☎ +44 (0) 1625 252233 ✉ contact@cancerlegalexperts

Cancer Legal Experts GDPR POLICY

What is this policy for?
Cancer Legal Experts (CLE) are committed to data protection, and this policy sets out your individual rights and obligations in relation to personal data. We are also committed to being transparent about how we collect and use the personal data of our clients, experts, contractors and any other individual we collect personal data from.

Who is this policy for?
This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, apprentices and former employees. This policy also applies to the personal data of clients, experts and any other individual we collect personal data from for business purposes.

General Data Protection Regulation (GDPR)
The company (CLE) has appointed Danielle Timoney, Operations Manager as the person responsible for data protection compliance. She can be contacted at:-
danielletimoney@cancerlegalexperts.co.uk / +44 1625 252233

All and any questions about this policy, or request for information, should be directed to Danielle.

Definitions
Personal Data – is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.
Special Categories of personal data – means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
Criminal records data – means information about an individual's criminal convictions and offences relating to criminal allegations and proceedings.

Data protection principles
We process personal data in accordance with the following protection principles:

- We process personal data lawfully, fairly and in a transparent manner.
- We collect personal data only for specific, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data only for the period necessary for processing.
- We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

We will tell you about the reasons for processing your personal data, how we use such data and the legal basis for processing the data in our privacy notices, which are available and supplied where required. We will not process your personal data for other reasons. Where we rely on our

legitimate interests as the basis for processing data, we carry out an assessment to ensure that those interests are not overridden by your rights and freedoms.

Where we process special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with guidance on special categories of data and criminal records data.

We will update personal data promptly if you advise us that your information has changed or is inaccurate. Personal data gathered during your employment as employees, customers, suppliers or any other individual will be held on your personnel file (in hard copy or electronic format, or both). The periods for which we will hold personal data are contained in our privacy notices.

We will keep a record of our processing activities in respect of personal data in accordance with the requirements of General Data Protection Regulation (GDPR).

Data security
We take the security of personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees and contractors in the proper performance of duties.

Where we engage with a third party to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

International data transfers
We may, due to business purposes, transfer personal data outside of the UK and the transfer and use of this date will comply with this GDPR policy

Training (where applicable for employees of CLE)
We will provide training to you about your data protection responsibilities as part of any induction process.

If your role requires regular access to personal data, or if you are responsible for implementing this policy or responding to subject access requests under this policy, you will receive additional training to help you understand your duties and how to comply with them**.**

Your responsibilities
You are responsible for helping us to keep your personal data up to date. You should let us know as soon as possible if any data that you have provided to us changes, for example if you move to a new house or change your bank details.

You may have access to the personal data of your colleagues in the course of your employment or contract. Where this is the case, we rely on your assistance to help us meet our data protection obligations to employees, experts and clients.

Medico-legal experts and their administrative staff are responsible for understanding and adhering to CLE data protection policies.

If you have access to personal data, you are required:

- To access only data that you have authority to access and only for authorised purposes.
- Not to disclose data except to individuals (whether internal or external) who have appropriate authorisation.
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).
- Not to remove personal data, or devices containing or that can be used to access personal data, from our premises, without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- Not to store personal data on local drives or on personal devices that are used for work purposes.
- To report data breaches of which you become aware or suspect to danielletimoney@cancerlegalexperts.co.uk immediately.

Failure to observe these requirements may amount to a disciplinary offence. Significant or deliberate breaches of this policy, such as accessing your colleagues, expert or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to the termination of professional relationship.

Your rights

As a data subject, you have a number of rights in relation to your own personal data. You have the right to make a subject access request, and if you do make such a request, we will tell you:

- Whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if its not collected from you directly.
- To whom your data is or may be disclosed.
- For how long your personal data is stored (or how that period is decided).
- Your rights to rectification or erasure or data, or to restrict or object to processing.
- Your right to complain to the Information Commissioner if you think that we have failed to comply with your data protection rights.
- Whether or not we carry out automated decision-making and the logic involved in any such decision-making.

To make a subject access request, you should send your request to danielletimoney@cancerlegalexperts.co.uk . In some cases, we may need to ask for proof of identification before your request can be processed. We will inform you if we need to verify your identity and the documents we will require.

We will normally respond to your request within a period of one month from the date it is received. In some cases, such as where we process large amounts of your data, we may respond within three months of the date your request is received. We will write to you within one month of receiving your original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but we may charge a fee, which will be based on the administrative cost of responding to your request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.

We will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically unless you agree otherwise.

If you want additional copies, we may charge a fee, which will be based on the administrative cost of providing the additional copies.

You can require us to:

- Rectify inaccurate data.
- Stop processing or erase data that is no longer necessary for the purposes of processing.
- Stop processing or erase data if your interests override our legitimate grounds for processing data (where we rely on our legitimate interests as a reason for processing data).
- Stop processing or erase data if processing is unlawful.
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override our legitimate grounds for processing data.

To ask us to take any of these steps, you should send a request to danielletimoney@cancerlegalexperts.co.uk .

Data breaches

A data breach is defined as any incident that has affected the confidentiality, integrity, or availability of personal data. Any breach that is likely to have an adverse effect on individual's rights or freedoms must be reported. If you become aware of a data breach, you must contact danielletimoney@cancerlegalexperts.co.uk immediately, who will provide advice on further action, and whether the ICO needs to be informed.

Where a report to the ICO must be made, it should be done without undue delay or within 72 hours of the breach being identified. The report must contain the following information:

- Our details.
- Details of the breach.
- What personal data has been placed at risk.
- What actions have been taken to contain the breach and recover the data.
- What training and guidance has been provided.
- Any previous contact with the ICO.
- Amy miscellaneous support information.

We will notify you of any breach that affects your personal data without undue delay. You will be notified to afford you the opportunity to take the necessary steps in order to protect yourself from the effects of the breach. In any such event, we will provide you with the following information:

- The circumstances surrounding the breach.
- The details of who will be managing the breach.
- Any actions we have taken to contain and manage the breach.
- Any other pertinent information that can support you.

How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details on page one of this policy.

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113
Website: https://www.ico.org.uk/make-a-complaint

Last Updated: 19th November 2025