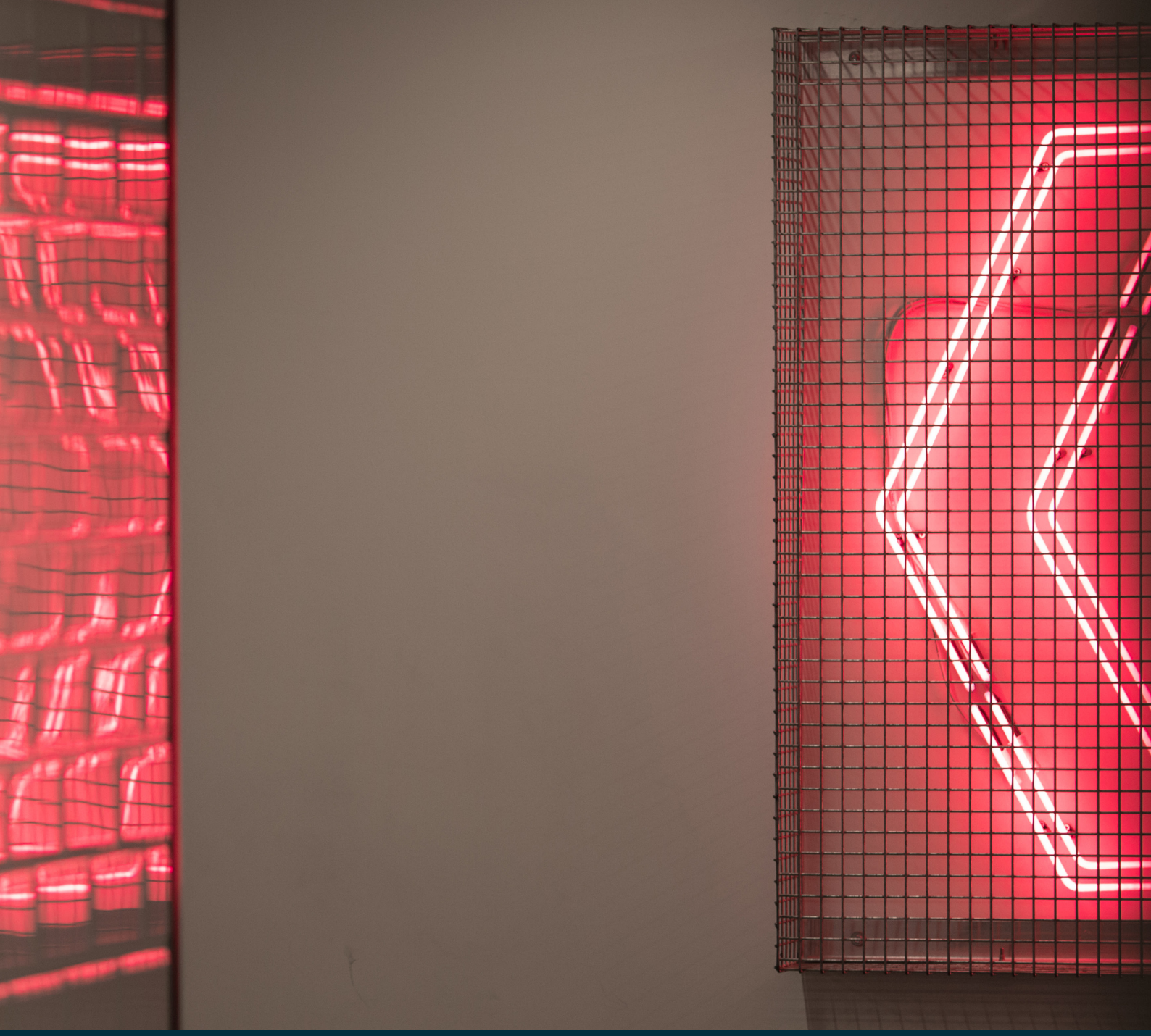
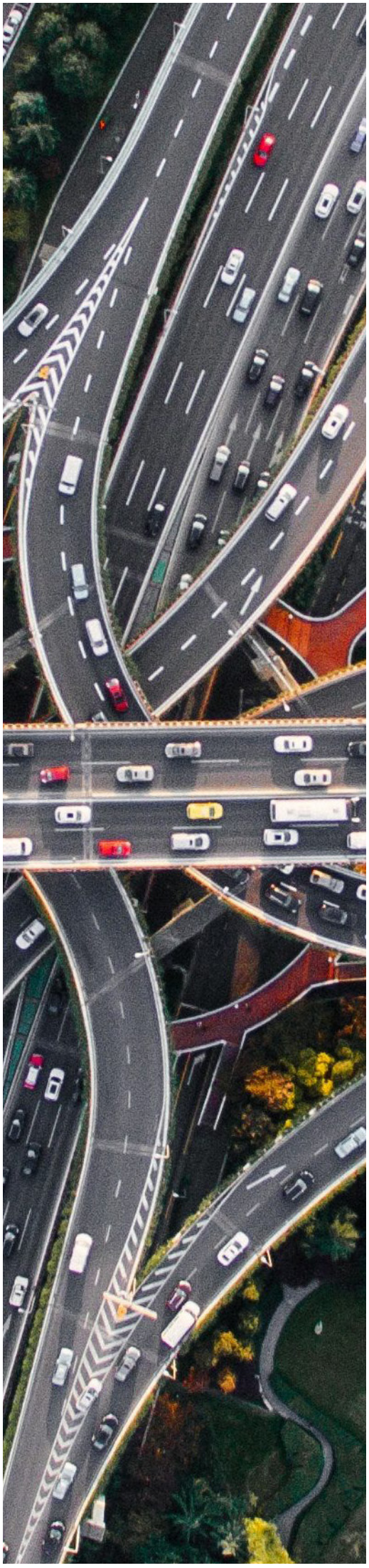


