Professional Paralegal Register

A Guide to GDPR

For Paralegals

Professional Paralegal Register

The European General Data Protection Regulation (EU GDPR) come into force on 25th May and requires all organisations who handle, process or control personal data to comply by this date.

The regulation applies to any information that is capable of identifying an individual which includes client contact lists, contact details including social media accounts, online identifiers such as IP addresses and genetic/biometric data.

The new regulation requires organisations to effectively strengthen their controls, implement new policies, procedures and processes and to ensure that these are documented and evidenced to show compliance.

Paralegals need to evaluate their existing position, prepare for these changes, and ensure that their data protection systems are robust.

Ignoring GDPR on the grounds that you have a small business or are a sole practitioner is unwise as the GDPR covers all forms of data so you need to be able to track and manage your clients details will be your first priority.

Owning and understanding client data is crucial to remaining competitive as data enables Paralegals to improve understanding about clients and deliver better services.

If you are a data controller you must register with the ICO.

What Paralegals and Paralegal Law Firms can do to prepare for GDPR

Understand your data

What information do you currently hold?

You could start by undertaking an information audit to include all data including client notes, hard copy documents, recordings and digital data.

Where is your data held?

You need to know exactly where it is held and by whom, who has access to it and who you share any data with eg an IT team or accountant.

You must be able to find a client's data and be able to delete it upon request and have systems in place that can prove that you have deleted it. Do you hold information that you might be able to refuse a right to be forgotten request "for the establishment, exercise or defence of legal claims"?

You could start a data discovery audit to see which type of data moves the most eg lots of people having access and looking at details on databases .

If you have staff, then all staff should receive training on the GDPR. Run a data-security test to ensure that you know what to do in the event of a breach.

Where possible you should show good practices in protecting data such as encrypting laptops and mobile devices that contain data.

Contracts with third party suppliers should be reviewed and you should ask about what steps they are taking to protect your data.

Data processors must ensure that all contracts with suppliers comply with GDPR.

If you store any client records or eg Wills offsite then you need to check that your supplier has tracking processes in place to ensure security of data at all times.

Consent must be obtained for every communication method. Under GDPR you must make it clear the lawful basis for processing the data and how long you will keep it for. You must make sure that your clients are aware that they can complain to the ICO if they feel there is a problem with the way you are handling their data.

Paralegal practitioners and Paralegal firms that do not carry out large scale systematic monitoring of clients data will not be required to appoint a DPO.

The GDPR gives more rights to consumers/clients.

You must ensure that you are aware of these rights and include them in your data collection processes and procedures. You must make it clear to your clients that they have these rights and explain how they can exercise these rights .

Building trust with your clients by being compliant will make your clients want to interact with you and ultimately make them more likely to choose you over a competitor who is not making this information clear enough.

Checklist

Here are steps to help you or your organisation .

- Ensure you are registered with the ICO if you are a data controller
- List all the data you currently hold, how it is stored, what it is used for and by whom
- Establish what personal information you hold, what the retention period should be and adopt a procedure to erase data
- Review third party contracts– do they contain the mandatory obligations prescribed by the GDPR?
- Ensure you or your employees can recognise/respond to data subjects who want to exercise their rights eg the right to be forgotten
- Review/amend privacy notices
- Review and increase security of data where necessary
- Review how you would identify a breach, document it and notify the ICO within 72 hours.

This information is provided as a guide only and not intended to address the circumstances of any individual or entity.

75% of data held by companies is estimated to be unusable post GDPR

You should use these guidelines in conjunction with reading the GDPR as these only provide a snapshot of the requirements.

The information contained in these guidelines are for general use and are not intended to address any individual circumstance. You should not act on this information without appropriate professional advice.

Contacts

https://ico.org.uk

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

PPR Conference

Find out more useful information at the Paralegal Conference

ppr.org.uk/conference