tenable™

Thirteen Essential Steps to Meeting the Security Challenges of the New EU General Data Protection Regulation

September 13, 2017

Table of Contents

Once in force, the European Union General Data Protection Regulation (GDPR) will require every multinational company that offers products or services to European Union residents to adhere to a strict set of data privacy and security measures. These requirements will apply equally to those companies' business partners and call for the use of emerging technologies and for systems design concepts that will likely be new to U.S. information security professionals. However, those professionals can leverage much of their existing capabilities, along with the addition of a few key components, to meet these new requirements and enable compliance with the Regulation in all 28 EU member states.

Organization of this Document

IT leaders in many multinational companies have recognized the need to begin the process of making changes to their information infrastructure in order to meet the many requirements of the Regulation. This document was envisioned to assist information security professionals in prioritizing changes and additions to their information security programs. Those familiar with current EU protection regimes can skip directly to the Thirteen Essential Steps section; those not familiar will likely want to read the entire document through in order to see the context in which the Regulation was promulgated. The Appendices offer an in-depth look at key concepts of the Regulation and a comparison of the Regulation with the existing regime, the Data Protection Directive 95/46/EC.

What is the General Data Protection Regulation?

On May 4, 2016, the official text of the General Data Protection Regulation (the "Regulation") was published in the Official Journal of the European Union, capping a four-year process to replace the European Union's principle data privacy and security regime, the Data Protection Directive 95/46/EC (the "Directive").[1] The Directive, enacted by the European Parliament and the Council of the European Union in 1995 and primarily applicable to organizations located in the EU, set a high bar for the protection of personal data but proved inadequate to resolve challenges posed by changing technology. A fundamental limitation of the Directive was that it didn't require individual EU member states to pass one standard text into law. Instead, it listed a set of data privacy principles and directed those states to pass legislation based on them, leading to a unique version in every state. As a result, implementation varied by state and enforcement often lacked real teeth. Conversely, the Regulation is binding on all EU members as enacted and, at 88 pages, was designed to address the disruption to data privacy wrought by the rapid evolution of information technology and business models over the past 20 years. In May of 2018, the Regulation will be enforceable by the data protection authorities (called "supervisory authorities" by the Regulation) of member states.

While multinational companies can likely meet some of the law's requirements right now, most will find that they need all of those two years in order to be completely ready for enforcement.

Why is the Regulation Important to Information Security Professionals?

a. **The penalties for violations are much more severe.** The penalties for the violation of existing privacy regulations in EU vary among member states, with the potential for fines in the €150-900k range. In a number of matters involving privacy violations, supervisory authorities had little recourse against large, well-funded multinationals who could view such fines as merely a cost of doing business. Under Article 83(5) of the Regulation, however, those authorities can impose fines of up to €20M or 4% of the offending company's global annual revenue, whichever is higher. In anticipation of such regulatory power, legislative bodies in France are discussing increasing the maximum fines that can be levied by France's supervisory authority, the CNIL, to match those under the Regulation now, rather than wait for May of 2018.

b. **The definition of "personal data" has expanded.** In the U.S., definitions of personally identifiable information (PII) vary among jurisdictions and, at the federal level, among agencies. The National Institute for Standards and Technology (NIST), for example, is relatively prescriptive in its definition of PII:

> Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[2]

The Regulation defines personal data in a similar but expanded way by including a person's "identity" in other contexts:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.] [emphasis added][3]

These additions to the definition of personal data are important to information security professionals because they implicate data that may not seem, at first glance, to qualify as personal. IP addresses, application User IDs, Global Positioning System (GPS) data, cookies, media access control (MAC) addresses, unique mobile device identifiers (UDID), and International Mobile Equipment IDs (IMEI) are some examples. As a consequence, companies and third parties that "process" this data will have to do so with a legal basis that is listed in the Regulation. For example, using software to travel through a network to inventory software for licensing purposes is considered processing of personal data (application User IDs) and implicates the Regulation.

c. The Depth of the phrase "technical and organisational [security] measures." The Regulation requires data "controllers" (the entities that have the last word on how the data is used) to "implement appropriate technical and organisational measures"[4] to protect personal data. In fact, the Regulation uses this phrase 21 times. In doing so, the Regulation cites as examples the rather amorphous "ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems" and the more specific "encryption" and the "ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident."

