In an uncertain world, one thing international organizations can be sure about is the need to mark 25 May 2018 in their calendars. Why? Because on that date, the new General Data Protection Regulation will come into effect. This will impact every organization in the world that collects or retains personal identifiable data from any European individual.

Four years in the making, this European data protection initiative aims to harmonize the fragmented data privacy framework across the European Economic Area (EEA), and ensure that fundamental rights are protected in today’s digital economy. Legislators believed that an increase in legal certainty would both reduce compliance costs and encourage long-term consumer confidence in the safety of the global digital marketplace. This is why GDPR’s jurisdiction cannot be limited to the EU and requires extraterritoriality to be addressed.

Formalizing the global reach of European data privacy regulations should come as no surprise to international businesses. Establishing a consistent level digital playing field for organizations inside and outside the EU by expanding the territorial scope of legislation was a widely-publicized GDPR objective.

In our experience, many organizations that are located outside Europe but have a global employee and customer base, remain behind the curve in assessing the risks and opportunities of GDPR. They do not have clear visibility, understanding and control over the personal data they process, nor appropriate access to its movement across multiple geographical locations. This lack of engagement could be a risky strategy. With massive fines and requirements for notification that will push more breaches into the public eye, GDPR promises to make data privacy a potential public relations challenge.

This paper aims to highlight the areas of GDPR that international businesses need to consider, and the practical steps they can take to ensure that they are ready for the 2018 deadline.

Understanding what’s new in GDPR

So, what will change under GDPR?

What’s new in GDPR at a glance:

<table>
<thead>
<tr>
<th>Applies to data processors not just data controllers</th>
<th>Data processors can be held directly liable if the company is found responsible for a breach. This was limited to data controllers under the EU Directive.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records of processing activities</td>
<td>Data controllers must maintain records of their processing activities.</td>
</tr>
<tr>
<td>Accountability</td>
<td>Organizations must demonstrate how they comply with GDPR and document what personal identifiable data they have and why.</td>
</tr>
<tr>
<td>Data Protection Impact Assessments</td>
<td>These must be carried out to consider an individual’s privacy when an organization is creating or updating a product or service that includes processing likely to result in a high risk to the rights and freedoms of data subjects.</td>
</tr>
<tr>
<td>Higher standards of consent</td>
<td>Consent by a data subject must be freely given and based on clear, easily available information about what they are agreeing to. It must be as easy to withdraw consent as it is to give it.</td>
</tr>
<tr>
<td>Enhanced rights for individuals (data subjects resident and/or citizens in the EU)</td>
<td>Individuals have the right to be informed, object to processing and be forgotten (through erasure) – as well as rights regarding access, rectification, restrictions on processing, data portability and automated decision making.</td>
</tr>
<tr>
<td>Data Protection Officer (DPO)</td>
<td>A DPO is not mandatory for all organizations but a senior individual must be made responsible for GDPR compliance.</td>
</tr>
<tr>
<td>Breach Notification</td>
<td>Organizations have a duty to report a breach of personal data within 72 hours and failure to do so may result in a fine.</td>
</tr>
<tr>
<td>Level of fines</td>
<td>GDPR sees a significant increase in fines – up to 4% of global annual turnover.</td>
</tr>
</tbody>
</table>

1. Processor – ‘means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller’ (Article 4 EU GDPR Definitions)

2. Controller – ‘means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data’ (Article 4 EU GDPR Definitions)
GDPR: a framework for a digital world

In seeking to transform data protection culture as well as practice, GDPR has bold ambitions. It encourages organizations to make privacy and data protection core business values, instead of a casual afterthought. The GDPR follows the line of previous EU data protection legislation, requiring organizations to carefully assess and implement appropriate technical and organizational measures and processes to make sure that any data processing consistently protects the rights of the data subjects. By placing the principle of ‘data protection by design and default’ at its heart, GDPR requires organizations to only process the personal data necessary for the specific purpose for which it was collected, and to implement controls to protect that data throughout the process lifecycle. And what counts as personal data? GDPR defines this as “any information relating to an identified or identifiable natural person.” This may include data such as physical address, email address, IP addresses, age, gender, location, health information, search queries, items purchased, cookies and RFID tags for any EU citizen.

This comprehensive definition may bring many more international organizations that interact with EU citizens within the reach of EU regulators.

As well as trying to investigate how the directive applies to their businesses, many of the organizations that we talk to are using GDPR as an opportunity to review and fully understand the personal data that they retain. Many wish to find practical ways to minimize data to reduce risk. Organizations are also actively revising processes for data storage and – perhaps most challengingly – how access to personal data is controlled and restricted. It is widely acknowledged that identity and access management is just one of the critical technology pillars for GDPR compliance that remains a challenge.

