PROTIVITI FLASH REPORT

Preparing for the General Data Protection Regulation – The Clock Starts Ticking Now

May 31, 2016

After four years of negotiation, the European Union's General Data Protection Regulation (GDPR) was adopted on 14 April 2016, replacing European Union and national data protection legislation.[1] The GDPR came into force on 26 May 2016, and from this date, those subject to the regulation have been given a grace period of two years to review current practices and procedures and become compliant.

This legislation shares two common high-level objectives: harmonizing the fragmented legacy legislation among EU member states, and addressing public perceptions that doing business on the Internet is inherently risky. Many concerns arise from the wide publicity given to successful cybercrime attacks resulting in personal data theft. The explosive use of mobile devices, adoption of big data analytics and increased volumes of personal data being digitally generated, processed and shared creates opportunities for EU citizen data to be exposed. The GDPR aims to make the online environment more trustworthy and harmonized, therefore supporting a smoother functioning of the EU's Digital Single Market.

The General Data Protection Regulation (GDPR)[2]

The GDPR replaces the European Union's 1995 Data Protection Directive (DPD), which was enacted in the early days of the Internet, when many of the digital communication methods used today did not exist. This legislation provides a unified set of rules designed to give European citizens more control over their private information in a digitized world of smartphones, social media, electronic banking and global e-commerce. The aim of the GDPR is to strengthen trust and provide a higher level of protection for all individuals across the European Union and applies to firms outside Europe doing business with EU consumers.

Because the European Union's Parliament approved the GDPR as a regulation rather than a directive, its implementation will be consistent across all Member States and will not require any further local laws to be enacted – i.e., there is no need for a country-specific law such as the UK Data Protection Act.

The following key areas regarding the new regulation should be noted:

- An increase in material sanctions for breaches of regulations
- The need for companies to formally appoint a data protection officer (DPO)
- The requirement to perform a data protection impact assessment
- The need to integrate data protection methods into business-as-usual (BAU) processes
- A requirement to establish a compliance framework
- Requirements to report data breaches within 72 hours of a data breach becoming known

[1] http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

- Clarity on international data transfers within multinational companies
- Increased rights of data subjects
- Revised rules on establishing consent from data subjects
- Increased responsibilities for data processors for reporting data breaches.

Further discussion about and recommendations for each of these topics is presented in the following pages.

Is your organisation subject to the GDPR?

The GDPR defines personal data as follows:

> *Any information relating to any person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.*

The GDPR has expanded territorial applicability and increased scope to all those that process data about EU citizens; those who store or use this data or who even market to EU clients are subject to the GDPR. Even if orders are not part of the interaction with EU citizens, the moment an organisation obtains personal data from them, regardless of the purpose, the organisation is subject to the GDPR.

It is worth noting that the GDPR has also expanded the definition of "personal data" to include online identifiers, including IP address, cookies and so forth, which will now be regarded as such if they can be linked back to the data subject without undue effort.

What are the implications of not complying with the GDPR?

Article 79 states that a company that violates certain provisions of the GDPR, such as the basic processing principles or the rules relating to cross-border data transfers, may be subject to fines amounting up to €20 million or to 4 per cent of the data controller's or data processor's total global worldwide annual turnover of the preceding financial year, whichever is higher.

Preparing for GDPR compliance

Companies are advised to act now and utilise the two-year grace period to bring their business into full compliance with the GDPR. An organisation located outside the European Union and not subject to the prior regulation will likely need this time to implement the required changes. The broad scope of the GDPR, both in terms of organisations to which it is applicable and the steps required to reach and maintain compliance with it, means that preparations should begin sooner rather than later.

Organisations should consider the following high-level requirements and recommendations:

- **Appoint a data protection officer:** Article 37 of the GDPR states that data controllers and processors shall designate a data protection officer (DPO) where the core of the organisation consists of processing operations which

  a) require regular and systematic monitoring of data subjects on a large scale; or

  b) consist of processing on a large scale of special categories of personal data relating to criminal convictions and offences.

