Risk. Reinsurance. Human Resources.

EU General Data Protection Regulation

A new era in data protection

May 2017

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

Introduction

"The European Union data privacy landscape is about to undergo dramatic change, with lasting enterprise wide implications for the way that organisations handle, protect and use the personal data of EU individuals.

Organisations of all sizes, across all industries, and geographies that process personal data of EU residents need to take steps now to comply with the new EU General Data Protection Regulation by 2018, to satisfy management fiduciary duties and avoid potentially costly penalties."

Kevin P. Kalinich, Esq., Global Cyber Practice Leader, Aon Risk Solutions

---

The European Union General Data Protection Regulation (EU GDPR) is set to come into effect on the 25th of May 2018 and will strengthen the rights of individuals online, while creating significant obligations for businesses operating in an increasingly connected world.

The regulation applies to information which directly or indirectly identifies an individual, including customer lists, contact details, genetic/biometric data, and online identifiers like IP addresses.

While the EU GDPR builds on the prior EU Data Protection Directive, it brings significant changes in several areas. All organisations globally that process personal data either relating to the offering of goods or services, or the monitoring of activities of EU residents, will need to comply.

The new regulation will require organisations to strengthen existing controls, implement new processes and procedures, and document, embed and evidence them appropriately. Organisations will also have to consider the best ways of enabling individuals to exercise their rights surrounding their personal data and its use.

The EU GDPR is therefore a game-changer when it comes to the collection, processing and storage of personal data, and one with global implications. As such, organisations need to evaluate their existing position, prepare for the impending changes, and ensure their data protection systems are robust going forward.

Requirements

The business changes needed to comply with the EU GDPR will vary from organisation to organisation, however they are likely to be significant.

For instance, organisations should only collect personal data needed to fulfil specific, documented purposes, and where there is a permitted basis under GDPR for the collection. Public authorities, organisations processing large amounts of special categories of data, or whose core activities involve the regular and systematic monitoring of individuals, must appoint a data protection officer with expert knowledge.

The regulation introduces the concept of accountability, requiring organisations to embed privacy controls into their operations and mandatory privacy-risk impact assessments for any new project likely to result in a high risk to individuals' privacy.

The EU GDPR introduces a 72-hour notification requirement for all personal data breaches, except those which are unlikely to pose a risk to individuals. In the case of serious incidents, there will also be a duty to notify the affected individuals of the breach. Currently, the EU only requires organisations in certain sectors or countries to notify breaches or cyber attacks to regulators.

Fines for non-compliance with the EU GDPR will increase to as much as €20 million or, if higher, to 4% of an organisation's annual global turnover. This is a significant escalation from the current penalties under existing data protection laws. Fines for serious violations have the potential to reach the billions for large, global companies.

The EU GDPR will create significant challenges for business, particularly following a loss or exposure of personal data per the effective date of the 25th of May 2018. Here we explore a couple of potential fictional scenarios.

Scenario of a European retail company with headquarters in Brussels

A retail company based in Belgium, with operations in Belgium, France and the Netherlands, takes a proactive approach to the EU GDPR. Handling customer data from its Brussels headquarters, the company implements tough new security measures to limit any loss of personal data, while appointing a data security officer and a top-down assessment of data privacy measures.

Some time after the EU GDPR has come into effect, the firm suffers a cyber attack that results in the loss of a large cache of personal data. The cyber attack exposes weaknesses in the firm's controls, particularly in relation to deletion of personal data no longer required for business operations or record keeping. However, the firm's incident response team effectively responded to the attack, notifying the Belgium regulator and individuals as required.

While the firm is now liable to censure by the Belgium regulator – and potentially within the other territories in which it operates - thanks to its proactive approach to data privacy protection, the penalties it faces are reduced in light of its efforts to comply with the EU GDPR.

Scenario of a US-headquartered global pharmaceutical firm

A US headquartered pharmaceutical, with offices and factories throughout the world, is a conglomerate formed from the mergers of several smaller institutions over the course of the past 15 years. Because of this conglomerate and some incompatible IT, accounting, and financial systems, the company's approach to GDPR has been fragmented, with several parallel efforts having been conducted with limited oversight from headquarters.

