protiviti®

A COMPANION DOCUMENT TO THE GDPR READINESS DECISION TREE – QUESTIONS AND ANALYSIS

April 19, 2017

The General Data Protection Regulation (GDPR) represents perhaps the most sweeping changes to the protection of personal data in the last two decades. The 88 pages of the Regulation's text addresses a litany of operational areas, including mandates for demonstrating a legitimate basis for "processing" personal data, data security, and tightly delineating what can be done with personal data and by whom. With a May 25, 2018 deadline looming and potential fines of €20M or 4% of a company's annual global revenue for violations, the importance of an effective data protection program has never been greater. Robert Half Legal and Protiviti can show you the way forward.

Some common misconceptions about the GDPR:

- The Regulation is only applicable to EU-based businesses. The Regulation applies worldwide to all organizations that "process" the personal data of EU residents.
- Privacy Shield and the Regulation are the same. The Regulation addresses nearly all aspects of the protection of personal data, whereas Privacy Shield is a data transfer mechanism, designed to facilitate the transfer of personal data from the EU to the U.S. Even if no personal data were to ever leave the EU, the Regulation would still apply.
- All data is required to be encrypted. Article 32 of the Regulation offers suggestions as to how to protect personal data, including encryption and "pseudonymisation," but does not require a particular method. Ultimately, it's up to the organization to determine what's most appropriate**. As with other aspects of the Regulation, the Article 29 Working Party will eventually provide more guidance.**

The following represents a series of questions that every organization should ask when preparing for GDPR compliance remediation-related efforts; while by no means exhaustive, it serves as an overview of the many interrelated components of a global data protection program.

Questions	Recitals/ Articles	Analysis	How We Can Help
Do you have the necessary support for data protection? ☐ Is there a Data Protection Steering Committee or a related committee that will assume the role of data protection? ☐ Is there an executive sponsor that will be the Committee's advocate?		Without a committee whose function is to promulgate data protection throughout the enterprise and an executive sponsor to act as its advocate, if not champion, data protection projects and programs have a high potential for failure.	We can develop a committee charter, identify which departments and business units require representation, and develop an agenda for (and assist with) the committee kick-off.
Are you, in principle, subject to the GDPR? ☐ Do you "process" the personal data (or special personal data) of an EU data subject? ☐ Do you "monitor the behavior" of EU data subjects?	Rec. 24; Arts. 3, 4	Just about *anything* that can be done to personal data can be considered processing: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. While "monitoring" is likely more than simply tracking where someone clicks on a website, how much more in unknown at this point. As a practical matter, if you are engaging in user analytics, presuming that you are subject to the regulation is a good idea.	By interviewing process and subject matter experts, business owners, IT, and stakeholders, we can determine the scope and depth of the processing taking place within the organization and likely uncover processing that was heretofore unknown.

Questions	Recitals/ Articles	Analysis	How We Can Help
Is there an underlying policy and set of procedures and notices governing the collection, use, sharing, and disposal of personal data?		Privacy policies and privacy notices are two different documents. A policy sets broad standards of conduct with respect to personal data, the violation of which is subject to discipline; a notice conveys specific information to data subjects. Some applicable policies and related procedures and notices include: • Privacy • Acceptable Use • Bring Your Own Device (BYOD) • Data Classification	Development of policies and related documents requires an understanding of not just the Regulation, but other mandates that the organization must follow. Our experience in developing a wide range of policies and related documents across industries gives us the ability to develop the correct document set for a given compliance environment.
Do you have a legitimate basis for each type of processing of personal (or special personal) data?	Arts. 6,9	Consent is typically the worst choice for use with employees; also, consent can always be revoked and if that is the basis for processing, a mechanism needs to be in place to receive and acknowledge revocations.	We can analyze the details of the processing and share what data protection authorities and industry commentators have stated on the subject.
Are you required to employ a Data Protection Officer (DPO)? ☐ Does processing consist of regular and systematic monitoring of data subjects on a large scale? ☐ Does processing consist of processing on a large scale of special categories of data pursuant to Article 9? If not required, who will be primarily responsible for managing data protection and reporting to management?	Arts. 37-39	Even if a DPO is not required, someone should be designated to be responsible for understanding data protection requirements, the organization's data inventory, and data usage. This person will also be responsible for reporting to management.	Currently, there's a debate as to what the qualifications and background of a DPO should be. We believe that it will depend on the unique needs of the organization and as a consequence can develop a job description, complete with recommended skills and qualifications.

