GDPR Clarity: 19 Frequently Asked Questions Answered

Published: 29 August 2017 **ID:** G00333107

Analyst(s): Bart Willemsen

Summary

The European General Data Protection Regulation has impact far beyond the EU alone. Security and risk management leaders can't "go at it alone," but must involve a multidisciplinary team to translate requirements and prioritize risk mitigation actions by using these FAQs.

Overview

Key Findings

The European General Data Protection Regulation (GDPR) will globally impact the processing of all personal data on EU residents and takes effect on 25 May 2018.

Though a *data protection* regulation, there are few prescribed technological requirements; rather, application of technology under the regulation is based on privacy risk.

There is still a lack of detailed operational regulatory guidance, while vendors and internal business stakeholders overwhelm SRM leaders with their own interpretation. This makes it difficult for SRM leaders to prioritize actions, and balance *not enough* versus *too much.*

Recommendations

Security and risk management leaders responsible for a privacy management program and preparing to meet EU GDPR requirements must:

Prepare the organization for sustainable compliance by obtaining board approval for a remediation plan.

Direct legal counsel to provide definitive interpretation of GDPR texts and assist in identifying operational requirements and demands.

Use the FAQs in this document to prioritize actions, implement technical and organizational security controls, and avoid pitfalls while enhancing the privacy management program's maturity.

Strategic Planning Assumptions

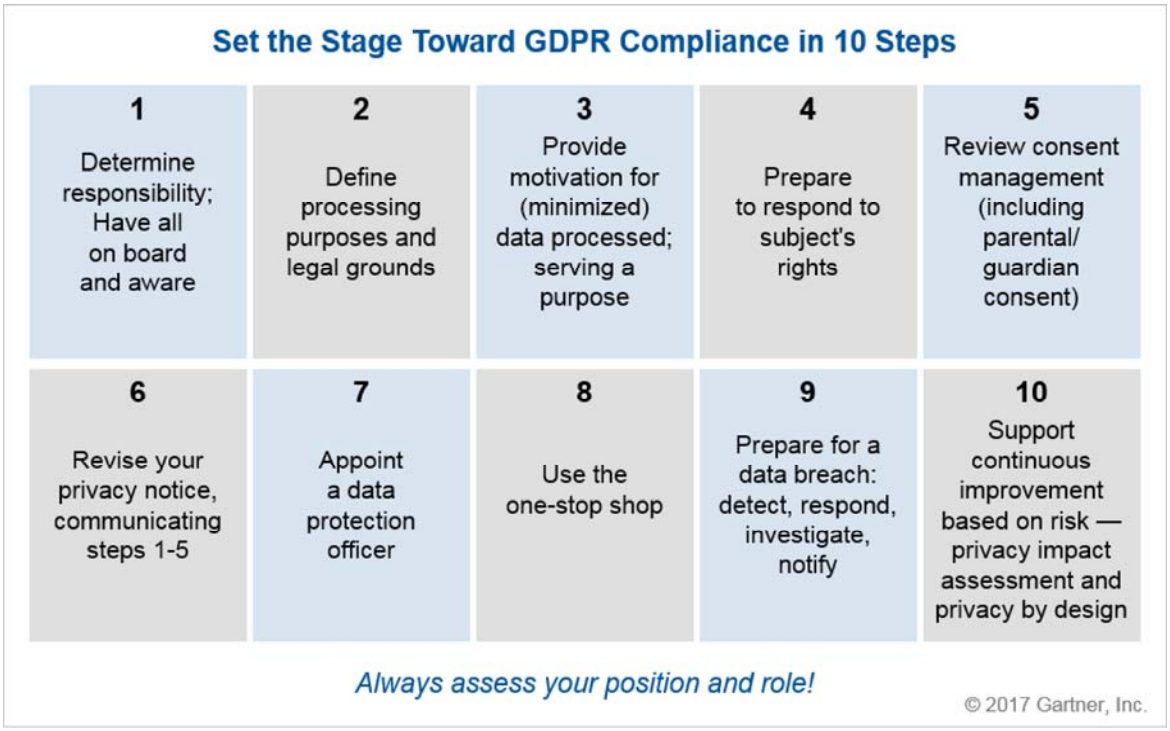
On 25 May 2018, less than 50% of all organizations impacted will fully comply with the GDPR.

Before 2020, we will have seen a multimillion Euro regulatory sanction for GDPR noncompliance.

