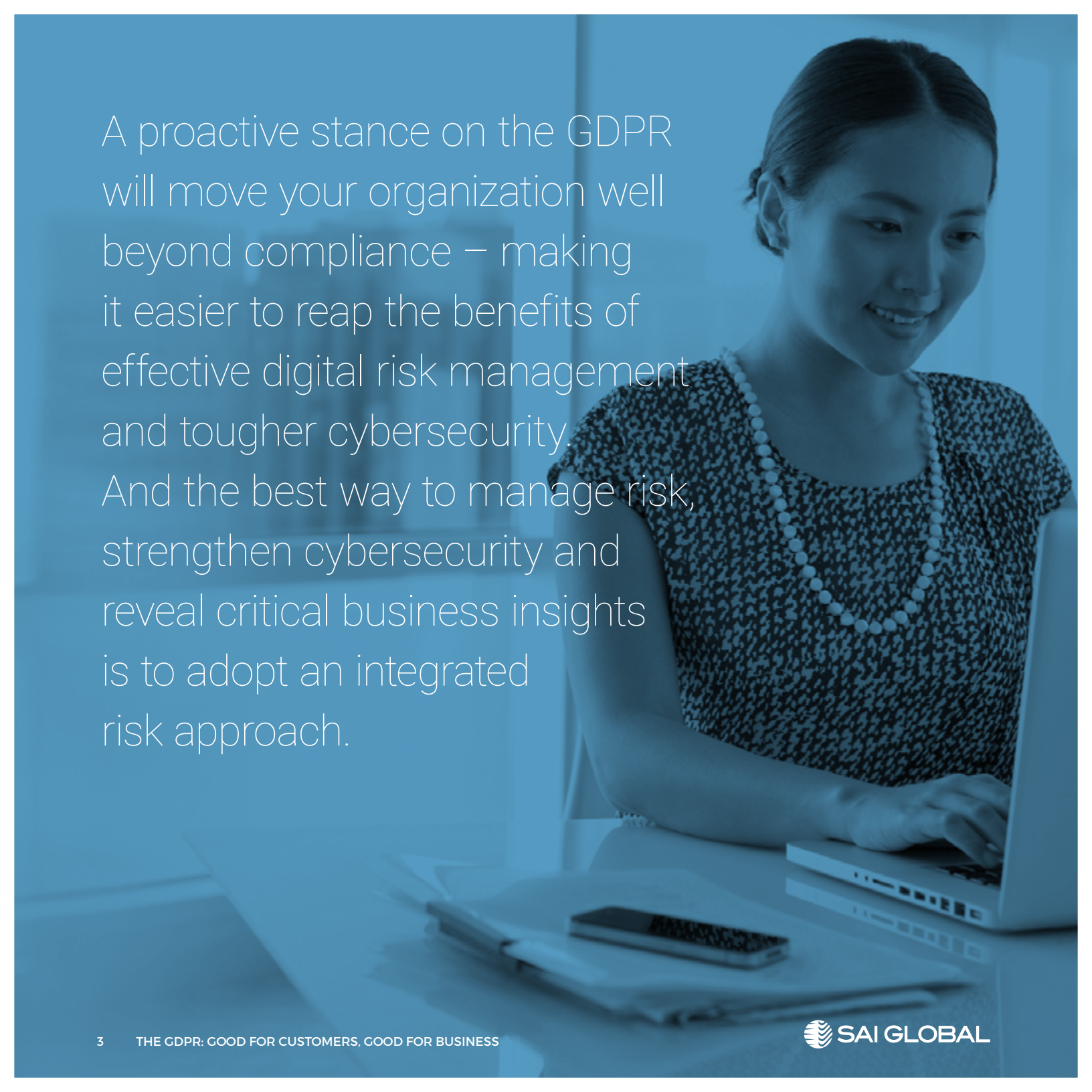
SAI GLOBAL

The GDPR: Good for customers, good for business

Contents



A proactive stance on the GDPR will move your organization well beyond compliance – making it easier to reap the benefits of effective digital risk management and tougher cybersecurity. And the best way to manage risk, strengthen cybersecurity and reveal critical business insights is to adopt an integrated risk approach.