General Data Protection Regulation

Helping you understand the new era of data protection

SA LAW



Confused about the impact of the new General Data Protection Regulation? Worried that you aren't doing enough to meet your new obligations? SA Law has been helping clients to understand the new era of data protection, and guiding them towards compliance.

WHAT IS GDPR?

The General Data Protection Regulation is European legislation that harmonises the way organisations handle the personal data of EU nationals. GDPR came into force on 25 May 2018, and caused the biggest shake-up of data protection law for 20 years. It introduced new obligations for organisations, more accountability and a greatly increased fine for non-compliance. Even if the UK leaves the European Union, GDPR is here to stay.

WHY WAS THE LAW INTRODUCED?

The modern information era has turned personal data into a valuable commodity. Unfortunately, the laws that protect personal data were written before Facebook and Twitter existed, and when Google was just a relatively small start-up. As a result, the rapid expansion of online services over the last ten years caused a great deal of confusion over how organisations should protect people's identities, particularly in the face of escalating online crimes such as identity theft. GDPR brought the law up to date with the modern era.

ARE THE CHANGES SIGNIFICANT?

While many of the core obligations remain the same, there are some key changes that fundamentally affect the way your organisation handles personal data, from the way you talk to customers, to the way you recruit employees.

The most visible change is the new fine, which rises from £500,000 to around £18 million or 4% of your worldwide annual turnover, whichever is greater. If you suffer a data breach, you may also need to pay compensation to individuals who have been affected. Although the media painted a picture of apocalyptic ruin for any organisation that failed to comply with the new law by the launch date, the ICO has taken a more pragmatic approach when assessing reported data breaches. Nevertheless, it is paramount that you are compliant with the new law.

Perhaps the most significant change is the need to obtain free and unambiguous consent to hold a person's data. Implied consent no longer applies, so pre-ticked opt-in boxes don't count. This has meant that most organisations have needed to reconfirm consent to some degree with customers, marketing lists and employees. For anyone under the age of 13, consent must be obtained from their parents.