In essence, the Regulation is asking controllers to employ information security frameworks, which enable professionals to create consistent, repeatable processes and implement controls that are generally accepted by the information security community. While multinational companies can likely meet some of the law's requirements right now, most will find that they need all of those two years in order to be completely ready for enforcement.

Where the Regulation will come as a surprise to those professionals is the recommendation (if not outright requirement) to use "pseudonymisation," which might be better known as "tokenization" or "aliasing." The Regulation cites pseudonymisation 15 times, and what is striking here is that it represents a control that is likely new to the vast majority of professionals, almost certainly to those outside of the payment card industry, where tokenization has some currency. This requirement is going require a substantial amount of work (mostly on the part of third party service providers) to re-engineer IT architecture and processes; other requirements, such as data protection by design and by default (described below) will only add to it.

d. The jurisdictional reach has expanded. The jurisdictional reach (called the "territorial scope") of the Regulation is, effectively, global. Companies based outside of the EU that offer goods or services to data subjects (i.e., individuals) there are covered by the Regulation. However, those that are involved in the "monitoring of the[] behaviour" of those data subjects are also covered. This concept of monitoring is closely linked to the concept of "profiling," which is processing personal data to "analyse or predict aspects concerning that natural person's performance at

work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[.]"[5] In other words, the analysis of personal data to predict shopping preferences or to suggest products or services that is commonly used by e-commerce providers. This jurisdictional reach potentially includes any organization that performs analytics using personal data of EU data subjects, including for information security purposes.

Companies based outside of the EU that offer goods or services to data subjects (i.e., individuals) there are covered by the Regulation.

Thirteen Essential Steps

1. Use an information security framework. Article 32 of the Regulation mandates that controllers and processors "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk." Information security frameworks represent a collection of best practices accumulated by professionals across industries over time and, as such, offer ideal starting points for developing appropriate measures. Frameworks such as the NIST Cybersecurity Framework (2014)[6] and ISO/IEC 27001[7]/27002[8] offer accepted industry standards for data protection. While the EU does not prescribe a particular framework, a company's adherence to the standards set out in any of these frameworks will make demonstrating compliance with Article 32 much more likely in the event of a breach.

2. Identify personal data, including "special" data. Given the Regulation's expansive definition of personal data, just about any type of monitoring of IT systems, network-attached devices, or mobile devices is going to implicate personal data. So-called "special" data presents another challenge: the Regulation defines it very broadly as well and includes genetic or biometric data and personal health information. Because biometric data is considered "special" data and is implicated in logical and facility access controls, professionals will likely find that their own information security systems contain special data. They may be surprised to learn that special data also includes:

    - Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership; and

    - Data concerning a person's sex life or sexual orientation

    One recommended approach to address this is "data discovery," which involves using both active system scanning and passive network monitoring to locate unencrypted sensitive data in an enterprise information ecosystem. From there, discovery team members can determine whether to remove the data or apply controls.

3. Include unknown assets and shadow IT in your search scope. Two phenomena – unknown assets and shadow IT – have the potential to invite intense scrutiny by supervisory authorities in the event of a breach or misuse of personal data. Employees or contractors storing, without authorization, the personal data of others on mobile devices or with cloud service providers create tremendous exposure to malicious actors; those assets or services do not have the benefit of the enterprise's information security program, may have unpatched vulnerabilities, or be simply unfit for storing such data. Once compromised, supervisory authorities will ask why the company didn't have a program to combat such phenomena. Moreover, U.S. regulatory authorities may get involved, as they did in the Google Street View case.[9]

4. Determine if your processing is considered "high risk." Recital 89 of the Regulation suggests that "high risk" processing operations of personal data may be those "which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing." In other words,

the opportunities for high-risk processing appear throughout the enterprise. In fact, it may be preferable to presume that existing or planned processing is indeed high risk and proceed from there.

5. Conduct a data protection impact assessment (DPIA). U.S. federal law requires that all federal agencies perform a privacy impact assessment (PIA) before initiating a new collection of personal data and before developing or procuring IT to collect, maintain, or disseminate it.[10] Canada has its own requirement for PIAs[11] and in the United Kingdom, while not mandatory, PIAs are commonplace.[12] The Regulation analog to this, the Article 35 data protection impact assessment (or DPIA), similarly requires that an assessment be conducted "[w]here a type of processing in particular using new technologies" is likely to result in a high risk to individuals. Information security leaders who are using the NIST Cybersecurity Framework can apply the categories in its Identify function to support the DPIA process. Similarly, information security leaders who are using ISO/IEC 27002 can apply its Information Classification and its Security in Development and Support Processes to support the DPIA process.