Analysis

Security and risk management (SRM) leaders should prepare for the European Union's General Data Protection Regulation. The initial approach toward compliance contains 10 steps (see Figure 1). The primary objective of these preparations is to protect privacy — a fundamental right and freedom of people. [1] The GDPR is the EU's latest mechanism to mitigate privacy risk where the impact on an individual is highest. The GDPR stresses the importance of a data subject's rights, the manner in which data breaches are dealt with, and general control over personal data.

Figure 1. Initial Steps Toward GDPR Compliance



Source: Gartner (August 2017)

Data breaches can lead to substantial monetary and reputational damage. The GDPR represents additional consequences for organizations that fail to adequately protect personal data. Companies found in violation of the GDPR can be fined up to 4% of their global annual revenue or 20 million Euros, whichever figure is highest. More importantly, the media coverage following such a finding can cause substantial damage to a brand (see Note 1).

> Broken client trust moves customers to the competition.

Following the empowerment of individuals, a person who feels unprotected [2] may even bring an organization under regulatory scrutiny by filing a complaint.

It is crucial for SRM and business leaders to identify all business processes impacted by the GDPR. As these impacts occur across the company, every employee that handles personal data must feel a sense of responsibility. Adherence to this continent-spanning regulation requires a multidisciplinary approach that has the support and commitment of all stakeholders.

Basic Introduction of Scope and Applicability

Important role definitions include the data subject (in other words, the individual the personal data pertains to), the data controller and the data processor. It is important to assess whether the organization operates as a controller or a processor. For each business process, security and risk management leaders should urge the business stakeholders to assess the appropriate role in collaboration with legal counsel. The first four questions and answers below address the necessary explanations.

What is a controller and what is a processor?

The GDPR references data controllers and data processors; these roles are a matter of definition rather than choice (see Article 4 GDPR (https://gdpr-info.eu/art-4-gdpr/)). To determine the appropriate role for each processing activity, consult legal counsel. For the purpose of this document, readers should remember the following starting points (summarized in Table 1).

Table 1. Data Controller Versus Data Processor Responsibilities

Data Controller	
Controls what personal data is processed	
Data Processor	Uses data only as instructed by data controller
Responsible for processing purpose (in other words, determines why that personal data is processed)	
Data Processor	
Responsible for the means of processing	

Data Processor	
May create third-party agreements with data processors and subprocessors	
Data Processor	May create subprocessor agreements as authorized by the data controller

Source: Gartner (August 2017)

The "means" of processing may include any third-party service provision. Few organizations perform 100% of data processing themselves. Any third party involved in processing of personal data on behalf of the data controller functions as a "data processor." This then includes an outsourced complaint-handling call center, cloud-hosting provider, or any as-a-service third party. Data controllers must acknowledge the risk involved in where a data processor is deployed (for example, a SaaS, infrastructure as a service [IaaS] or identity and access management as a service [IDaaS] provider), and prioritize the following:

Data processors should only use personal data as is instructed by the data controller. Noncompliance on the part of a data processor with regards to the data controller's instructions, or the GDPR itself, reflects on the data controller's reputation. Data controllers must therefore demand assurance via data processor agreements to ensure personal data is properly handled by the data processor.

"Subprocessing" takes into account the full data life cycle, and regards any other data (sub)processor in the chain. Data controllers should take this chain into consideration when selecting a third-party service provider and demand that the requirements of data processors are applied to subprocessors as well.

SRM leaders must revise the vendor selection must-have criteria, and add qualitative protection requirements via procurement in the vendor selection process. This enhances a data processor's "fit" with the overall data controller's risk appetite and privacy compliance requirements.

Organizations should be aware that they can occupy both roles in different processing activities. Using a cloud-hosting provider's services, an organization may be a data controller and the hosting provider the data processor as it stores and processes the data on behalf of the data controller. However, when deploying EU-based employees, the cloud provider may be the controller for the HR activities. Similarly, a marketing agency may be a B2B client's data processor in the initial service provision, but when it uses the data gained in contracts to enrich profiles for a campaign of its own, it is the data controller for the latter activity.

What is personal data? Is the GDPR about security or about privacy?

The GDPR focuses on the protection of personal data and, hence, protects privacy. Adequately securing personal data is only a subset of all privacy-related requirements. Rather than a prescribed, limitative list of data items, "personal data" in the GDPR depends on context. Many things can be personal data. In short, personal data is any information relating to an identified or identifiable natural person (i.e., a "data subject"). Depending on context then, even singling out a record pointing at an individual may lead to identification, such as with IP addresses, location data, cookies, employee record number or even a (hashed) unique identifier (UID). For example, where a piece of paper contains "1,000," it's just a number. If that paper is a salary slip with a name, bank account and social security number, the figure as an attribute is personal data of sensitive nature. When in doubt, SRM and business leaders should ask the company's legal advisor for clarification.