The new law also gives people the 'right to be forgotten', which means they can ask you to erase all data you hold about them. The new law also gives you less time in which to fulfil Subject Access Requests, so if someone asks to see a copy of all information you hold about them, you only have one month to comply under normal circumstances.

There are other changes that you will need to assess the impacts of, including new categories of personal data, and the requirement to report data breaches within 72 hours. For a full list, check out our 12-point outline of the key changes at https://salaw.com/gdpr-getcompliant/

> "A good solid, commercial and knowledgeable firm."
>
> LEGAL 500

WHAT SHOULD I BE DOING?

Meeting the new GDPR obligations can be boiled down to three compliance objectives. You must ensure that:

- All personal data you hold has been gathered correctly
- Your systems and processes store, use and dispose of personal data in accordance with the regulations
- Your employees are trained in their compliance responsibilities.

Our recommended roadmap to achieving this covers four logical stages:

1. Plan and audit

As always, change programmes such as these work best when they are organisation-wide in scope, and driven from the top. Begin by assembling an appropriate compliance team, with a senior leader as spokesperson and chair. Next, assign a budget. Although GDPR activities may not require extensive investment, some budget for awareness is likely to be needed.

2. Prepare

To identify the actions you need to take, you must first understand what the organisation is doing at the moment. Initiate a comprehensive fact-finding exercise to determine the full nature of the personal data you hold and how you process it. Ask key questions such as:

- How did you gather the data?
- How long have you held it for?
- Did every individual give their consent?

At the same time, understand how information flows around the organisation, and how employees actually handle it. All of this information helps to determine:

- The gap between your current systems and processes, and your GDPR compliance requirements
- The gap between how employees currently handle information, and the way they should be handling it
- How compliant your data is. For example, who do you need to obtain consent from?

With the gaps identified, you can plan your strategy for closing them.

> "Highly impressive, with an immediate grasp of the issues. They always come up with solutions which are pragmatic, sensible and commercial."
>
> CHAMBERS & PARTNERS

THINK POSITIVELY

One final thing to bear in mind is your attitude towards GDPR. It's easy to see it as a large stick with potentially devastating impacts when something goes wrong, but this won't help rally employees to the cause. Therefore, we recommend a more positive perspective. In an age where high profile data breaches and poor handling of the aftermath has weakened our confidence in many brands, GDPR represents an opportunity to 're-inspire' customer trust. In effect, it presents an opportunity for competitive differentiation that could help you stand apart from the crowd.

3. Implement

Start with systems and processes, and any policies that you use to govern them. These may need to be redrafted to reflect the new changes. The aim is to create a flexible Information Governance Framework (IGF) that complies with the regulations, yet enables you to deliver on short and long-term business objectives.

You can also begin to deliver awareness and education activities that prepare employees for the new law. Larger organisations will likely need a more formal change programme, while smaller ventures may only require a few informal training sessions.

Finally, begin the process of reconfirming consent with customers, employees and anyone else whose data you hold.

4. Deploy

Deploy your new information regime, and spend some time ironing out any bugs. It also helps to run a few breach scenarios to make sure everything operates smoothly, from employees notifying you promptly, to your marketing function preparing customer awareness communications, to your PR team making preparations for damage control.

5. Manage

Once compliant with the new data protection law, you need to stay compliant by keeping it at the heart of your organisation.

Make sure employees are following your data protection processes, policies and procedures on a day-to-day basis, including regularly reviewing, minimising and deleting data in line with requirements.

Data protection must stay on the agenda for operational meetings, and all new projects and organisational changes must be planned and implemented with 'privacy by design' in mind.

Ongoing data protection training is essential, both as part of your induction process and as refresher courses. Run regular data breach drills so you can execute your data breach plan swiftly. If faced with a breach, make sure you follow up by investigating the causes, implementing change, and communicating developments to staff and customers as required.

HOW CAN WE HELP YOU?

We can help you tackle the new data protection legislation head-on. SA Law's GDPR Response is designed to protect your organisation in this 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 postmortem 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 on the road to GDPR compliance 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