  Key consideration**:** *If a company has not yet appointed a DPO, someone with the appropriate skills and experience should be assigned and take accountability for this important role in order to meet the requirement.*

- **Perform a data protection impact assessment:** Article 35 of the regulation requires data controllers to perform a data protection impact assessment (DPIA) in situations in which processing operations present specific risks to the rights and freedoms of data subjects. The assessment should contain at least a general description of the planned processing operations and an assessment of the data privacy risk.

  Key consideration**:** *Undertake a DPIA to understand key data privacy risks the organisation may face, and establish a prioritised plan to mitigate these. This DPIA should include an assessment of the type of private data processed and the types of risks it may face in complying with the GDPR requirements. We also recommend that such a DPIA be included as part of a broader information risk assessment driven top down by senior management.*

- **Integrate data protection methods in during design:** Article 25 requires a data controller to consider the privacy and protection of personal data within each project developed (both structural and conceptual) from the design stage. The GDPR associates the principle of data protection by design to the principle of data protection by default, which enforces personal data protection, stating that, by default, companies should treat personal information to the extent necessary for their intended purposes for a period strictly necessary for such purposes and should ensure that personal data is not accessible to an indefinite number of people.

  Key consideration: *Review application development processes to ensure that data protection is being considered and executed as outlined by the GDPR. The same review should be performed for existing business processes that leverage private information.*

- **Establish a compliance framework**: Data controllers and processors are required to document policies enacted and measures taken to demonstrate that processing of personal data is performed in compliance with the GDPR. Such policies should also establish a culture of monitoring by periodically reviewing, assessing and evidencing that their data processing procedures maintain compliance with the main tenets of the GDPR: Minimise data processing, adequately and proportionately retain data, and build in appropriate safeguards.

  Key consideration: *One of these policies should be a data classification policy that implements a systematic way for an organisation to identify personal data and documents where it is being processed or stored so the organisation can formulate and enact procedures to protect that data. Another key process which forms part of the framework is a risk assessment process that includes both business impact analysis and risk appetite setting activities. Data privacy awareness training should also be part of this framework to ensure staff are trained to understand their obligations.*

- **Be better prepared for reporting data breaches**: One new obligation is for data controllers to notify personal data breaches (those likely to result in a high risk to the rights and freedoms of the data subjects) to their local data protection authority (DPA). This must be done without undue delay and, where feasible, within 72 hours of awareness. Additional processes for incident handing and breach reporting may be required to meet these requirements.

  Key consideration: *Review current disclosure processes to ensure they comply with the GDPR. Ensure that appropriate processes and procedures are in place to detect, respond and recover quickly from incidents within the timeframe permitted. Educating executive and technical teams on incident response and reporting procedures will be critical. Moreover, preparing responses well in advance of a crisis occurring is also advisable.*

- **Evaluate the legitimacy of international data transfers:** Binding corporate rules (BCRs) and standard contractual clauses remain valid tools for transferring personal data outside the European Union within a multinational company. However, these are not sufficient to transfer data to third parties outside the European Union.

  The GDPR does not replace the legacy Safe Harbour agreement, and therefore the rules for data transfers to third parties outside the European Union remain ambiguous whilst the European Union and the United States finalise the Privacy Shield. Those hoping for a revamp in this area, after Safe Harbour, will be disappointed. An organisation must ensure it has legitimate basis, described in Article 46, for transferring personal data to jurisdictions that are not recognized as having adequate data protection regulation. If the organisation plans to engage in intragroup international data transfers, it will need to comply with the BCRs, set out in Article 46.i of the GDPR.

  Key consideration: *Because uncertainty still exists regarding the handling of data transfers to the United States, organisations should closely monitor activities with regard to Privacy Shield or other Safe Harbour agreements as they move closer. With interfirm transfer requirements, organisations can consider the use of BCRs; however, these are not straightforward and will require legal consultation. Consideration of options to re-locate data held by third parties back into Europe should also be made. Furthermore, strategic choices of future data centres and cloud service providers should be considered to reduce the uncertainty risk and complexity associated with data transfers outside the European Union.*

- **Implement processes supporting the new rights of data subjects:** Under the GDPR, data subjects are given rights such as the right to data portability and the right to be forgotten, and they may choose to exercise them.

