A roadmap to GDPR compliance

How to meet the requirements of the General Data Protection Regulation

SA LAW

GDPR COMPLIANCE

GDPR is the biggest shake-up in data protection law for 20 years.

When it came into force on 25 May 2018, it ushered in a new era of personal data transparency and accountability, with more obligations for organisations, and a new maximum penalty for non-compliance of €20 million or 4% of your global annual turnover. There has never been a more pressing need to ensure you are handling the personal data of your customers, colleagues and other individuals compliantly.

WHAT ARE YOUR GDPR OBLIGATIONS?	WHAT SHOULD YOU BE ASKING YOURSELF?	ROADMAP TO GDPR COMPLIANCE
Accountability & Communication		
• Demonstrate that your organisation takes data protection seriously • Deliver ongoing data protection training and internal communications for employees	• Who is responsible for data protection? • Who from across the organisation should be part of the data protection/GDPR compliance team? • Do we need a Data Protection Officer? • How will we communicate changes to our stakeholders?	✓ Get GDPR on the boardroom agenda now ✓ Build an effective compliance team, and assign budget ✓ Keep customers, employees and other stakeholders informed to enhance confidence in your brand ✓ Define the roles and responsibilities of employees who manage personal data in your organisation
Data, Record Keeping & Governance		
• Process data fairly, lawfully and transparently • Demonstrate that personal data systems and processes are compliant 'by design' • Maintain clear, accurate and accessible records • Ensure suppliers and business partners can protect your personal data, and process it compliantly	• What personal data do we hold, how is it collected, who uses it, and how and where is it stored? • Is any of our personal data held overseas? • Are our suppliers and business partners going to be compliant with GDPR? • Who will conduct data privacy impact assessments, and who will sign them off?	✓ Conduct a personal data audit, and map the flow of different data types around your organisation ✓ Keep records of how personal data is processed ✓ Request the data protection policies of relevant suppliers and business partners ✓ Build compliance into all processes and look for other ways to protect data (e.g. pseudonymising)

WHAT ARE YOUR GDPR OBLIGATIONS?	WHAT SHOULD YOU BE ASKING YOURSELF?	ROADMAP TO GDPR COMPLIANCE
Policies & Procedures		
• Ensure you have an up-to-date and clearly understandable data protection policy • Provide a privacy notice that explains how you process personal data, and the rights of individuals	• Where are the gaps in our current data protection/privacy policies and procedures?	✓ Develop a timeline to update policies. What are the quick fixes? What will take more time? ✓ Road test your data protection and privacy policies. Are they easy to understand and put into practice?
Consent		
• Obtain consent freely and unambiguously from all individuals whose personal data you hold • Consent notices for children must be drafted with parental consent in mind	• How do we obtain consent currently, and are our consent records up-to-date and accurate? • Do we hold the data of any children (i.e. under the age of 18?)	✓ Reconfirm consent, explaining why you are doing it, and emphasising that it enables you to provide your service ✓ Develop robust practices around the processing of children's data
Rights of the Individual		
• Individuals have the right to make a Subject Access Request (SAR) to find out what personal data you hold about them and how it is processed • SARs must be fulfilled within one month and cannot be charged for • Individuals have the 'right to be forgotten' by asking you to erase all data you hold about them	• How would we deal with a SAR or request to be forgotten? • Would employees recognise a SAR if they received one, and would they know what to do with it? • What personal data do we retain and how long do we retain it for? Are we holding data too long?	✓ Develop processes for SARs and erasure request ✓ Make sure employees know what an SAR is and what to do if they receive one ✓ Implement a data retention policy in line with commercial needs
Data Breaches		
• Report data breaches to the relevant authorities within 72 hours of their discovery • Notify individuals whose personal data may have been compromised if required • Maintain a register of breaches	• How do we protect personal data? Consider IT policies, processes and employee behaviour • Which practices carry the greatest risk of a data breach (e.g. travelling, working from home, etc.)? • Do employees know how to recognise data breaches and where to report them? • How would we manage negative publicity associated with a data breach?	✓ Ensure effective IT security measures are in place and that employees know when and how to use them ✓ Educate employees about data breaches and how to report them internally ✓ Allocate roles and responsibilities for dealing with a breach if it occurs ✓ Create post-mortem procedure to identify risks and areas for improvement

HOW CAN WE HELP YOU?

We can help you to tackle the new data protection legislation head-on. SA Law's GDPR Response is designed to protect your organisation as we enter the new era of data protection transparency and accountability.

We can support you with a range of bespoke services, including:

GDPR Response Toolkit

Our fixed-price service gives you a clear roadmap to compliance with all the relevant document templates you need and an advice helpline to guide you through implementation. Price: £995 plus VAT.

Data Strategy, Risk Assessment & Audit Support

Helping you to understand your current data protection culture and devising and implementing strategies that solve compliance gaps.

Communications & Training

Delivering employee communications, including on-site training about data protection obligations, and board and senior management briefings.

Crisis Management

Minimising the financial and reputational damage of a data breach, including a PR plan to tackle negative publicity, and post mortem activities to prevent similar incidents.

Ongoing Assistance

Resolving data protection queries, concerns, requests and complaints as they arise, whether you need a quick telephone consultation or ongoing support with an initiative.

MEET THE TEAM

Chris Cook Partner

Head of Employment & Data Protection
chris.cook@salaw.com

Julie Gingell Partner

Director of Marketing & Business Development
julie.gingell@salaw.com

CONTACT US

To find out how we can help you, contact Chris Cook on **01727 798000** or at **gdpr@salaw.com.**

Visit our dedicated webpage for more exclusive resources to help you comply with GDPR, and for further information about SA Law's fixed price compliance toolkit.

FIND OUT MORE →

https://salaw.com/gdpr-getcompliant/

SA Law helps people like you with all aspects of their business, professional and personal lives. With an exceptional track record of winning success for clients, our solutions are targeted, practical and engineered to deliver the best possible outcome.

salaw.com

St Albans: +44 (0)1727 798000
London: +44 (0)20 7183 5683
gdpr@salaw.com

@SA_Law