SAI GLOBAL

The General Data Protection Regulation (GDPR) comes into effect across the European Union (EU) on 25 May 2018, and will impact any organization handling the data of EU citizens. On the one hand, businesses that approach the GDPR as a once-in-a-generation business opportunity that will also bolster their cybersecurity efforts are likely to prosper. Those who see it as simply another burdensome piece of privacy or digital security legislation, on the other hand, risk falling behind their more proactive competitors.

Understanding the GDPR: What it really means for your business

The GDPR is a much-anticipated regulatory change that aims to "harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy."[1]

However, its impact will be felt around the globe, since it applies not only to organizations located within the EU, but also those located outside the EU that offer goods or services to, or monitor the behavior of, EU 'data subjects'. The Australian government, for example, is advising that the EU GDPR may impact:

- Any business with an office in the EU
- Any business whose website enables EU customers to order goods or services in a European language (other than English) or enables payment in euros
- Any business whose website mentions customers or users in the EU
- Any business that tracks individuals in the EU on the Internet and uses data processing techniques to profile individuals to analyze and predict personal preferences, behaviors and attitudes[2]

The Regulation was four years in the making, but has deeper roots in the EU's 1995 Data Protection Directive. Subject to considerable debate, the GDPR was finally approved by the EU Parliament in April 2016 and comes into effect, after a two-year transition period, on 25 May 2018.

The GDPR is set to directly apply in the UK, despite Brexit. It will come into effect before the UK's withdrawal from the EU and the UK government has signaled its intention to continue the GDPR's application as part of the law of the UK.
The reasons for the UK's position, as outlined in the Queen's speech, suggest the GDPR may become a benchmark both inside and outside the EU:

- More than 70% of all trade in services is enabled by data flows – data protection is critical to international trade

- It will help put the UK in the best position to share data with other EU member states and internationally after it leaves the EU

- Staying close to the rights and obligations of the GDPR should be the least disruptive data protection option for future international trade and should "cement the UK's position at the forefront of technical innovation, international data sharing and protection of personal data"[3]

While some of the principles of data protection remain unchanged since the directive and the various consequential enactments (including the UK's Data Protection Act), the new regulatory scheme brings data protection into the digital age. While the EU has lagged behind for some time on data privacy legislation, the GDPR acknowledges the unprecedented challenges that the digital revolution has brought, and that we now live in "an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established."[4]

What the GDPR means or US companies

What the GDPR means for US companies
Many American businesses, regardless of industry, are effectively becoming 'data companies' as they gather customer information to personalize their offerings and as a source of revenue in itself. Implementing GDPR-compliant data practices across all their operations will be difficult for American businesses. It is likely that the best solution will be to separate US and EU data operations. This will add complexity and cost, but will allow companies to ensure compliance and maximize opportunities in the two marketplaces.

The GDPR is significant in the fact that it is a regulation, which is a binding legislative act. It replaces a directive, the Data Protection Directive 95/46/EC, which sets out the goals for EU countries, but leaves implementation to each country.

Key terms

Data subject: A natural person whose personal data is processed by a controller or processor.

Data controller: The entity that determines the purposes, conditions and means of the processing of personal data

Data processor: The entity that processes data on behalf of the data controller.

Data protection authority: A national authority tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the EU.

Data protection officer: An expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set out in the GDPR.

EU regulations, directives, standards and legislation

Regulation: A regulation is a binding legislative act that must be applied in its entirety across the EU.[5]

Directive: A directive is a legislative act that sets out a goal all EU countries must achieve, however it is up to each country to devise its own laws on how to reach that goal.[6]

Standard: Standards are technical specifications defining requirements for products, production processes, services or test methods. These specifications are voluntary.[7]

Legislation: The EU's normal legislative procedure gives the same weight to the European Parliament and the Council of the European Union. On certain questions (e.g. taxation), the Parliament gives only an advisory opinion.[8]

What data does it apply to?

Article 4 (1) of the GDPR defines personal data widely, as any information relating to an identified or identifiable natural person (a data subject), including:

- Name
- Identification number
- Location data
- An online identifier
- Anything that identifies a person directly or indirectly by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person (including IP addresses, for example, and even data that replaces clearly personal details such as a name with another unique identifier such as a number)

Risks? What risks?