What is "processing" of personal data?

Any action on data may be considered processing — from obtaining or creating the data to destruction at the end of its life cycle, and all actions in between. This includes copying, changing, pseudonymizing, transferring, storing and, more broadly, everything an organization does with the data, even calling it to a screen to look at it or the purging action itself, for that matter.

Does the GDPR apply to us?

If your organization has an establishment in the European Union, the regulation applies. But the effect goes beyond territorial boundaries of the EU alone. If you're offering services or goods to the EU, the GDPR applies as well. The same goes for organizations that, regardless of their own establishment, are monitoring an individual's behavior in the EU. This includes, for example, tracking an individual online to create a profile, or even to determine or predict the individual's preferences.

> In general, the GDPR brings a framework of best practices that, if adhered to, aid in compliance under multiple non-EU jurisdictions as well.

10 Steps Toward GDPR Compliance

The following (numbered) questions and answers explain the 10-step program toward GDPR compliance as depicted in Figure 1.

1. Who in the organization is responsible for compliance?

The business (process) owner is responsible for compliance. Preparing to comply does not necessarily mean only going through the formal articles one by one. Setting the stage for compliance requires setting up the organization to enable the correct mutual responsibilities. Hence, the organization should appoint business process owners. It is important that these leaders receive a mandate to make risk-based choices. Part of their responsibilities will be to conduct privacy impact and risk assessments periodically, and to address whether the outcome is within the mandated risk appetite. Therefore, they should also have the resources and discretion to mitigate accordingly. Leaders should emphasize to staff their accountability for adherence to privacy requirements. The implementation of a privacy-dedicated awareness exercise enables sufficient knowledge of the privacy management program.

The data protection officer (see Question 8) assists in this compliance plan, but is not formally accountable. To enable the organization to make an informed decision, security and risk management leaders must assess both privacy and business risks. They then suggest mitigating measures to the business process owner to decide on and implement as instructed. The business representative explicitly accepts the residual risk, or increases mitigation until the residual risk is within acceptable limits.

> When it comes to personal data, we see the most effective mitigating solutions originate in business process re-engineering, data minimization and improvement of security.

2. How to determine legal grounds and processing purpose?

Consult with legal counsel to determine the appropriate legal grounds for processing. There are only a few options provided in the GDPR, such as a contract agreement with the subject. The business process owners determine the processing purposes; in other words, they identify and explain the reasons to process personal data. Examples include execution of a contract agreement with an individual, compliance with regulatory requirements (such as a tax law dictating the retention of financial transactions), quality of service improvement, and the ability to handle complaints.

3. What personal data can I process?

With the proper controls, almost any data can be processed. However, an organization must first determine the legal grounds for processing, and document the processing purposes. Once these purposes are determined, the organization can provide the reason for what personal data must be processed to achieve those purposes. Data minimization dictates that whatever information that cannot be justified as necessary in respect to the purpose should be purged. For example, an organization might sell a car with a payment plan in the EU. Purposes for processing the buyer's personal data include receiving the monthly payments, retaining the transactions to comply with the applicable tax law, and having the transaction information available in case a payment went wrong and a complaint was filed. The legal grounds for processing originate in the contract agreement with the buyer, and the personal data necessarily processed includes name, car purchase, payment plan, and bank account information. Asking for the customer's marital status is unnecessary for these activities and must be avoided.

The subsequent cross-relation of data processed in connection with the purpose(s) that data serves dictates the authorization and access management controls that leaders must implement. Enabling only the authorized use of personal data carries inherent requirements to prevent other disclosures. This in turn dictates authorization and access management and the application of pseudonymization tooling.

As a purpose is achieved and the retention period set for the processed data expires, organizations should delete the personal data. Some retention periods may be prescribed, such as in the tax law example above. Other periods may have to be provided a reason by the organization. Time is a critical success factor for a data breach. Therefore, retention periods ideally are as short as possible and only as long as can be justified as "necessary" in the context of the processing purpose. The resulting retention scheme, however, does two things:

- Retention periods dictate the authorization and access policies during the personal data life cycle, enabling usage of the data in the context of predefined, documented purposes.
- The longest retention period per record determines the end of the personal data life cycle.

