect, we are already subject to strict rules of confidentiality. It is therefore already part of the fabric and culture of our firm to keep your information private and secure.

We would ask you to help us keep your data secure by carefully following any guidance and instructions we give e.g. communicating bank account details and transferring funds to us.

We are sometimes obliged to share your Personal Data with external authorities without notifying you e.g. as required by the Money Laundering & Terrorist Financing Act 2017 (as amended), our Sanctions Policy and Proliferation Financing Policy. The prevention of Crime and the Protection of Vulnerable Individuals are now both a Recognised Legitimate Interest [RLI] under the DUAA.

In all other cases, we will be transparent, and we will explain to you why we are requesting your data and how we are using it.

Lawful Bases for Processing your Data

The law states that we are allowed to use personal information only if we have a **proper and lawful reason** to do so. This includes sharing it with others outside the firm e.g. an auditor of a relevant quality standard.

The amended UK GDPR says we must have one or more of the, now seven, (Article 6) bases:

- **Contract:** the processing is necessary for a contract we have with an individual, or because they have asked us to take specific steps before entering a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. A legitimate

interest is when we have a business or commercial reason to use your information.

- **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
- **Recognised Legitimate Interest (7th basis added by DUAA):** see examples above.

Here is a list of all the ways that we may use your personal data, and which of the reasons we normally rely on to do so.

Use of your Personal Data	**Our reason/justification for processing**	**Legitimate Business Interest + RLI**
Opening, progressing, closing, archiving and storing a matter/case file	• Contract • Legitimate Interest • Legal Obligation	Fulfilling your instructions (the retainer) Complying with regulations and the law
Direct marketing to you	• Legitimate Interest	Keeping our records up to date, working out which of our products and services may interest you and telling you about them Providing information on changes in the law and inviting you to contact us for advice
To make and manage client payments. To manage fees, charges and interest due to clients To collect and recover money that is owed to us.	• Contract • Legitimate Interest • Legal Obligation	Keeping accounts systems up to date Complying with SRA Accounts Rules and other regulations Effective and efficient management of a sustainable business
To detect, investigate, report, and seek to prevent financial crime. To share personal information where necessary for purposes of safeguarding national security, protecting public security or defence To help Safeguard vulnerable individuals	• Contract • Legitimate Interest • Legal Obligation • Recognised Legitimate Interest [RLI] (DUAA)	Developing and improving how we deal with financial crime including suspected money laundering as well as complying with our legal obligations in this respect Complying with regulations that apply to us. Being efficient about how we fulfil our legal and contractual duties.

To make disclosures to public bodies, or bodies carrying out public tasks where the requesting body has confirmed it needs the information to carry out its public task. • To manage risk for us and our customers. • To comply with laws and regulations that apply to us. • To respond to complaints and seek to resolve them.		RLI
To run our business in an efficient and proper way. This includes managing our financial stability, business capability, planning, communications, corporate governance, and audit.	• Legitimate Interest • Legal Obligation	Complying with the SRA Accounts Rules and Code of Conduct and other regulations that apply to us Being effective and efficient about how we run our business To allow external consultants, advisers and auditors to inspect files
To exercise our rights and comply with obligations set out in agreements or contracts	• Legitimate Interest • Legal Obligation • RLI	Complying with contractual requirements e.g. for the provision to clients of Public Funding by Public Bodies RLI

Criminal Convictions Data

Further to our lawful bases for processing personal data we rely on further conditions contained within the Data Protection Act 2018 (as amended) for processing these types of data. These conditions are contained in Schedule 1, Part 3 of the Act. The primary condition we rely on is known as "legal claims" where;

This condition is met if the processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights

We would normally also rely on another condition in Schedule 1, Part 3 of the Act known as "consent" where, due to the nature of these types of data we would obtain your consent prior to processing them.

If our reason for processing data is in connection with the Schedule 1, Part 2 of the Act, condition 18, safeguarding of individuals and children at risk. This is because the processing will be necessary for the purposes of;

(a) protecting an individual from neglect or physical, mental or emotional harm, or

(b) protecting the physical, mental or emotional well-being of an individual,

In this condition;

(a) in the circumstances, consent to the processing cannot be given by the data subject.

(b) in the circumstances, we cannot reasonably be expected to obtain the consent of the data subject to the processing.

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection

Also, due to the nature of these data types, we comply with Schedule 1, Part 4 of the Data Protection Act which requires us to have an appropriate written policy explaining our security procedures, and data retention periods and we are required to retain this policy document and produce it to the Information Commissioner on request. Our policy is set out in the firm's Information Management & Security Policy.

