GDPR Series

US multinationals should develop an EU privacy regulator affairs strategy: 3 questions to consider

Two requirements of the European Union's (EU) General Data Protection Regulation (GDPR)—**data-breach notification and data-protection impact assessments (DPIAs)**—will boost corporations' contact with EU data-protection authorities (DPAs). This contact can elevate the chances of triggering a DPA to investigate a company's privacy practices after the GDPR takes effect in May 2018. To manage this risk, multinationals should consider developing a game plan that defines their relationship, approach, and communication plan with DPAs that have jurisdiction over their major European operations. To begin that process, there are three key questions to consider.

pwc

1) How will these GDPR requirements work in practice?

1. ***Mandatory data-breach notification (GDPR Article 33):*** If a data controller determines that a compromise of EU personal data poses a risk to the rights and freedoms of individuals, the company must notify the "lead" DPA—generally where its European operations are established—within 72 hours. The lead DPA will determine whether to further investigate and involve other EU DPAs. When a data breach poses a "high" risk to individuals, data controllers must notify affected individuals. Data processors, for their part, must notify "without undue delay" the data controllers on whose behalf they process EU personal data of breaches that could pose any risk to individuals.

2. ***Mandatory DPIAs (GDPR Article 35)***: Whenever a data controller uses new technologies to process EU personal data that pose a "high risk" to the rights and freedoms of individuals, the company must prepare a detailed assessment of the impact of processing such data, including a systematic description of the operations, whether processing is necessary and proportionate, and any mitigating factors. The company must submit the completed high-risk DPIA to its lead DPA. In reviewing these DPIAs, it will be the prerogative of the DPA to further investigate the proposed initiatives.

2) How will these reporting requirements pose risks to multinationals?

Europe's enforcement of the GDPR is uncharted territory, which makes risk determination especially difficult. Three factors point toward a mixed-risk picture for multinationals:

- ***Increased regulator fining capacity:*** The GDPR provides for DPAs to impose a fine on companies of up to 4% of annual global revenues for egregious violations of the GDPR. Member states can also add to these fines. The Netherlands, for instance, has more than doubled its own fining capacity to 10% of annual revenues. European privacy advocates are pressuring DPAs to fully exercise these new powers after May 2018.
- ***Prioritized guidance from the regulators:*** The Article 29 Working Party has issued guidance further defining several parts of the law. The guidance has indicated that data-breach notification and DPIAs will be two of the first topics on which it will take action. This prioritization suggests the high importance the DPAs place on these capabilities, and may also signal that they expect companies to be fully equipped with these capacities by May 2018.
- ***Constrained resources:*** DPAs have openly discussed concerns that their current staff levels are not sufficient to administer new GDPR obligations. If DPAs receive steady streams of data-breach notifications and DPIAs in the summer of 2018, they may lack the capacity to launch follow-up investigations or even perform proactive enforcement sweeps.

Three initiatives that should be added to your 2017 GDPR transformation agenda

1. Develop an EU DPA relationship plan
2. Inventory and define high-risk processing activities
3. Build notification and DPIA capabilities

3) How should US multinationals manage these risks?

Here are three initiatives businesses should add to their 2017 GDPR transformation agenda:

1. ***Assess relevant DPA relationships.*** Chief privacy officers (CPOs) should use the window before GDPR's go-live date of May 2018 to develop a DPA engagement strategy. The plan should identify relevant DPAs based on the company's data-processing footprint in Europe, prioritizing member states where their companies undertake high-risk processing. For prioritized countries, CPOs should determine how their DPAs prefer to interact with and gain an understanding of multinationals in their jurisdictions. Some, for example, prefer direct personal contact, while others prefer indirect exposure at events, while others insist on arms-length, formal communication. Establishing the level of exposure and interaction with DPAs may greatly aid companies in the event of a data-breach notification or controversial DPIA.
2. ***Define and inventory high-risk processing activities.*** The GDPR's Article 30 requires companies to inventory their data-processing activities. Once complete, businesses should establish criteria to rank these activities into low, medium, and high tiers of risk to the "rights and freedoms" of EU individuals. These risk determinations are critical to data-breach notification and DPIA requirements.
3. ***Build data-breach notification and DPIA capabilities.*** Many U.S. companies have a head start in developing the people, processes, and technologies needed to execute timely data-breach notification and thorough DPIAs. Even those with an initial advantage, however, face a more significant task in modifying their procedures to address unique EU requirements, training personnel, and testing the repeatability of their controls.

The GDPR contains at least 20 requirements that will be further defined by the various EU stakeholders over the next few months. Multinationals can get ahead by accelerating work on data-breach notification and DPIA capabilities and by keeping an eye on additional clarity provided by the EU. Businesses that implement and test these controls by May 2018 stand a better chance of avoiding the largest fines.

How PwC can help

For a deeper discussion about preparing for the GDPR, contact:

Jay Cline

Principal, Data Privacy Practice Leader
jay.cline@pwc.com

Jocelyn Aqua

Principal, Data Privacy Risk & Regulatory Practice
jocelyn.aqua@pwc.com