6. Perform and document risk mitigation actions. An organization's ability to mitigate risk in connection with the processing of personal data and document that mitigation is crucial in several contexts. Recital 83 requires that controllers and processors evaluate the risks inherent in the processing and then implement risk mitigation measures. In the event that processing is considered "high risk," the Regulation requires controllers to consult with supervisory authorities when they're unable to sufficiently mitigate those risks (Recs. 84 and 90). In the event of a data breach, the controller will likewise need to document the mitigation actions it has taken in response (Art. 33(3)(d)), engage with the supervisory authority (Art. 36), and further demonstrate the effectiveness of those actions in light of a proposed administrative penalty (Art. 83(2)(c)). Processors will likewise have to document risk mitigation as part of their technical and organizational measures (Art. 28(1)) and damage mitigation in the event of a breach (Art. 83(2)(c)).

7. Review your use of encryption and plan for pseudonymization. The Regulation cites use of encryption as an exception to the requirement that controllers notify data subjects in the event of a personal data breach, assuming that the personal data in question was effectively encrypted (Art. 34(3)(a)). It also cites encryption as one "technical and organisational" security measure (Art. 32(1)(a)). However, pseudonymization plays a larger and overall substantial role throughout the Regulation. Notably, it is cited in the context of processing data for purposes not previously consented to by the data subject (Art. 6(4)(e)), as a "technical and organisational" security measure (Art. 32(1)(a)), as part of an industry Code of Conduct (Art. 40(2)(d)), and in the event of processing personal data "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[.]" (Art. 89(1)). While the rationale for such a prominent role for pseudonymization under the Regulation is unclear, professionals should begin investigating how to incorporate into their overall security program and budget accordingly.

8. Add "resilience" to your CIA triad. Article 32 of the Regulation requires that controllers and processors implement security measures that include the "ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services[.]" While the first three components are well known to professionals as the "CIA triad," the fourth one – resilience – is relatively new. Regulation does not define the term (in fact, it only appears once); however, one scholarly analysis stated that

> [i]t seems likely that redundancy is key—that is, that the failure of any discrete component should not cause systemic failure. In addition, the ways in which information is stored, accessed, modified, and transferred will all need to be carefully crafted so that a single failure or manipulation does not cause downstream consequences that are detrimental to the system as a whole or that allow for exploitation/modification of information.[13]

The concept of resiliency is explicitly addressed by the NIST Cybersecurity Framework which states, "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply

the principles and best practices of risk management to improving the security and resilience of critical infrastructure."[14]

9. Review your Business Continuity and Disaster Recovery plan. Article 32(1)(c) requires, as a security measure, "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident[.]" Professionals should review both their own business continuity and disaster recovery plans as well as the uptime commitments in vendor service level agreements to determine if changes need to be made in light of the Regulation. Organizations using the NIST Cybersecurity Framework can apply guidance in its Recover function. Likewise, organizations using ISO/IEC 27002 can apply its Information Security Aspects of Business Continuity Management.

10. Review your incident response plan. In the event of a data breach, a controller must be able to report to the relevant supervisory authorities "without undue delay" and where feasible, within 72 hours of becoming aware of the breach (Art. 33(1)). In the event of a "high risk" event, the controller must notify data subjects "[w]ithout undue delay" (Art. 34(1)). A processor must be able to notify the controller "without undue delay" (Art. 33(2)). Notifications from the controller must contain the following:

    - The nature and details of the breach;
    - Contact information for the data protection officer;
    - The likely consequences of the breach; and
    - What measures have been taken (or are proposed) to address the breach, including efforts to mitigate adverse effects.

    The near ubiquity of data breach notification laws in the U.S of means that breach notification procedures are likely already an element of your incident response plan. When reviewing, determine if you can meet the 72-hour notification standard and your capabilities for documenting post-breach mitigation to supervisory authorities.

    Organizations using the NIST Cybersecurity Framework can apply guidance in its Respond function. Likewise, organizations using ISO/IEC 27002 can apply its Information Security Incident Management.