Questions	Recitals/ Articles	Analysis	How We Can Help
Have you searched your global enterprise for personal or special personal data and identified: ☐ Where it resides; ☐ Who has access; ☐ Who is the business owner; and ☐ Who is the respective data steward or custodian? Have you determined: ☐ How long the data is retained?	Rec. 30; Art. 4(1)	The process for searching an enterprise for sensitive data is "data discovery." Once discovered, data that is no longer necessary is eliminated; specific controls are applied to the rest, such as user access controls (UAC), encryption, etc.	Data maps are invaluable in succinctly documenting the location of personal data throughout the global information ecosystem. We offer maps in a variety of formats to fit specific needs.
Have all third parties that have access to the data (either co-controllers or processors) been identified? Is it clear: ☐ What data elements (name, national ID number, etc.) each has access to? ☐ What can they legally do with the data? ☐ What they are, in practice, doing with the data?	Art. 28	Interviews with business owners and the cataloging of software applications will assist with finding the underlying contracts with third parties. Typically, several rounds of searching are needed to locate all of them.	Legal and HR teams are often surprised at which third parties have access to personal data and what they are doing with it. We can conduct interviews with appropriate team members and with third parties and uncover all of the needed details.
Have all Notice, Choice, and Consent requirements for each use of personal data been met?	Arts. 7, 9	For employees, consent is typically not a valid means for use of personal data; some other basis, such as the fulfilling of a contract, will be needed. When data is processed by third parties, reviewing Notice, Choice, and Consent requirements with them and documenting compliance is crucial. Special personal data has its own requirements for Notice, Choice, and Consent.	Reviewing contracts for compliance with Notice, Choice, and Consent is not sufficient; in practice, the processing of personal data can vary greatly from what is stated in a contract. We can audit how data flows and its use throughout the organization to promote alignment between policy and practice.

Questions	Recitals/ Articles	Analysis	How We Can Help
Can the organization respond to requests for data subject access and make requested changes or deletions without undue delay?	Arts. 15, 16, 17, 20	This includes the so-called "Right to be Forgotten."	Data subject access requests can be particularly time consuming for organizations that haven't prepared for them well in advance. Our approach is to create an access request response plan that takes into account the information most likely to be requested and the best form for producing it.
Do you have a means to demonstrate the "organizational and technical [security] measures" you have applied to the personal data?	Art. 32	Components can include: • Encryption or pseudonymisation • Protecting the confidentiality, integrity, availability and resilience of processing systems and service • The ability to restore access to personal data after an outage • A process for regularly testing the effectiveness of these measures	Requirements for written information security plans are not uncommon in the U.S.; we can leverage our experience in developing them in order to assist in demonstrating the effectiveness of your security program. If your organization has any third-party information security certifications such as ISO/IEC 27001, we can leverage them as part of our efforts.
Are there transfers of personal data outside of the EU? ☐ Are they to a country that provides "adequate" protection? ☐ If not, for every use of personal data that is transferred outside of the EU, is there a transfer mechanism, such as Privacy Shield (U.S.), Standard Contracts, and/or Binding Corporate Rules?	Arts. 35-39	A list of "adequate" countries can be found here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm	Data transfer mechanisms, when drafted correctly, can alleviate the need to amend agreements individually. We can flag which contract terms are the best candidates and forward to an organization's counsel.
Does the organization have a breach notification plan that enables it to notify supervisory authorities within 72 hours of a suspected breach? Can it provide meaningful details?	Arts. 33, 34	While the Regulation offers few specifics beyond the 72-hour rule (or the "without undue delay" rule for processors), the U.S. National Institute on Standards and Technology (NIST) Special Publication 800-61 offers valuable guidance that can be readily adopted by the commercial sector.	The 72-hour time limit can prove especially challenging for organizations not involved in highly-regulated operations, such as healthcare or telecommunications. We can prepare a plan that addresses all aspects of breach notification, as a stand-alone document or as part of a larger incident response plan.

Questions	Recitals/ Articles	Analysis	How We Can Help
Is a Data Protection Impact Assessment (DPIA) necessary? Is there: ☐ A new technology that is likely to pose a high privacy risk to data subjects? ☐ Automatic processing plus a legal effect on the data subject? ☐ Large-scale processing of special personal data? ☐ Systematic, large-scale monitoring of a public area?	Art. 35	As with breach notification, the Regulation offers few specifics on DPIAs; NIST guidelines (such as SP 800-122) are very helpful.	With deep experience in assessments and audits of all types, we can conduct a DPIA that gives you visibility into the most likely trouble spots as well as ways to mitigate them.
Are third parties being held to the same standards as the data controller for: ☐ Notice, Choice, and Consent? ☐ Information security? ☐ Cross-border data transfers? ☐ Breach notification?	Art. 28	Unlike under the Data Protection Directive, third party co-controllers and processors are held to effectively the same standard as data controllers and are directly subject to regulation by supervisory authorities.	Your third parties often represent the biggest data protection risks. Moreover, many of them offer little stated assurances as to how they protect personal data, and it's not clear how they will respond in a breach or to a legal demand for documents. We can address these concerns with a discussion with third parties, informed by foundational work we have already completed for you.

.

Face the Future with Confidence

protiviti®