THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

CAPCO

It's a major regulatory development and there are just two years to prepare for compliance. The time to understand the impacts and implications - and to get ready for implementation - is now.

The clock is ticking louder every day. The EU General Data Protection Regulation (GDPR) rules will become compulsory from **25 May 2018[i]**. Organisations, businesses and institutions will need to take action to implement effective compliance measures. Key activities will include end-to-end process reviews, adjustment or amendment of relevant controls and re-alignment of risk profiles. Everyone concerned also needs to take into account the tough penalties that come with breach of this legislation. Who are the key actors? And what do they need to know?

Decision-makers and others in responsible roles must get involved. They need to understand quickly that the law is changing to the GDPR and that the time scales are tight. They need to appreciate the impact the new Regulation will have. Finally, they need to identify the areas within their business operation that could cause compliance problems. The tasks ahead are not trivial. Ensuring compliance could have significant resource implications, especially for larger and more complex organisations. All those concerned **must** keep at front of mind the urgency of the situation. We only have **24 months** as a lead-in period for raising awareness and implementing required changes. Compliance will be challenging, even for organisations starting to prepare now. For those who delay until the last minute, time – and regulatory tolerance – will undoubtedly run out.

PENALTIES

The Regulation will enforce tough penalties; the proposed fines are **up to 4% of annual global turnover or €20million, whichever is greater.**

KEY CHANGES

Below is a breakdown of the key changes proposed by the Regulation:

1. The definition of personal data will become broader, bringing more data into the regulated perimeter

Previously, personal data has been defined as data which relates to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Regulation expands the definition of personal data such that data privacy will encompass other factors that could be used to identify an individual, such as their genetic, mental, economic, cultural or social identity.

The Regulation will require that personal data held must be documented and include where it came from and with whom it is shared. An information audit may be required, across the organisation, or within particular business areas to complete this documentation. Under the Regulation, if inaccurate personal data is held and has been shared with another organisation, the other organisation must be told about the inaccuracy so it can correct its own records. This will not be possible unless it is known exactly what personal data is held, where it came from and who it is shared with.

Additionally, measures must be taken to reduce the amount of personally identifiable information stored and ensure that information is not stored for longer than necessary.

2. If a business is not in the EU, they will still have to comply with the Regulation

Non-EU controllers and processors who deal with EU subjects' personal data must comply with the new Regulation. Although enforcing regulation beyond EU borders will be a challenge, those providing products or services to EU customers, or processing their data, will face sanction under the Regulation if an incident is reported.

Organisations, businesses and institutions should have competent and well-tested controls along with complete and accurate back-ups to assimilate an audit trail. Having a suitable controls framework in place will provide support if an incident is reported or when it comes to any form of data breach in supporting a case to minimise regulatory impact.

3. Special protection for children's data

The Regulation will bring in special protection for children's personal data.[ii] If information is collected about children (in the UK defined as anyone under 13 years old) then parental consent will be required in order to lawfully process their data.

4. Rules for obtaining valid consent will change

The consent document must be laid out in simple terms, and it is likely that the consent will be required to have an expiry date. Where the consent is for processing a child's data the privacy notice and the consent must be written in language a child can understand. Silence or inactivity will not constitute or imply consent. Unless there is a positive consent, consent is deemed to be withheld.

5. Introduction of data breach notification regulations and changes in liability will have a profound impact on the supply chain

There is no obligation to notify authorities of data breaches under the current Directive, although there are some sector-specific requirements, such as those applicable to communications providers and ISPs under the E-Privacy Directive. The Regulation will bring in a breach notification duty across the board. This will be new to many organisations. Not all breaches will have to be notified to the regulator, only ones where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach and, where the breach puts individuals' data at risk, the data subjects must also be informed.[iii] Although the exact timelines for breach notification are still unclear, these changes place a greater emphasis on supply chain data security. Regular supply chain reviews and audits will be required to ensure they are fit for purpose under the new security regime. The Regulation clearly calls for more effective data breach investigation, categorisation, containment and response infrastructure.

Organisations, businesses and institutions must ensure they have the right procedures in place to detect, report and investigate a personal data breach. This could involve assessing the types of data held and documenting which ones would fall within the notification requirement if there was a breach. In some cases organisations, businesses and institutions will have to notify the individuals whose data has been subject to the breach directly, for example where the breach might leave them open to financial loss. Larger organisations will need to develop policies and procedures for managing data breaches – whether at a central or local level. Failure to report a breach, when required to do so, will result in a fine as well as the penalty for the breach itself.

6. Subject Access Requests and the "right to be forgotten"

The rules for dealing with subject access requests will change under the GDPR. In most cases organisations, businesses and institutions will not be able to charge for complying with a request and normally will have just a month to comply, rather than the current 40 days. There will be different grounds for refusing to comply with subject access request – manifestly unfounded or excessive requests can be charged for or refused. If any request is to be refused, policies and procedures will need to be in place to demonstrate why the request meets the refusal criteria.

Additional information will also need to be provided to people making requests, such as data retention periods and the right to have inaccurate data corrected. If a large number of access requests are being handled the impact of the changes will be considerable so the logistical implications of having to deal with requests more quickly and provide additional information will need to be addressed. The Regulation also requires that data subjects should have the "right to be forgotten". This requirement will extend to search engines and tools. The extent to which data controllers should be burdened with the responsibility of deleting information is not yet clear however.

7. Introduction of mandatory privacy risk impact assessments

A privacy impact assessment (PIA) is a tool which can help identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

The Regulation will contain conditions under which a PIA will always be required such as in high-risk situations, for example, where a new technology is being deployed or where a profiling operation is likely to significantly affect data subjects.