11. Invest in security certifications or attestations. Article 42 of the Regulation introduces the idea of "the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors." EU certification bodies will now begin work on an EU-wide seal/mark that incorporates the requirements of the Regulation—the European Data Protection Seal. However, there is neither a published timetable for the development and release of the certification mechanism, nor is there an indication of its requirements. The certification process may resemble current certification or attestation processes such as ISO/IEC 27001 or SOC2 and, as a consequence, companies should be able to leverage their existing certifications or attestations. If your company is considering making such an investment, the Regulation is just another reason to move forward.

12. Be ready for the "right to be forgotten." Under current EU law, data subjects have the right to access personal data that a controller has about them and, if the processing is not in compliance with the law, to have that data rectified, erased or blocked. Under Article 16 of the Regulation, the data subject also has the right of rectification and, under Article 17, to have personal data erased simply because it is no longer necessary for the controller to have it—the so-called "right to be forgotten." This section of the Regulation embodies the result of litigation between the Spanish data protection authority and Google, whereby Google was required to eliminate links that referenced a Spanish data subject's financial difficulties that were resolved some years before.[15] The decision was important

because it stood for the proposition that both non-EU entities and search engines were subject to EU jurisdiction. Given how often enterprise data is simply archived rather than deleted and the sheer volume of such data, removing irrelevant person data on request is going to be a big challenge. Server and device logging, which can capture a substantial amount of personal data by itself, will likely be a target for erasure requests.

13. Call your attorneys. The Regulation represents a sea change in how the personal data of EU data subjects is governed throughout the data's life cycle, and meeting the mandates of the Regulation will require help from your attorneys, whether inside or outside your company. Some operations, such as transferring the personal data of EU data subjects to the U.S., are especially contentious, and necessitate close cooperation between information security and legal team members. While network and information security is considered under the Regulation a "legitimate" basis for processing personal data, expect requests from EU data subjects or their works council representatives to justify specific processing actions.

The white paper has been prepared by Scott M. Giordano upon request by Tenable™, Inc., and does not constitute legal advice.

How Tenable™ Can Help

Tenable™ delivers comprehensive solutions that provide continuous visibility and context, enabling decisive actions to reduce your cyber exposure gap and better protect your organization. With SecurityCenter Continuous View® (SecurityCenter CV™) we can help your security team prepare for GDPR compliance by addressing these essential steps:

Use an information security framework. SecurityCenter CV helps you effectively implement and automate technical control monitoring for leading security frameworks, including ISO/IEC 27001/27002, NIST Cybersecurity Framework and the CIS Controls. Organizations, including those adopting multiple frameworks, rely on SecurityCenter CV out-of-box reports, dashboards and Assurance Report Cards to efficiently automate, demonstrate and communicate conformance.

Report conformance. SecurityCenter CV allows organizations to bring multiple data types together into a single reporting interface, so that you can rapidly share the right data with the right personnel in the right context. For example, SecurityCenter CV cross-references technical controls into multiple frameworks so that the out-of-box reports, dashboards, and Assurance Report Cards can efficiently automate and demonstrate conformance to a wide audience.

Identify personal data, including "special" data. SecurityCenter CV can actively scan systems and passively listen to network traffic to identify unencrypted personal and special data in your enterprise, and as it enters and/or leaves your enterprise. You can then determine how to remove the data or apply appropriate controls to secure it.

Include unknown assets and shadow IT in your search scope. SecurityCenter CV delivers total visibility of known and unknown assets on your network that may be processing personal data. Using Nessus® Network Monitor (passive traffic analysis) and event monitoring tools you can detect devices, services and applications in use and identify associated vulnerabilities, further ensuring you have full visibility of where possible GDPR risks may be.

Invest in security certifications or attestations. Security certifications and attestations typically require evidence that controls are in place and operating effectively. With SecurityCenter CV, you can automate the continual assessment of controls. This allows you to evaluate and report on conformance outside of any audit cycle, providing proof of ongoing compliance or enabling timely adjustments and course corrections when needed.

About Tenable Network Security

Tenable, Inc. is the Cyber Exposure company. Over 23,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of

Nessus, Tenable built its platform from the ground up to deeply understand assets, networks and vulnerabilities, extending this knowledge and expertise into Tenable.io™ to deliver the world's first platform to provide live visibility into any asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, large government agencies and mid-sized organizations across the private and public sectors. Learn more at tenable.com.

