HOW TO

COMPLY WITH THE GENERAL DATA PROTECTION REGULATION ("GDPR")

The General Data Protection Regulation ('GDPR') came into force on 25 May 2018 and made important changes to data protection law. We can help you with them.

Personal data is an invaluable asset and many organisations rely on their ability to collect and process it in order to operate their business. The GDPR will apply to the processing of personal data by both data controllers and data processors. The new measures include increased accountability and a requirement on organisations to take a more proactive and transparent approach to data protection compliance.

Once the UK leaves the EU, and subject to any agreement, scrutiny of the UK's Data Protection Act 2018 may be needed to assess it in terms of the adequacy of data protection legislation in the UK.

1. Bigger fines:	Fines of up to €20million or 4% of global turnover (whichever is the greater), depending on the breach (half that for processors).
2. Mandatory breach notifications:	Three levels of breach reporting apply - data controller to regulator (within 72 hours); data processor to data controller (without undue delay); and data controller to data subjects (without undue delay).
3. Transparency/ accountability:	More information must be given to individuals – data must be processed "Lawfully, fairly and in a transparent manner ..." and organisations must be able to evidence that they comply, with clear record-keeping.
4. Information notices and additional individual rights:	Fairness and transparency of processing requires more extensive information to be given to individuals, including a qualified right to be forgotten and a right to data portability. and organisations must be able to evidence that they comply, with clear record-keeping.
5. Pro-active privacy:	Data Protection Impact Assessments need to be undertaken by organisations where processing operations are "likely to result in a high risk" and data should be protected by design of systems, and a default setting of privacy.
6. Data governance:	The organisation needs to implement measures to reduce risk of breach and to take governance seriously. Certain organisations are required to formally appoint a 'Data Protection Officer' to monitor and advise them on GDPR compliance and communicate with regulators.
7. Policies:	Data controllers must implement data protection policies, which will need to be transparent and easily accessible.
8. Legitimate interests:	Data controllers who rely on legitimate interests should maintain a record of the assessment made to demonstrate compliance.
9. Consent:	Data controllers who rely on consent are subject to stricter requirements. Consent must generally be 'unambiguous', granular and capable of being withdrawn as easily as it is given. It is unlikely to apply in an employment context any longer - other legal bases are needed.
10. Wider territorial scope:	GDPR applies to organisations based outside of the EU who target and/or monitor EU customers, even if that entity has no EU presence.
11. Pseudonymisation and data minimisation:	The processing of personal data in such a way that the data can no longer be attributed to the data subject is encouraged as a measure to protect data. You should only collect, use and keep the data you need for a particular purpose.
12. Data processors:	Direct obligations for data processors; companies that conduct outsourced services will be caught by GDPR.
13. Incentives for compliance:	Seals and certifications will be available to inform data subjects of the level of an organisation's compliance.

WHAT DO YOU NEED TO DO?

There are a number of actions you can take, to ensure compliance with the GDPR and DPA 18:

- **GOVERNANCE** – Establish who has ownership of data protection and privacy compliance within your organisation and establish reporting lines directly to the board.
- **GAP ANALYSIS** – Review your data protection compliance.
- **REMEDIATION** – Update and document processes, policies and procedures to ensure that you can demonstrate compliance if required.
  - » Review the personal data (including consents) held to ensure that it is adequate, relevant and limited to the minimum extent necessary in relation to the purpose for which it is processed.
  - » Review contracts with suppliers (and template new contracts) to ensure that they include robust data processing obligations.
  - » Carry out risk assessments before embarking on a project which involves the processing of personal data.
  - » Change employment contracts and handbooks to move away from the use of consent.
  - » Review and update IT systems.
  - » Check your organisation's insurance policy cover for data protection related risks.
- **RECORD KEEPING** – Keep records internally to demonstrate compliance.
- **TRAINING** – Train staff and suppliers, and/or recruit compliance officers.

HOW SHOOSMITHS CAN HELP YOU

- **Shoosmiths' GDPR Drive** – We can help you assess the extent to which your organisation processes personal data in accordance with the Data Protection Act 2018 and the GDPR by carrying out a detailed audit/review, and supporting your ongoing compliance obligations. We can provide a report and work with you in order to agree a tailored service that identifies key risk areas for your organisation and which arms you with the information you need to address any key non-compliance or outstanding actions. It will also mean you can optimise your data collection and use to make the most of the data for greater purposes and drive business benefits.
- **Reviewing/drafting and updating** governance policies, employment contracts, employee handbooks, privacy notices, consent/other statements used to collect personal information, data protection template contracts and clauses, Data Protection Impact Assessment templates, and templates for the other decisions and tools which you will need to demonstrate compliance and policies relating to: cookies, privacy policies, data protection, document retention, data security, data breach, subject access requests, bring your own device, social media and CCTV.
- providing **a managed contract update/negotiation service**.
- **Rapid Response On Call Team** and **in-house support for Breaches** – use our tried and tested process when in crisis.
- **Data Subject Requests Support** – innovative tools, personnel, and precedents dedicated to streamlining this complex and time-intensive task.
- **DP Experts for hire** – mini clinics within your business to address live issues and deliver targeted support.
- **Training** including **Bespoke E-learning tools**, **Collaborative training** and **networking sessions with your peers** to share best practice and **One-on-one** training and/or **legal training sessions**. Try our "**breach out" room exercise** to work through responding to a data breach scenario within your organisation and test your processes.
- **Data Protection certification** – assessment of your processing operations, products or services against compliance. A useful benchmark for the business.
- **Codes of Conduct** – codes can be used as authority for data transfers under the GDPR. Get in touch if you want to be included in our Industry or Sector specific forums creating codes and sharing knowledge and experiences.

For any further information please visit **www.shoosmiths.co.uk/data** – We can help you with that.