In the example of the car purchase, the access rights of the customer service employees to a completed transaction are revoked after a few months, if no complaint was filed. However, the transaction itself may have to be retained for seven years in total, following the regulatory tax requirement.

To enable adequate protection of personal data and allow insight into relevant privacy risks, the sensitivity of personal data that is processed should be observed in the processing context. Barring regulatory requirement, processing special categories of personal data — for example, revealing information about health, ethnicity or religious beliefs — should be avoided where possible. Organizations are encouraged to verify the necessity and legality of processing special categories of personal data with their legal counsel.

4. Should we prepare for data subjects to exercise their rights?

Yes. The GDPR does provide data subjects with a set of rights over the administration and use of their personal data, though some of these rights already exist. GDPR Articles 12 through 23 deal with the rights of data subjects; this research highlights a few such rights. Organizations that control their personal-data processing activities throughout the data life cycle should have less trouble enabling these rights. The "right to be forgotten," for example, mainly follows the retention scheme (see Question 3). In the example of the car purchase, there is a valid reason to retain the customer's personal data as long as the payment plan hasn't ended. Note that, at the end of the determined data life cycle, the responsibility to control deletion of personal data extends to both the backup and the data processor's environments.

The right to data portability can be assured by implementing a self-service portal. This also enables other rights, such as the right to access what personal data is processed, or the right to correct or amend it. When established, the same online platform can be used to provide transparency (statements and notices), and notification. Where an assessment shows that a subject's rights requests are expected to be few and far between, a manual process to hand over the personal data will suffice.

Considering the evolution of the Internet of Things (IoT), (big) data analytics and increasing application of machine learning and artificial intelligence technology, Article 22 provides an interesting right: The right "not to be subject to a decision based solely on automated processing, including profiling." Barring the exceptions provided in that same article, this implies a strong focus on automation of analytics and the use of the subsequent results. Analytics activities used for "what advertising do we show on a website," for example, will likely not have a high impact; but in other use cases, such as determining whether someone gets a mortgage, credit card or job, caution is advised.

5. Is there anything special about consent?

Yes. The characteristics of consent are quite specific. For one, it should be freely given, indicating that there can be no coercion or pressure. This brings a complication in, for example, employee relations, where an employee might be afraid to lose his job when not consenting to a specific processing activity. Employers should therefore tread carefully when relying solely on that basis.

"Consent" in the GDPR requires the circumstances to include several conditions:

" *By a clear affirmative act* ." Silence or implied consent and prechecked boxes, then, are a thing of the past. The organization must ask outright for consent.

" *Specific* ." When the processing has multiple purposes, consent should be given for all of them. Obtaining separate consent is advised where the processing activities are not inherently related. Buying a pair of sunglasses in a web shop, for example, does not automatically lead to receipt of the daily newsletter from that moment on. The burden of proof — that consent was indeed obtained in a correct and explicit manner — lies with the data controller.

"(As an) informed and unambiguous indication of the data subject's agreement to the processing of personal data ." For consent to be informed, the identity of the controller and the processing purposes should be provided. This requires use of plain language when providing the information the consent is based on. Likewise, member states have additional requirements for the protection of children (minors), as their consent may not be deemed valid.

Finally, the burden of proof that consent was obtained lies with the data controller. Thus, proper consent management includes not only administration (logging) of the consent itself, but also the conditions under which it was provided.

6. What should I include in my privacy notice?

Revision of a privacy notice is necessary, but can only be done properly after completion of a privacy impact assessment (PIA). The result of a PIA provides clear and transparent insight into the actual data processing activities and provides the organization with the privacy policy basis. A good privacy statement, or notice, is written in easy-to-understand language, and is short (or layered according to the following different subsections). It contains the following items:

An introduction of the data controller ("who we are")

An explanation of the personal data that is processed

A description of the purposes for which that personal data is processed

An explanation for the duration of the retention periods applicable

A description of data processors that are involved on behalf of the data controller

An indication of who to contact ("contact us") in case of a complaint, a question, or when a data subject wishes to exercise his or her rights

7. What is a data protection officer (DPO) and do I have to appoint one?

The role of the DPO is not a new one, but under GDPR is now formalized. The DPO not only looks after protection of the data, but also is usually tasked with developing and implementing the organization's privacy policies and processes. Representing the regulatory authority internally, so to speak, the DPO assists organizations in complying with their legal obligations. Aside from the security aspect, the DPO also addresses principles such as openness, fairness and transparency about personal data.