Shortly after the EU GDPR has come into effect, data protection authorities in three EU countries receive complaints from employees of a recently acquired entity that their personal data has been unlawfully transferred to the US. The acquisition in question was previously headquartered in an EU country, but post-merger, the HR and operational administration of its employees and personal information was transferred to the appropriate departments in the US, for reasons of efficiency.

After a detailed investigation, one of the regulators finds that after a two year process, there were insufficient controls, care and protection placed around the personal information of the affected employees, and that there are several similar issues affecting other groups of employees. Given the wide-spread nature of the violations, the the Data Protection Authority (DPA) seeks to impose a fine based on a percentage of the group's worldwide turnover, rather than the local entity's turnover.

These scenarios might be fictional right now, but they could become reality in the near future. With limited time to prepare organisations are advised to make sure they are ready for the new regulatory requirements.

Given the significance of the changes and the increased enforcement powers of regulators, business leaders need to ensure they are taking steps to comply with the impending rules.

Action checklist

We have outlined ten steps to help businesses prepare:

1. The board should be accountable for data protection and ensure data protection risks receive ongoing attention and review from the C-suite.
2. Perform a risk analysis on new projects to identify privacy risks and necessary mitigation measures and assess the appropriate technical and organisational measures required.
3. Create a data-processing register detailing what data is held by the company, how it is stored and transferred, what it is used for and by whom.
4. Classify personal information in terms of risk, to comply with data retention periods, and establish a procedure to erase data when the retention period has passed.
5. Evaluate and actively manage existing contracts with third party service providers with whom you share personal data on an ongoing basis, to ensure they include all of the mandatory obligations prescribed by the EU GDPR.
6. Establish, embed and test a procedure to handle personal data incidents.
7. Increase the privacy-awareness of your employees.
8. Ensure employees can recognise and respond appropriately to requests from data subjects seeking to exercise their rights under the EU GDPR (for example: right to object, right to be forgotten). Any processes for responding to such rights should be clearly documented and embedded into business practices.
9. Determine and document whether your organisation should have a Data Protection Officer.
10. Review and amend privacy statements and notices to meet the enhanced transparency requirements.

Common pitfalls

As with any change within an organisation, there are various challenges to navigate. When implementing the EU GDPR, be aware and avoid the following common pitfalls:

1. Not having a clear understanding where and how personal data is stored, how it moves around your enterprise, how it is protected and how it is deleted once no longer required.

2. Underestimating the challenges of implementing a robust, effective programme for data subject rights, such as subject access requests and requests to delete personal data.

3. Not having an enterprise-wide incident response plan in place. The plan should incorporate escalation plans and nominated advisors covering all required stakeholders, including business operations, legal, PR, and key third parties such as IT service providers on whom you rely.

4. Failing to consider supplier / third party data protection management on an ongoing basis.

5. Failing to implement and maintain internal training programmes and procedures.

Conclusion

Addressing the EU GDPR will require careful consideration and coordination by internal stakeholders in order to accommodate the multi-faceted nature of the issue.

The actions that have been detailed above will be best served by parallel work streams, along with task dependencies and crossover. This can be a challenging task to manage given the limited time left to comply. The organisations that will progress most smoothly will be those that commit significant resource and have senior buy-in early in the process, and that do not underestimate the tasks ahead.

Now is the time to consider the implications of the EU GDPR and to prepare and respond in a manner that is proportionate to the nature of your business. Data and individual privacy rights are increasingly significant issues facing firms globally, and the EU GDPR sets the tone for future data privacy standards that will have increasingly global implications.

Contacts

Adam Peckman
Global Cyber Risk Consulting Practice Leader
+44 (0)7803 695 386
adam.peckman@aon.co.uk

Alexander Carte
+44 (0)20 7061 2302
Managing Director Stroz Friedberg
acarte@strozfriedberg.co.uk

Spencer Lynch
+44 (0)20 7061 2304
Managing Director Stroz Friedberg
slynch@strozfriedberg.co.uk

Vanessa Leemans
+44 (0)20 7086 4465
Global Cyber Chief Operating Officer
vanessa.leemans@aon.co.uk

Kevin Kalinich
+1 312 381 4203
Global Cyber Practice Leader
kevin.kalinich@aon.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance. For further information on our capabilities and to learn how we empower results for clients, please visit: http://aon.mediaroom.com/

STROZ FRIEDBERG
an Aon company

AON
Empower Results®