  Key consideration: *Organisations may need to develop additional policies and processes to respect the new rights of EU citizens. These plans may not be straightforward as organisations may not have processes and technology in place to deal with these requests. Furthermore, rules on record retention and requirements for referential integrity may also complicate the ability for companies to adhere to this requirement. Organisations therefore need to be aware and prepare well in advance for key changes required for process and technology to make them effective to meet the GDPR requirements.*

- **Organisations may need to re-establish consent:** Data subjects must give clear and affirmative consent to the processing of their personal data. This can consist of ticking a box when visiting a website or taking another action or making a statement clearly indicating acceptance of the proposed activity. However, according to the GDPR, silence or inactivity, or pre-checked boxes, will not suffice as consent, which needs to be obtained separately from standard terms and conditions and cannot be conditional on using the service being offered.

  Key consideration: *Organisations need to carry out an exercise to establish whether the consent received from EU citizens has historically complied with the GDPR requirements. Those who currently hold or have appropriated personal data not in line with the GDPR will need to obtain that consent from data subjects before continuing to use their personal data. This exercise may not always be straightforward and will require sufficient planning to execute effectively and ensure data they hold on EU citizens is compliant with GDPR requirements*

- **Review current contracts:** Data processors will have direct responsibilities to regulators and data subjects to report data breaches. Previously, data controllers were primarily responsible for this. Increased responsibility and liability implications will affect contractual arrangements for

those sharing personal data. Also, previously, data controllers were in control about how and when to report breaches to the regulator. This procedure will now change.

Because of the changes in responsibility for breach notification, contracts between parties involving data protection will need to be reviewed to ensure that appropriate measures are put in place. Data processors and data controllers will also need to undertake further care regarding third-party contracts to ensure no undue exposure, specifically concerning liability to third parties and additional reporting responsibilities.

Key consideration: *Organisations should review their contracts with third parties and ensure they understand their roles and responsibilities in relation to the GDPR. Where existing policies and practices fall short of the GDPR requirements, additional remediation may be required to manage their data privacy risk*

In Closing

Many organisational leaders are not aware of the GDPR, and those who are do not feel they are ready to fully comply with its specifications. Because the penalty stakes are becoming more material, some of the requirements will have major implications on how organisations store and process personal information. Many of these organisations must make significant changes to business processes and underlying technology in order to support the rights of EU data subjects in the future.

Moreover, those throughout the supply chain of personal data must take greater care when acquiring, sharing and using personal information, ensuring that suitable business contracts are in place to manage the new expectations arising and accountabilities that follow from noncompliance.

Organisations should start preparations for compliance immediately so that any obstacles encountered can be resolved before the GDPR becomes effective on 26 May 2018. The scope of the new regulations is relatively broad, encompassing all companies both within and outside Europe – whether they are data controllers or data processors – that utilize personal data of EU residents. Using these recommendations as a blueprint to prepare for the new regulations can give your organisation a head start on reviewing its practices and analysing where changes may be required for its data protection programme to come closer to compliance.

.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

France
Bernard Drui
+33.14.296.4111
bernard.drui@protiviti.fr

United Kingdom
Andrew Clinton
+44.207.024.7570
andrew.clinton@protiviti.co.uk

Ryan Rubin
+44.207.389.0436
ryan.rubin@protiviti.co.uk

Jonathan Wyatt
+44.207.024.7522
jonathan.wyatt@protiviti.co.uk

Italy
Alberto Carnevale
+39.02.6550.6302
alberto.carnevale@protiviti.it

Hernan Gabrieli
+39.02.6550.6301
hernan.gabrieli@protiviti.it

Giacomo Galli
+39.02.6550.6303
giacomo.galli@protiviti.it

Germany
Michael Klinger
+49.69.963.768.100
michael.klinger@protiviti.de

Kai-Uwe Ruhse
+49.69.963.768.100
kaiuwe.ruhse@protiviti.de

The Netherlands
Anneke Wieling
+02.03.460.405
anneke.wieling@protiviti.nl

United States
Cal Slemp
+1.203.905.2926
cal.slemp@protiviti.com

protiviti®
Risk & Business Consulting.
Internal Audit.