Appendix A: Key Concepts of the Regulation

Personal data. "Personal data" is not limited to identifiers such as national identification or similar numbers but includes data that can ultimately be linked to an individual by cross referencing other data. U.S. information security professionals are often surprised to learn that business contact information and business email addresses of EU individuals are personal data. The definition includes "online" identifiers produced by "devices, applications, tools and protocols," which means that just about any software or electronic device will produce personal data. Biometric data, such as that obtained from fingerprint or retinal scanners, and genetic data are considered "special" personal data, and require explicit consent from the data subject.

Processing. Any action performed on personal data, including storing, is considered "processing," even if not performed by "automated means," and is within the scope of the Regulation. Arguments that a particular action does not qualify as processing will likely fall flat as a consequence. Allowing data to be automatically deleted under a document retention policy, for example, will qualify.

Controller and Processor. A data controller is an entity that determines "the purposes and means of the processing of personal data," a phrase that that has been the subject of much debate. A processor is an entity that "processes personal data on behalf of the controller." The distinction between the two, however, is also often the subject of debate. For example, travel agencies consider themselves to be the co-controllers of the organizations that contracted with them to provide employee travel services, even though those agencies wouldn't have access to employee data except for the contract. Under the Regulation, the processor arguably has all or nearly all of the duties of the controller, and as much exposure to regulatory sanctions.

Technical and organizational measures. The phrase "technical and organizational measures" is not defined by the Regulation, but can be thought of as the EU analog to the administrative and technical controls cited in NIST Framework for Improving Critical Infrastructure Cybersecurity[16] and the ISO/IEC 27002 Code of Practice for Information Security Controls.[17] The primary information security section of the Regulation (Article 32) states that in assessing the appropriate level of security, "account shall be taken…of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed." Since a risk-based approach is already a standard practice for developing and deploying an information security program, this clause offers some relief for beleaguered professionals and their budgets. Article 32 also offers some additional (potential) relief: an "approved certification mechanism" can be used to demonstrate compliance. While it's too early to determine if existing certifications (such as ISO/IEC 27001) can be leveraged to obtain an EU-approved certification, Article 32 offers the possibility.

Data protection by design and by default; data minimisation. "Data protection by design" is the EU's implementation of "Privacy by Design" (or "PdD"), which is the philosophy and approach of embedding privacy into the design of technology, business practices and physical design.[18] The Regulation (Article 25) requires that the data controller incorporate privacy protection measures at the time that the processing is contemplated and when the processing takes place. Article 25 cites pseudonymization as one such measure, and does so in furtherance of implementing the principle of "data minimisation," which the Regulation defines as use of personal data that is "adequate, relevant and limited to what is necessary in relation to the purposes for which they [the personal data] are processed[.]" Article 25 also requires that the data controller implement measures that, by default, ensure that "only personal data which are necessary for each specific purpose of the processing are processed." It further states that these measures "shall

ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." Article 25 poses a big challenge to professionals for a number of reasons, most of which relate to cost and the risk of opening up weaknesses. Historically, information security controls have been implemented after the business processes they support are already in use. Changes to them and the associated security program is a multi-year process at best, and asking an organization to do so "merely" in support of the Regulation is likely to be met with skepticism and rejected out of hand. Any time a security program is re-engineered, the opportunity for introducing new weaknesses or re-opening existing ones is present and may well defeat the entire process. This Article is perhaps the most problematic for professionals and their companies and merits a discussion of using compensating controls in lieu of PdD.

Data Protection Impact Assessments. Article 35 requires that when processing of personal data is contemplated and is "likely to result in a high risk to the rights and freedoms of natural persons," the data controller must perform an assessment on the potential impact on the personal data. This, of course, begs the questions of what qualifies as "high risk," what are "the rights and freedoms of natural persons," and the necessary contents of the assessment.

