The Law Society

Countdown to GDPR

The 25 May 2018 deadline is fast approaching for compliance with the new EU General Data Protection Regulation (GDPR). By now, you should have audited and assessed the personal data on EU citizens that your firm holds and have procedures and policies in place to meet the requirements.

Read on for our five top tips to ensure you're on track.

Pearl Moses
Head of Risk and Compliance, The Law Society

1 Make a plan and make it known

Carry out a gap analysis to identify where existing compliance is good, and where there are likely to be difficulties in complying with the GDPR. You can then formulate a compliance plan that can be broken down into manageable sections for implementation – you may wish to refer to the ICO's '12 steps to take now' to help with this, available on their website.

While it's not compulsory for most firms to appoint a data protection officer, consider making a designated person responsible. You also need to make everyone in the firm aware of the implications of GDPR.

2 Audit and map your data

Knowing what information your firm holds, where it came from and who you share it with is essential to be able to demonstrate your compliance with the GDPR and to maintain appropriate records of your processing activities. You should therefore carry out a data mapping exercise and, if necessary, a full information audit.

3 Check you have consent

Ensure you are clear about the grounds for lawful processing relied upon by your firm. Consent is just one of the legal grounds for processing personal data and many law firms will have other grounds for processing, for example a contract or legitimate interest. Note though, that previously received consent from a client or any other individual can only be relied upon if the standard of that consent meets the new requirements under the GDPR.

4 Ensure you're ready to process data subject access requests

Reviewing your processing and handling of data is vital in becoming compliant with the GDPR. Ensure all data can be easily viewed, deleted or transferred if requested. Rights to access personal data under the GDPR include the right to be forgotten or to have information deleted, the absence of a fee for access to data and a new, lower, time limit of one month for responding to requests.

5 Have procedures in place for handling a data breach

The safety and security of the data your firm holds are paramount to meeting the requirements of the GDPR. Should your firm suffer a data breach of any kind, it's vital that you have policies and procedures in place to identify your vulnerabilities, limit the damage, document it and report it to the relevant agencies. Failure to deal with data security could lead to hefty fines – up to four per cent of your annual turnover.

For support and information on GDPR, see the Law Society's dedicated web resources here:
www.lawsociety.org.uk/GDPR

For additional support on compliance-related issues facing law firms and information on Risk and Compliance Service membership, visit:
www.lawsociety.org.uk/riskandcompliance