“Compliance can be viewed as an expense, but without GDPR, compliance organizations could find themselves too expensive to do business with.”
Dominic Newton, DPO, NTT Security

However, as we embrace the commercial opportunities of the digital world, should we allow GDPR to be a constraint? Or will consumer demand for new and innovative global services not be matched by an expectation that their personal information is protected? GDPR may be a milestone, but global security professionals have been on a journey to protect data and privacy for many years. Not only does much of the directive build on existing EU legislation, it also aligns with the direction of travel of other jurisdictions. While differences exist between countries in their approach and the level of legislative development, there are signs of upward convergence towards important data protection principles in particular in certain regions of the world.4

**Australia**

The Australian government recognizes the similarities between GDPR and the Australian Privacy Act 1988. Both sets of regulation focus on fostering transparent information handling practices and business accountability, to give individuals confidence that their privacy is being protected. Both data protection regulations require businesses to implement measures to ensure compliance with a set of privacy principles, and take a ‘privacy by design’ approach to compliance. In addition, data breach notification and privacy impact assessments, mandated in certain circumstances under the GDPR, are expected in similar circumstances in Australia. But the advice recognizes that GDPR will require some additional steps, suggesting that complying with GDPR could improve consumer trust through enhanced privacy practices, allowing for more consistent internal privacy procedures and systems across the business.5

**South Africa**

South Africa’s 2013 Protection of Personal Information Act (PoPI) shares many similarities with GDPR. In our experience, companies that have embraced PoPI will benefit significantly in terms of their journey to GDPR compliance. But a note of difference is the level of non-compliance penalties, which are significantly lower under PoPI than GDPR. South African companies that have not invested in PoPI but wish to trade with the EU and process personal data face an uphill journey ahead of May 2018.

**United States**

In a recent PwC survey of over 200 US executives, 92 percent of the respondents cited compliance with GDPR as a top priority on their data privacy and security agenda in 2017. So where are the US and EU in terms of harmonizing data protection? After significant negotiation between the European Commission and the US Government, the EU-US Privacy Shield was adopted in July 2016. This new framework for transatlantic exchanges of personal data for commercial purposes was necessary after the previous Safe Harbor framework was ruled invalid by the European Court of Justice. The US robustly regulates data protection through a variety of laws and rigorous enforcement, but with the ink hardly dry on this latest attempt to provide ‘adequate’ data protections, some commentators anticipate that perceived gaps by EU Working Parties in Privacy Shield may still be challenged by the European Courts. Whether Privacy Shield will be enough to meet GDPR compliance is still uncertain, and we anticipate more clarity after the annual joint review process.

---

5. www.oaic.gov.au

---

“In my experience, a CISO’s responsibility is to always do the right thing, maintaining a sound data protection framework, and implementing controls and processes that keep the data entrusted to us secure. As an international organization, we have been planning and incorporating GDPR requirements into our business for some time – in order to react to the changing landscape, minimize risks and keep our board informed regarding potential impact and opportunities for business.”
John Petrie, CISO, NTT Security

www.nttsecurity.com
Japan

Japan has recently made significant enhancements to the Act on the Protection of Personal Information (APPI), and established a new Personal Information Protection Commission (PPC). As with GDPR, APPI has a comprehensive definition of personal information or 'special care-required personal information'. Regulators are advising organizations on the value of finding ways to anonymize or pseudonymize data so that it can still be used effectively for big data analytics without a connection to an individual. And, as with the GDPR principle of accountability, the amended APPI requires a business to keep records of how, or from whom, it obtained personal information and to whom it transferred this data. Japan is one of the countries that the European Commission has prioritized for possible adequacy discussions, as its decision recognizes that the country’s system approximates that of the EU Member States.

European Economic Area countries

The rules relating to data exports to non-EU/EEA countries, such as Norway, will not change significantly because they were already fully harmonised under the old framework. Data exports will continue to be allowed where the European Commission has established that the level of data protection in the destination country is adequate (Article 45). As a non-EEA state, understanding the importance of demonstrating adequate levels of data protection for GDPR compliance, the Swiss Federal Council initiated a revision of its Data Protection Act, which is expected will be influenced and enacted in the same timeframe as GDPR.

This variety of global data protection initiatives, some driven by GDPR and some not, is one of the reasons that organizations seek to work with data protection advisors with international knowledge and up to date, relevant experience of these frameworks. As well as compliance, other geo-political factors are also a consideration. Data protection is an international moving target for businesses in an internet age. Whether this is considering the impact on GDPR of the Brexit vote in the UK, or that of President Trump’s executive order repealing the online privacy protections established during the previous administration, it is important to seek help from compliance advisory experts who are always available to support clients as they plan and execute their data protection strategy.