Increased fines for non-compliance is the risk attracting the most attention from boards around the world. Organizations in breach of the GDPR can be fined up to 4% of annual global turnover or revenue (or €20 million, whichever is greater). This penalty applies regardless of the level of an organization's EU presence, so even a US company with a small EU market will face a fine based on global turnover/revenue.

The GDPR does take a tiered approach to fines, however, and this maximum would apply only in relation to serious offenses such as breach of requirements relating to international transfers or the basic principles for processing, such as conditions for consent. The GDPR also empowers other actions, such as warnings, reprimands, bans on processing, suspension of data transfers and the correction of an infringement. So organizations face a combination of fines, financial loss and decreased productivity for non-compliance.

And the environment within which these penalties apply is fueling concerns. The GDPR is far-reaching, introduces many new obligations, tightens requirements around consent and confers enhanced rights on individuals, including the right to be forgotten, rights to understand profiling by controllers and third-party data processors, and the right to port data between organizations.

Risks? What risks?

Under the GDPR, the European Data Protection Board will be established and the regulation envisages the issuing of guidelines and establishment of codes of conduct and certification mechanisms by the Board. Without this governing body to issue guidelines and certify organizations as GDPR compliant, a level of uncertainty is added to the mix.

However, the biggest threat may be one that isn't found in the regulation – the risk of reputational damage. Customers expect privacy and are increasingly punishing organizations that break their trust.

Key principles

Article 5 of the GDPR contains principles relating to the processing of personal data, with an emphasis on:

Fair, lawful and transparent processing: Data processing must meet GDPR requirements and the individual data subject must be aware of the processing.

Purpose limitation: "Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."

Data minimization: "Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed."

Accuracy: Data should be up to date and, if inaccurate, erased or rectified without delay.

Storage limitation: "Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."

Integrity and confidentiality: Ensuring appropriate cybersecurity, including protection against "unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

Show me the benefits!

On the other side of risk and threat is opportunity. Organizations that can stay ahead of the cybersecurity game and maintain authorized data sharing and access will build and protect trust, and the GDPR is a framework for achieving this.

Taking steps to comply with the GDPR means:

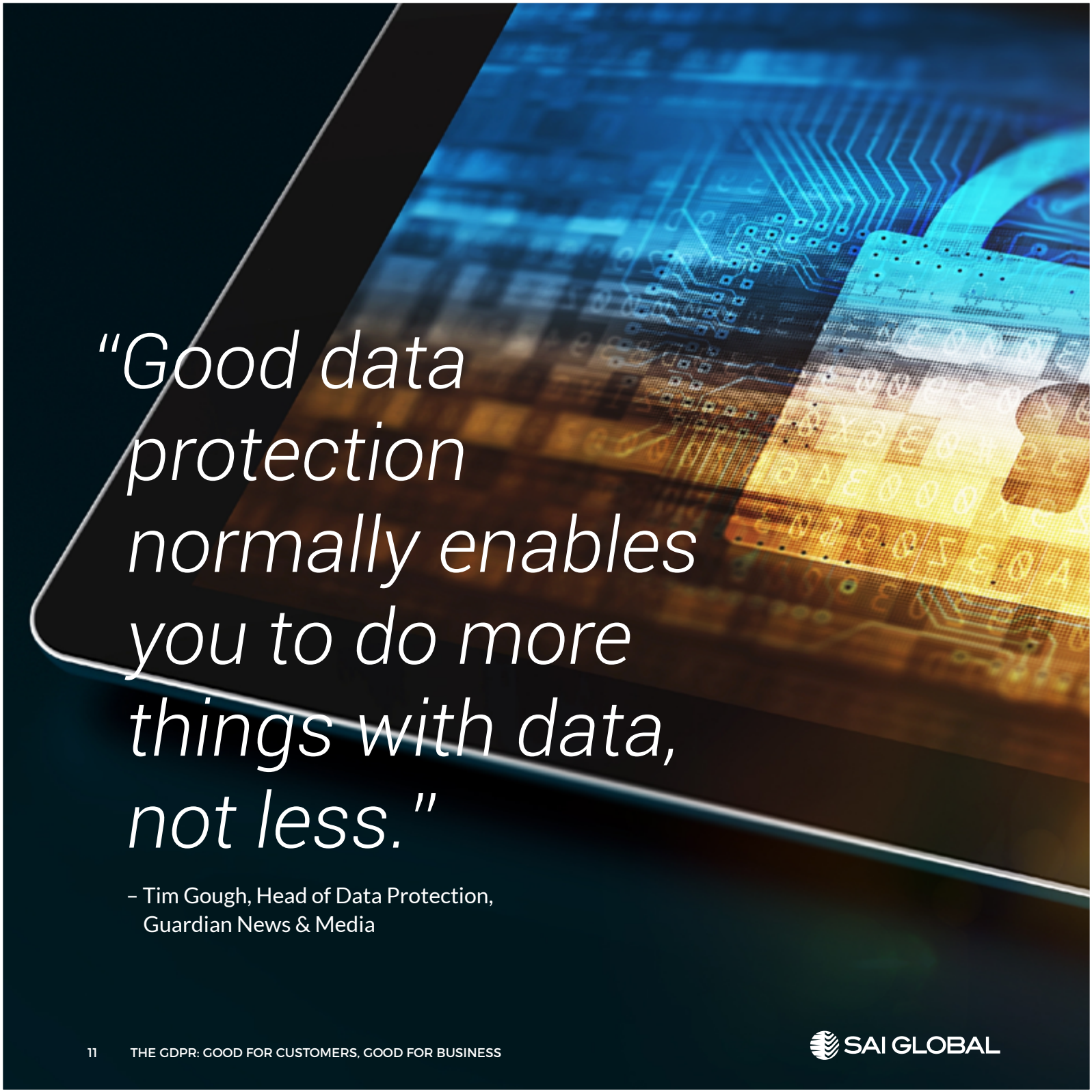
- Your organization will be at the forefront of responsible data practices, building a strong foundation of trust with customers
- Unlocking business opportunities for those outside the EU, allowing them to market to, and win business, in the EU market
- Safer and simpler cross-border transactions for organizations within the EU

GDPR compliance involves addressing accountability requirements around documentation, data protection impact assessments, and data protection by design and by default. This translates to increased transparency and ease of monitoring and accessing data. And the thorough review of data-handling practices triggered by the GDPR can bring people within your organization together, creating opportunities to improve customer satisfaction, business processes and techniques for managing data across the business.

The GDPR's data breach notification requirements should also prompt organizations to adopt internal procedures for handling data breaches – and a proactive response to a crisis is an opportunity to not only repair trust but to build it too [link to SAI trust white paper].

Finally, the GDPR can be a path to better business insights. Organizations with a reputation for hygienic data handling and practices are likely to learn more about their customers. Research shows that "customers are willing to share their information if they know you are using it to help them get what they want while ensuring that the information is kept secure."[9]

Powerful business insights can be pulled from this data, helping you improve your offering and better target your ideal market.



"Good data protection normally enables you to do more things with data, not less."

– Tim Gough, Head of Data Protection, Guardian News & Media

SAI GLOBAL

What should you do?

If you haven't already started to prepare for the GDPR, it's time to act now. And while it's a considerable and complex task, breaking it down into phases will help you cover the fundamental requirements:

1. Discover: Locate and classify your data

Document what personal data you hold, where it is stored, how it is stored, where it came from, who you share it with and how it is made secure. To create this information awareness you may need to organize an information audit across the organization or within particular business areas. Also look at the various types of data processing you carry out, and identify your legal basis for carrying it out. The end result will be an inventory of all your data.

2. Plan: Run a gap analysis, allocate resources and set a timeline

Once you have a clear idea of your current data storage, practices and security, a gap analysis will allow you to identify the measures and solutions that can help move you towards GDPR compliance. You should also conduct a data privacy impact assessment and a vendor review, to ensure you have a complete picture of your requirements. Getting ready for compliance will take time and resources, so develop a thorough plan.

SAI GLOBAL

3. Implement: People, processes, policies and technology

Make sure you have the right people on-board to drive the measures required to implement GDPR compliance. It's important to design then document a process that will deliver the information and actions required.