Types of Personal Data we process

Type of Personal Information	**Description**
Financial	Your Bank account details and your financial status and information
Contact Information	Where you live and how to contact you
Socio-Demographic	This includes details about your work or profession, nationality etc.
Transactional	Details about payments to and from your bank accounts
Contractual	Details about the products or services we provide to you
Behavioural	Details about how you use our services
Communications	What we learn about you from letters, emails, and conversations between us
Social Relationships	Your family, friends and other relationships
Open Data and Public Records	Details about you that are in public records such as the Land Registry, and information about you that is openly available on the internet

Documentary Data	Details about you that are stored in documents in different formats, or copies of them. This could include things like your passport, drivers' licence, or birth certificate
Special Category Data	The Law and other regulations treat some types of personal information as a special category. We will only collect and use these types of data if the law allows or requires us to do so. The UK GDPR defines special category data as: personal data revealing: • Racial or ethnic origin • Political Opinions • Religious or philosophical beliefs • Trade union membership • Genetic Data • Biometric data (where used for ID purposes) • Data concerning Health • Data concerning a person's sex life; • Data concerning a person's sexual orientation. Please note that biometric data may be used and processed by our suppliers to verify your ID. Details of such suppliers will be provided if requested together with details of where you can view their Privacy Policy.
Consents	Any permissions, consents or preferences that you give us. This includes things like how you want us to contact you.
National Identifier	A number or code given to you by a government to identify who you are, such as a National Insurance Number
Legal Aid Application and Bill and any information provided to enable the LAA to enforce its statutory charge etc.	Information required to submit an application for public funding and to claim our fees under any legal aid certificate issued to you. This may be "shared data" under our contract with the Legal Aid Agency. [See LAA Privacy Notice]

Note: Where acting for you involves us holding or processing **Special Category Data**, we will seek your explicit consent e.g. when we plan to obtain your medical records.

You have the right to withdraw your consent by contacting us as stated above.

However, if you do so then we may not be able to progress you case or indeed continue to act for you.

Sources of Data

We collect personal data from various sources:

Data	Source	Purpose
Data you give us when you instruct us to advise you or act for you	You	To enable us to decide whether to accept your instructions and to progress your matter
Data you give us by letter/phone/email and other documents	You	To enable us to decide whether to accept your instructions and to progress your matter
Data you give us when you visit our website, via a messaging service or social media	You	To enable us to deal with your query or request and to contact you if appropriate
Data you give us during interviews	You	To enable us to advise and represent you and to communicate with other solicitors and third parties on your behalf
Data you give us in client surveys	You	To enable us to improve our services and respond to any expressions of dissatisfaction
Data provided to us by referrers and introducers	Referrers	To enable us to contact you and to enable us to decide whether to accept your instructions and to progress your matter
Fraud Prevention Applications e.g. InfoTrack: Ecos; Thirdfort etc.	Agency	To enable us to comply with the law and regulations and carry out client due diligence checks
Estate Agents	Agents	To enable us to act on your behalf in relation to a land transaction
Other Solicitors	Solicitor Firms	As part of an exchange of information to enable us to progress the matter and advise you
Public Bodies	Public Body such as HMRC, HM Treasury, Local Authority, Land Registry, Land Charges Registry,	To enable us to advise you and progress your matter.

	Probate Registry, Legal Aid Agency, Police, CPS, Courts Service and other government departments	To prevent fraud and money laundering
Your GP or other medical professional	Doctor	To obtain appropriate medical reports
The Legal Aid Agency [LAA]	LAA	Under our contractual obligations we will receive "Shared Data" from the LAA if your matter is legally aided

Who we share your Data with

Subject to the SRA Code of Conduct and the requirements regarding client confidentiality, we may share your personal information with:

- Lawyers or other organisations on the other side of a matter or case
- Barristers or experts we instruct
- The courts and other tribunals
- Your Personal Representatives or Attorneys
- Auditors
- Compliance & Management Consultants
- Lenders
- Estate Agents, IFAs, Referrers, etc
- Organisations that we introduce you to.
- HM Revenue and Customs
- The government both Central, Local and Devolved
- Fraud Prevention Agencies including the National Crime Agency
- Government Departments like OFSI
- The SRA and other regulators
- ID checking organisations and
- SOW and SOF checking organisations.
- Independent complaint handling organisations

Automated Decision-Making

We do not currently use automated decision-making systems. All decisions relating to you and your matter are made by a human.

We may from time to time use artificial intelligence (AI) to support the progress of your matter. However, the decision on how to proceed will be made by a suitably qualified/authorised person within our firm.