Appendix B: Summary of Information Security Considerations Under the EU Data Protection Directive 95/46/EC and the General Data Protection Regulation

Consideration	Data Protection Directive Article	General Data Protection Regulation Recital or Article
Applies to:	Data controllers. Art. 4.	Data controllers and data processors. Art. 3(1).
Risk of liability to:	Data controllers. Art. 23.	Data controllers and data processors. Arts. 82 and 83.
Jurisdictional reach	Limited primarily to operations within EU member states. • See the Art. 4 (a) "establishment of the controller" and Art. 4(c) "makes use of equipment" standards.	Global. • See Rec. 131. Applies "to processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State…" • See also Art. 3(2). Applies to the "offering of goods or services" to, or the monitoring of the behavior of, EU data subjects.
What qualifies as "personal data"?	An "identification number or [] one or more factors specific to his physical, physiological, mental, economic, cultural or social identity…." of a natural person. Art. 2(a).	A "name, an identification number, location data, an online identifier or [] one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.]" Art. 4(1).
Are information security measures a "legitimate interest" of the controller or processor?	Unclear. • See Directive 2009/136/EC (the EU Cookie Directive), which cites "[t]he processing of traffic data … for the purposes of ensuring network and information security" as a legitimate interest.	Yes. Recs. 49 and 71.

Information security requirements	Data controller must "implement appropriate technical and organizational measures to protect personal data...." Art. 17(1).	Data controller or processor "shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk...." Art. 32(1).
Breach notification	None. • But see the ePrivacy Directive 2002/58/EC, which requires notification to the competent national data protection authority (DPA) in case of a breach (Art. 4(3)). • See also European Commission Regulation No. 611/2013, which addresses breach notification for telecommunications providers, internet service providers (ISPs), and the like.	• Controller to supervisory authority: "[w]ithout undue delay, and, where feasible, not later than 72 hours...." Art. 33(1). • Processor to controller: "[w]ithout undue delay...." Art. 33(2). • Controller to data subject: "[w]ithout undue delay...." in "high risk" events Art. 34(1).
Privacy protection integrated/ embedded during system design or implementation	Not required.	Required. "[T]he controller shall...implement appropriate technical and organisational measures...which are designed to implement data protection principles...in an effective way and to integrate the necessary safeguards into the processing[.]" Art. 25(1).
Data Protection Impact Assessments (DPIAs)	Not required.	Required in cases of "high risk" processing. Art. 35(1).
Potential financial penalties	Varies by EU member state; maximums range from €150k-900k.	Up to €20M or 4% of the offending company's global annual revenue, whichever is higher. Art. 83(5).

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. O.J. (L 281) (23/11), pp. 0031-0050.
[2] Erika McCallister, et al., NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) E-1 (2010), available at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 4(1). O.J. (L 119) 4.5.2016, p. 33.
[4] The Regulation uses British English and this white paper will use British English spellings of words cited directly from the Regulation.
[5] See Id. at n3, Art. 4(4).

[6] The National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, v1.0 (February 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[7] The International Organization for Standardization. ISO/IEC 27001 - Information security management, available at http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.
[8] The International Organization for Standardization. ISO/IEC 27002:2013. Information technology -- Security techniques -- Code of practice for information security controls, available at http://www.iso.org/iso/catalogue_detail?csnumber=54533.
[9] Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data, available at http://www.ct.gov/ag/cwp/view.asp?Q=520518.
[10] See Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch. 36).
[11] See Directive on Conducting Privacy Impact Assessments, available at http://www.statcan.gc.ca/sites/default/files/media/dcpia-defrvp-eng_2.pdf.
[12] David Wright, et al., Trilateral Research & Consulting, Privacy impact assessment and risk management, Report for the Information Commissioner's Office, 4 May 2013, at 6, available at https://ico.org.uk/media/for-organisations/documents/1042196/trilateral-full-report.pdf.
[13] Matt Bishop, et al., Resilience is more than availability. In Proceedings of the 2011 workshop on New security paradigms workshop (NSPW '11)(2011). ACM, New York, NY, USA, 95-104, available at http://dx.doi.org/10.1145/2073276.2073286.
[14] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February, 12, 2014, at 1, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[15] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014), available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.
[16] NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February, 12, 2014, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[17] See, generally, ISO/IEC 27002 Information Technology – Security Techniques – Code of Practice for Information Security Controls, Second Edition, 2013-10-01, available at http://www.iso.org/iso/catalogue_detail?csnumber=54533.
[18] Russell R. Densmore, Privacy Program Management Tools for Managing Privacy Within Your Organization (2013), at 88. For an in-depth description of Privacy by Design, see https://www.ipc.on.ca/english/privacy/introduction-to-pbd/.