An action plan for tackling third-party GDPR risk
An action plan for tackling third-party GDPR risk

The European Union’s General Data Protection Regulation (GDPR) has significantly increased the risk of outsourcing data-processing activities of business operations involving European individuals.

The GDPR expands the breadth and depth of third-party risk for large multinationals, which often engage thousands of vendors that perform some type of processing of EU personal data. These companies need an action plan and ongoing capability to mitigate the GDPR enforcement and litigation risk of their supply chain.

**Broader and deeper vendor GDPR risk**

Five articles in the GDPR add new requirements or deepen existing obligations from the legacy 1995 EU Directive on Data Protection:

- **Article 28, “Processor,”** requires contractual protections with data processors and their sub-processors, adequate data protection, and production of evidence of compliance with the GDPR;

- **Article 30, “Records of processing activities,”** requires data processors to maintain a detailed inventory of the EU personal data they host;

- **Article 32, “Security of processing,”** requires data processors and their sub-processors to implement comprehensive information security controls to protect EU personal data;

- **Article 33, “Notification of a personal data breach to the supervisory authority,”** requires data processors to report compromises of EU personal data to their clients without undue delay; and

- **Article 36, “Prior consultation,”** requires data processors to provide data protection impact assessments (DPIAs) to their clients in certain high-risk situations.

Companies which engage third parties to process their EU personal data will also want to contractually establish their service levels for assisting with responses to data subject rights requests under their purview and also to provide GDPR evidence of compliance on demand.
**Enhancing existing third-party risk-management programs to address GDPR**

Most multinationals already operate a third-party risk-management (TPRM) program to address their vendors’ information security risks. These programs often involve maintaining an inventory of third parties and the type of data they process; requiring vendors to adopt standard contractual clauses addressing information security; and vetting vendor responses to security due diligence questionnaires. A growing number also include on-site security reviews or audits in their programs.

To address GDPR vendor requirements, companies doing business in Europe should consider launching an action plan that enhances their existing TPRM program with the following components:

- Adding several columns of GDPR-related metadata to their vendor data inventory
- Adding new GDPR-related criteria to the vendor risk-ranking formulas
- Adding privacy-related requirements to the standard contractual clauses and rolling those addendums out to impacted third parties
- Adding privacy-related requirements to due diligence questionnaires
- Adding privacy controls to onsite audits
- Enhancing the frequency and rigor of ongoing vendor monitoring to detect changes in the scope of vendors’ data processing and facilitate reporting of DPIAs and suspected compromises of EU personal data

**Expanding the scope of data protection due diligence**

After reviewing GDPR requirements, it seems that the EU expects organizations to conduct a greater level of due diligence on their third-party relationships. Organizations must understand the nature, scope, context, scale and purposes of processing as it relates to services performed by third-parties in order to establish an appropriate level of oversight. One solution is to leverage a modified due diligence assessment which incorporates requirements from DPIAs. This assessment not only supports the EU’s objective of more stringent oversight for third-parties that handling data subject’s information, but is also helps identify processes that may result in a high risk to the rights and freedoms of natural persons, as defined by GDPR’s Article 35:

> “Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.”

In collaboration with its Data Privacy Officer (DPO) or appointed privacy leader, a firm should consider expanding its due diligence assessments to contain at a minimum the following: (1) a systematic description of the envisioned processing operations; (2) the purposes of the processing; (3) as applicable, the legitimate interest pursued by the controller; (4) an assessment of the business necessity need to perform the services; (5) an assessment of the risks to the rights and freedoms of the data subjects; (6) the measures envisioned to address the risks including safeguards and security measures; and (7) mechanisms to ensure the protection of personal data and to demonstrate compliance.

Under GDPR, all third parties (processors) handling data jointly (i.e., joint-controllers) or on behalf of another firm (i.e., controller) will be required to meet new requirements. If these requirements are not met, the controller and or the contracted third parties will be
held liable, resulting in potential fines, sanctions and brand impact. Therefore, it is important for organizations to update the due diligence process to consider these privacy requirements:

- Third-party breach notifications
- Records of processing
- Roles and responsibilities
- Security controls
- Doing business across borders
- Demonstrating compliance

When should a firm perform the modified due diligence assessment?

It is common practice for organizations to conduct assessments in high-risk situations, but when dealing with personnel data, organizations should consider taking a more strategic approach which considers unconventional processing activities, technologies and scope of services. Although organizations have the ultimate decision as to when due diligence assessments should be performed, it is important to evaluate all third parties that may impact the rights and freedoms of natural persons. Unfortunately, an exhaustive list of processes or activities that would require an assessment does not exist. But GDPR has provided some basic guidance and sample scenarios for consideration. The guidance includes but is not limited to the following:

- A third party is, or will be, performing a high-risk process or services which may impact the rights and freedoms of natural persons
- A third party is, or will be, systematically monitoring a large scale publically accessible area
- As referenced in Article 9(1), any third-party processing special categories of data on a large scale and/or personal data containing criminal convictions or offense
- A third party is, or will be, evaluating personal aspects relating to natural persons based on automatic processing, including profiling, and on which decisions are based that produce legal effects concerning the natural persons

Additional processing activities and businesses to consider:

- Consumer facing activities
- Activities relating to children
- Marketing and advertising
- Digital transformation
- Geolocation
- Profiling
- Tracking
- Public services
- Mass communications
- Joint ventures
- Global business operations
Time to update those contracts

Organizations now have a legal obligation to establish contractual agreements between controllers and processors which clearly define the roles, responsibilities and liabilities of both parties. The goal of each contract at a minimum should include:

- The subject-matter and duration of processing
- The nature and purpose of processing
- The type of personal data and categories of data subjects
- The minimum terms or clauses required of the processor
- The obligations and rights of the controller

This new requirement ensures that organizations not only comply with GDPR requirements, but it also ensures that controllers and processors provide appropriate protection over data subjects and their personal data.

Continue to improve ongoing monitoring

The harsh reality under GDPR is that organizations and their third parties are under more scrutiny to monitor and maintain compliance as referenced in Articles 28, 31, 32(d) and 39. Not only will third parties need to cooperate with the supervisory authority, but they will be expected to establish methods for determining the effectiveness of technical and organization measures. Such methods may include risk assessments, high-risk processes, the type of data and how it’s being processed and the number of active processors.

Termination of third-party relationships

Although GDPR doesn’t provide specific requirements around terminating a third-party relationship, organizations should still plan accordingly for this situation. One option is for organizations to develop a plan for bringing a service in-house or alternatively, finding a replacement third-party provider. No matter which option is chosen, each plan may vary based on each third party or the type of services being provided, and may include, but not be limited, to the following factors: (1) transition timelines, (2) technology and security requirements, (3) data retention and destruction activities (4) legal and regulatory requirements, (5) capability and resourcing needs, (6) impacts to services or business functions and or (7) strategic risks.

In conclusion

Implementation of GDPR will be time-consuming and complex, and will likely cause disruptions throughout the business unless organizations can adopt new strategies to manage the regulatory requirements internally and against contracted third-parties. The most successful organizations may be those which incorporate risk management practices that meet the new enhanced regulations — in a way that allows the organization to also meet defined business initiatives and objectives.
To discuss further, please contact:

T.R. Kane  
Global Third Party Risk Leader  
+1 (440) 390 8502  
t.kane@pwc.com

Jay Cline  
US Privacy Leader  
+1 (763) 498 2237  
jay.cline@pwc.com

Contributors:  
Justin Hall, Andrew Namoury, Nikhil Sarnot, Nehal Sheth, Michael Spadea and Dean Spitzer

pwc.com/us/gdpr