Personal Data we use

We typically will use the following types of personal data:

- Your Name
- Date of Birth
- Home address
- Contact details such as phone numbers and email addresses
- Bank details and account information
- Medical information (where applicable)
- Employment details
- Data that identifies you by cookies when you use our website

Sending Data outside the European Economic Area (EEA)

Unless you instruct us in a matter or case that involves an international element, we do not normally send your personal data outside the UK or EEA.

International Data Transfers

We confirm that we do not normally hold or process your data outside the UK but if we do, we will ensure there are sufficient "adequacy" arrangements or "safeguards" in place to protect your rights.

We will rely on the "UK-Extension" where appropriate. The UK Extension to the EU-US Data Privacy Framework refers to the UK's adequacy regulations for the US.

- The UK Extension is a partial adequacy finding. It allows UK organisations, to make restricted transfers to certain self-certified businesses in the US.
- Certain US businesses can choose to participate in the UK Extension by self-certifying to the US Department of Commerce that they will comply with the Data Privacy Framework (DPF) requirements.

If we rely on the UK Extension, we will only make a restricted transfer to a US business that has an active status on the DPF list. We will also be mindful of the type of data we are transferring e.g.HR or Special Category Data and take additional steps as necessary.

Your refusal to provide Personal Data requested

If you refuse to provide the information requested, then it may cause delay, and we may be unable to continue to act for you or complete your matter.

Marketing Information

We may from time to time send you letters or emails about changes in the law and suggestions about actions that you might consider taking in the light of that information e.g. reviewing your will. We will send you this marketing information either because you have consented to receive it or because we have a "legitimate interest".

You have the right to object and to ask us to stop sending you marketing information by contacting us at any time. You can of course change your mind and ask us to send the information again.

How long we keep your personal information

We are legally obliged to keep certain information for at least 5 years and typically store your file for 6 years before destroying it. In the case of LAA funded matters and cases involving a minor the files may be kept for a longer period of time.

This period will be set out in our closing letter to you.

We will store most Wills and other important deeds and documents indefinitely unless we are required to release them.

We will keep your name and personal contact details on our database until you tell us that you would like them removed e.g. where you have changed solicitor.

How to get a copy of your Personal Information

If you wish to access your personal data, then write to:

Name: Jamie Herbert

Data Protection Supervisor

55 Madoc Street Llandudno Conwy LL30 2TW

Telling us if your Personal Information is incorrect (The right to rectification)

If you think any information we have about you is incomplete or wrong, then you have the right to ask us to correct it. Please contact us as above.

Other Rights

As mentioned above you also have other rights, namely

- The right to erasure
- The right to restrict processing
- The right to data portability

You have the right to ask us to delete (erase) or stop us using your data if there is no longer any need for us to keep it (e.g. under a legal obligation).

In terms of data portability then subject to any lien we may enjoy for non-payment of fees, we will comply promptly (where permitted) to your request to transfer your physical paper file to another solicitor upon receipt of your signed consent. If your file is in electronic format, we will take reasonable steps to export the file to a "portable format" where possible so that your new solicitor can upload it to their system. As many different IT systems are used by the legal profession, we cannot guarantee that we can provide data in a compatible format.

Updating this Notice

This Privacy Notice will be updated from time to time as required, and as relevant changes under the DUAA come into force.

APPENDIX 1

Complaints under Section 103 of the Data Use and Access Act 2025

(Section 164A Data Protection Act 2018)

1. Statutory Complaints Rights

1.1 Data subjects have a right to make complaints directly to the data controller concerning personal data handling.

1.2 Complaint channels must be electronically accessible (e.g. via email or web form) so we will provide a link via our website.

2. Acknowledgement and Timelines

2.1 Complaints must be acknowledged **within 30 calendar days** of receipt of the complaint so such complaints should be referred to the DPS immediately.

2.2 The DPS must undertake investigation **without undue delay**, including follow-up queries as necessary.

2.3 The outcome must be communicated in writing to the complainant once the investigation is concluded.

3. Escalation Procedure

3.1 Complaints may be escalated to the Information Commissioner's Office (ICO) only **after the controller's response** has been provided.

3.2 The DPS must inform the complainant in writing of their escalation rights and refer them the ICO's website for further information https://ico.org.uk/make-a-complaint/

4. Reporting Obligations

4.1 If directed by the Secretary of State, the DPS may be required to report anonymised complaint data to the ICO, so it is vitally important that we keep careful central records and analysis of all complaints in an appropriate format.

5. Organisational Compliance Measures

- We will review and revise existing **data complaint handling policies**.
- Provide staff training on the **DUA-compliant complaints response process**.
- Implement a tracking system for dates, actions, and outcomes.
- Ensure alignment with quality protocols such as **LEXCEL, CQS** and the LAA's current Data Security Requirements as applicable.