8. Privacy by design

The current EU Directive does not include any clauses related to privacy by design but under the new Regulation, data controllers will have to implement appropriate measures to ensure that processing protects the rights of the data subject, that only the minimum personal data will be processed, and that the data is not disclosed more widely than necessary.

The essence of privacy by design is that privacy in a service or product is taken into account not only at the point of delivery, but from the inception of the product concept.

9. Future-proofing new contracts

Parties will need to document their data responsibilities even more clearly, and the increased risk levels will impact negotiations on security standards, risk allocation and pricing.

10. The international transfer of data

Since the Regulation will also be applicable to processors, organisations should be aware of the risk of transferring data to countries that are not part of the EU. Non-EU controllers will need to appoint representatives in the EU. The separate EU-U.S. Privacy Shield agreement also contains strict penalties for those in breach the privacy of European citizens and requires parallel consideration.

11. Introduction of data portability

The right to data portability is new in the Regulation. This is an enhanced form of subject access where organisations, businesses and institutions have to provide the requested data electronically and in a commonly used format. Many organisations will already provide the data in this way, but if paper print-outs are used, or an unusual electronic format, procedures will have to be revised and any necessary changes made.

12. Appointment of a Data Protection Officer (DPO)

Some organisations will need to appoint or (at minimum) designate a DPO to take responsibility for data protection compliance.

NEXT STEPS

For all the demands that it will make on resources through the preparation and implementation periods, GDPR should be still be seen as a positive step for businesses. (Not least because it brings clarity, direction and protection for those organisations achieving and maintaining compliance.)

As an immediate next step, organisations must ascertain whether they have adequate resources and expertise in such key areas as finance, information technology, compliance, risk, legal and IT service management. If they do not, they need to source external counsel that is fully capable of supporting them through preparation for, and implementation of, the proposed changes.

Competent specialists will be able to perform an initial review and make recommendations which align with business requirements, objectives and risk appetite. Where required, they should also be capable of supporting the achievement of the highly desirable European Privacy Seal[iv] ("EuroPriSe"). (This endorsement certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the EU Member States.)

With a very tight 24-month preparation period, the point bears repeating: competent, focused and effective preparation must begin now. For those organisations lacking in some or all of the core analysis and implementation skills, the first task must be to build their competence – with external help if needed. That help should be sought and engaged as rapidly as possible. The time to act on GDPR is now.

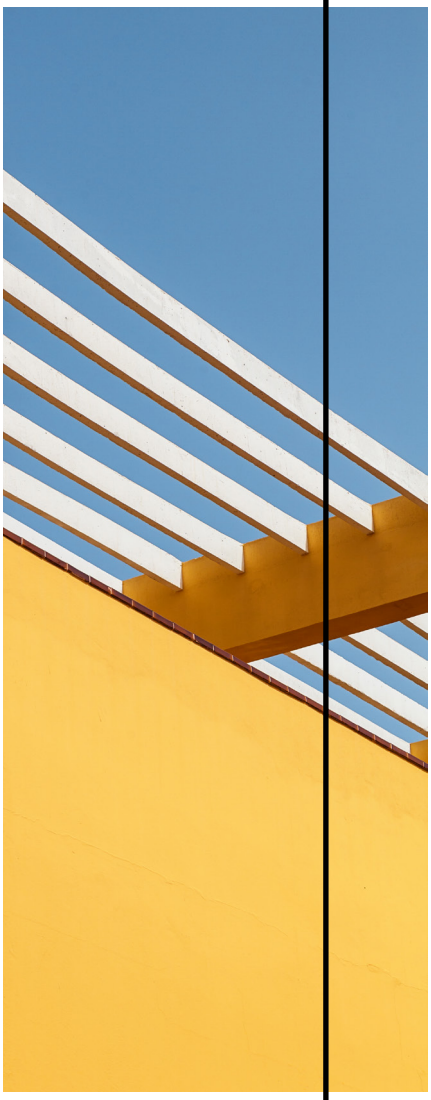
References

[i] The Regulation will enter into force on 24 May 2016 and will apply from 25 May 2018. The deadline for implementation is 6 May 2018. Source: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[ii] Proposal for a General Data Protection Regulation – Article 8

[iii] Supra 1, Article 32

[iv] http://www.european-privacy-seal.eu



AUTHORS

Roger Hamilton roger.hamilton@capco.com
Simon Stickley simon.stickley@capco.com
Andrew MacQueen andrew.macqueen@capco.com

ABOUT CAPCO

Capco, an FIS™ company, is a global management consultancy with a focus in financial services including banking and payments, capital markets, and wealth and asset management, plus a dedicated energy division. We combine innovative thinking with unrivalled industry knowledge to deliver business consulting, digital, technology and transformational services. Our collaborative and efficient approach helps clients reduce costs, manage risk and regulatory change while increasing revenues.

To learn more, visit our web site at www.capco.com or follow us on Twitter @Capco

WORLDWIDE OFFICES

Bangalore - Bratislava - Brussels - Chicago - Dallas - Dusseldorf - Edinburgh - Frankfurt - Geneva - Hong Kong - Houston - Kuala Lumpur - London - New York - Orlando - Paris - Singapore - Toronto - Vienna - Washington,DC - Zurich

To learn more, contact us in the U.K. at +44 20 7426 1500, in continental Europe at +49 69 97 60 9000, in North America at +1 212 284 8600, visit our website at CAPCO.COM or follow us on Twitter @Capco