Controllers should take steps to show they have taken data protection compliance into consideration, and have implemented appropriate compliance measures in relation to data processing activities. In particular, controllers should adopt internal processes and policies which meet the principles of privacy by design and data protection by default.

You should review your current data privacy policies and put a plan in place for making any necessary changes in time for GDPR implementation. Individual rights are also highlighted in the GDPR: check that your procedures cover all these rights and consider creating a system for subject access requests.

Also consider the technology available to automate the processes you've put in place to comply with the GDPR.

4. Test: How robust are your processes and incident response plan?

You should now start to make sure you have the right procedures in place to detect, report and investigate a personal data breach and that these are monitored continuously. GDPR training within your organization can help build awareness of this requirement for ongoing vigilance and ensure ongoing compliance with processes.

Assessment and breach management protocols should be regularly tested and updated to ensure their currency.

What could you do? What *will* you do?

To realize the business opportunities that the GDPR may bring, you need to ask yourself not just what you should do, but what you could do to make the most of this change. You can kick risk to the curb, revitalize cybersecurity efforts and make better, data-fueled business decisions if you:

- **Take a smart integrated risk management approach**

Information security is a key driver of trust and an issue close to most consumers' hearts.[11] One survey shows that in the US:

- 93% of adults say that being in control of who can get information about them is important and 74% feel this is very important

- 90% say that controlling what information is collected about them is important and 65% think it is very important[12]

The best GDPR compliance solution will integrate risk management to turn the GDPR into an opportunity. This is the Intelligent Risk approach: an approach that can help your organization navigate change and protect the valuable trust you've built in your brand or business by focusing on the risks to the drivers of trust, the risks associated with achieving your strategic goals and informing your organization's propensity to take risk.

- **Implement a digital platform to monitor compliance**

Building automated solutions and choosing products and solutions that enable more flexible data-handling practices can simplify compliance and reduce costs in the longer term. Automated platforms can help you identify assets; conduct continual improvement, business impact and risk assessments; assist with threat and vulnerability management; and more. By reducing the risk of data breaches via human error, they enhance your incident and breach-handling capabilities.

- **Map data to generate insights**

Data mapping is a key technique in identifying, understanding and mapping out a comprehensive overview of how data flows within, to and from your organization – facilitating compliance and also providing insights to improve business performance. GDPR is likely to make third-party risk greater, but data flows can help identify third-party risk that is incompatible with your risk appetite.

Data mapping

Data mapping identifies connections between two data sets. The key is to create the 'golden record' that orchestrates data on all activities – including breaches, record management, information security measures, self-assessments, data protection impact assessments and more – and combines it into a 'single source of truth'.

GDPR and third-party risk

Who do you rely on outside of your organization to help meet business obligations and demands? While third parties bring many business benefits, this reliance also carries risk – third-party risk. Regulatory violations are a key source of third-party risk, and the GDPR is likely to be a significant source of these.

While the GDPR can easily be seen as just another business burden, the benefits of compliance are great and will unlock opportunities both inside and outside the EU. As you put a plan in place for ensuring compliance with the fundamental requirements, consider framing the change as a business opportunity – and unlock even more opportunity.

Read more about getting ready for the GDPR or speak with an SAI advisor about GDPR solutions

SAI GLOBAL

References

1. EU GDPR Portal.

2. Office of the Australian Information Commissioner, Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation.

3. Paisner, Berwin Leighton 2017, 'GDPR and Brexit: UK Government unveils Data Protection plans', Lexology, 22 June.

4. EU GDPR Portal, GDPR key changes.

5. European Union, Regulations, Directives and other acts.

6. European Union, Regulations, Directives and other acts.

7. European Commission, European Standards.

8. European Parliament, About Parliament.

9. Olenski, S 2016, 'For consumers, data is a matter of trust', Forbes, 18 April.

10. Scribd, 'The Guardian reaches out to focus groups'.

11. SAI Global 2017, Consumer Trust Index

12. Pew Research Center, Internet & Technology 2015, 'Americans' attitudes about privacy, security and surveillance', 20 May.

SAI GLOBAL