Don’t forget the PR in GDPR

For GDPR, or indeed any compliance to be effective, failure must carry a reputational risk. Organizations that think this is just an IT issue have missed the fundamental necessity for every department within the business to think hard about data privacy. Sales, Marketing, HR, Finance: all process data and therefore may introduce risk. The new requirements for data breach reporting within 72 hours will be a challenge for many organizations – not just in how and what to report to the regulators, but in actually having the right systems in place to assess and analyze a breach. Not forgetting that the regulators could come knocking at any time to ensure that adequate protections are in place and a failure to satisfy them may result in a fine, even if an organization has not suffered a breach.

Publicly naming global companies that fail to meet GDPR requirements or suffer a breach will make consumers increasingly aware of risks to their personal data. The risk for organizations is one of trust: if a company is discovered to be at fault in maintaining its customers’ or employees’ privacy, questions may be asked about its capabilities elsewhere.

The principle of accountability within the regulation requires clear lines of responsibility and reporting. The GDPR therefore mandates the appointment of a data protection officer (DPO) for certain types of businesses – either because they are ‘public’ organizations, or because their activities include regular and systematic monitoring of data on a large scale. This is just one example of where GDPR is far from crystal clear on expectations and, as with all compliance, organizations will need to keep re-examining the regulation’s exact requirements.

The GDPR’s potential punitive commercial and reputational impact are inextricably linked, encouraging a board conversation around how privacy and trust are no longer mere compliance requirements. Instead, they hold a competitive advantage that can not only protect existing revenue, but also generate new and stronger business opportunities.

What is required of a DPO of an international company under GDPR?

- A DPO must be properly involved – this is not just a rubber-stamping role. DPOs must be consulted and kept informed of every aspect of the organization’s current and future activities relating to data privacy. That’s a very wide and somewhat ambiguous brief that includes drafting policy, advising how to handle direct marketing, defining what to do with requests from individuals, and of course, how to communicate with the regulators.

- A DPO must have “expert knowledge of data protection law”.

This doesn’t mean that they have to be an expert in IT and security systems, but they will need a legal and practical understanding of how the law protects privacy.

- The DPO can be an existing member of legal, administrative, governance or IT staff and it does not necessarily have to be their only role, but they will have to maintain their independence. They can also perform the role across subsidiaries for larger organizations.

- Organizations can outsource the role of DPO with the understanding that the consultant has full and unfettered access to the organization’s data. This will of course require specific contractual confidentiality and checks on the credentials and certifications of the individual or company.

- Whether a new appointment, existing team member or external consultant, the DPO must have clout within the organization. They should report to the highest level of management – the board, or the trustees – and organizations are legally obliged to give them support, training and resources.

- Once an organization has appointed a DPO, their details must be published and notified to the local regulators in the countries in which they are doing business.

- A DPO should have a degree of independence from their employer. Although the full extent of their responsibility remains unclear, the GDPR states that DPOs “shall not be dismissed or penalized... for performing his [or her] tasks” and should not “receive any instructions” on how to carry them out.

Data security specialists should have clear lines of communication with their DPO, who may or may not have knowledge of security processes or technology. And as with cyber resources, people with the right skills, knowledge and practical application of international data compliance will be few and far between. These professionals will need to join their security colleagues in the battle to build awareness of data privacy at all levels of the organization and ensure that executives and other influential stakeholders are kept informed about the progress towards GDPR compliance.

Organizations are at varying stages of readiness for GDPR – from identifying and clarifying the exact requirements and effect of GDPR to reviewing the adequacy of their existing program or seeking to create audited evidence of implemented controls and compliance with GDPR (see Figure 1). Wherever you are on your journey, this will require security and DPO executives to work together on assessing their GDPR readiness:

**Where are you on your journey to GDPR?**
Protecting and exchanging personal data are not mutually exclusive. A strong data protection system facilitates data flows by building consumer confidence in companies that care about the way they handle their customers’ personal data. In our experience, organizations across the globe are at very different stages in their preparations for GDPR. But whatever stage they are at, it is clear that international businesses wishing to operate in the global digital market must think about the impact of GDPR in order to seize its commercial opportunities, as well as mitigate risk. Over the coming months there will be much debate about the application of the regulation and the interpretation of its detail – particularly a Supervisory Authority’s ability to apply large financial penalties beyond its borders and the aggressive 72-hour reporting requirements. But as we have said, GDPR is just another milestone on the continuous road of privacy compliance, as in the race for increasingly innovative technologies that strive to make human life more efficient or fun. Consequently, businesses cannot afford to let GDPR constrain their digital aspirations. If the road gets bumpy, organizations may want to consider qualified external partners ready to help them navigate the long compliance journey ahead.

![NTT Security's GDPR Readiness Model](image)

---

**About NTT Security**
NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients’ digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit [www.nttsecurity.com](http://www.nttsecurity.com) to learn more.

---