GDPR mandates may require you to appoint a DPO, for example, if you are a public body; other organizations may have to as well. The GDPR dictates the necessity of a DPO where "regular and systematic monitoring of individuals on a large scale" takes place, or when the core activities include large-scale processing of (sensitive) personal data.

> Gartner advises organizations to appoint a DPO where you can. The multidisciplinary team responsible for adequate privacy protection simply needs a multiskilled expert to lead it.

This team includes business process owners, legal, audit, risk, HR and security professionals.

8. We operate in multiple member states; do we have to contact all the 28 data protection authorities?

Fortunately, no. The European Union currently has 28 member states and each has its own data protection authority (DPA). Each DPA focuses on protecting its own citizen's privacy rights. It may be necessary to contact a DPA, for instance, when a data breach potentially affects citizens of that particular member state. Should the breach pertain to individuals in all 28 member states, in the worst-case scenario, an organization would theoretically face required notification to all DPAs.

The regulatory authority in the member state where your organization's primary establishment sits will function as a lead authority, the "one-stop shop." Acting as a single point of contact, the other authorities are informed through the lead authority. Organizations not established in the EU should appoint, in turn, a representative allowing a similar one-stop shop entry for the regulatory authorities.

9. Will we be fined for a data breach?

Not necessarily. Barring the absence of any processing activity, 100% security does not exist. Organizations should assume a data breach will happen. They are responsible, however, for the application of sufficient preventative, detective and other countermeasures. Though experiencing a data breach in itself is not sanctionable, it is the ultimate moment to demonstrate sufficient control over personal data.

A data breach (or "every unintended loss of [control over] personal data") must be communicated to the regulatory authority within 72 hours of detection. When the breach has a potential impact on the subjects, the organization should notify those individuals as well. A subsequent investigation, or even the lack of notification, may reveal noncompliance, which in turn can be reason for regulatory action.

Security and risk management leaders should have a (frequently tested) data breach response playbook ready for dealing with data breaches (see "Toolkit: Security Incident Response Roundtable Scenario for Privacy"). Necessary capabilities for both before and after a breach include continuous risk assessment, adequate security control application, detection controls, and (timely) response procedures. In other words, important questions include:

What data is impacted?

Who is the data about?

Is the breach of harm/potential impact to the individual?

How did the breach happen?

Who do we notify and how?

10. Who can help to protect our data per the GDPR?

There's no privacy vendor that can do it all for you. To determine the organization's needs, SRM and business leaders should look at what functions they must perform for GDPR compliance compared against practices and security controls that may already be in place. If they can't perform required functions, they should consider provisioning a third-party service.

There are *privacy management* tools, such as integrated risk management, and consent and cookie management tooling. Then there are *privacy control* tools, which include data life cycle management and pseudonymization tools such as tokenization or masking. Finally, there are *security solutions* in all existing forms. Gartner is seeing a heightened interest in markets where various features are combined, such as cloud access security broker (CASB), data-centric audit and protection (DCAP) and data loss prevention (DLP). Adequate, demonstrable privacy protection requires a combination of these types of tools. Organizations may be tempted to focus immediately on enhancing security only, but that is seldom the correct approach.

> The bottom line is that all security controls must be applied on the basis of demonstrated, assessed risk.

A continuous risk assessment, as well as planning and prioritizing security improvement, are just as important as selecting the appropriate security controls for the current operation. GDPR requires *adequate* security, which, in the long run, may vary following the changing context of technology evolution and privacy risk.

Additional Questions

Should I move my data centers to Europe, and what about cross-border data transfers?

Not necessarily. There are indeed restrictions as to where personal data is allowed to be. There are, however, also mechanisms available to have data transferred to and from the EU. For the 31 European Economic Area (EEA) members, transferring data across national borders is permitted. There are also 11 countries with an "adequacy decision" from the European Commission, allowing cross-border transfers here as well. [3] Having a data center in either of these jurisdictions while operating in another is perfectly acceptable.

A transatlantic agreement called Privacy Shield (formerly Safe Harbor) exists to address cross-border transfers between companies in the EU and the United States. Though the long-term stability of the agreement may be under scrutiny, over 2,000 organizations have already self-certified for the Privacy Shield. The attestation itself provides end-user organizations a certain level of assurance of the framework's applicability. As long as the agreement is legally valid, a data center in the U.S. can also be used.

For all other cross-border transfers, SRM leaders should use either EU Model Contracts, to be obtained from the European Commission website, or Binding Corporate Rules (BCR). BCRs are of potential interest for global enterprises and large service providers mostly. A non-EU-based data center can still be deployed under coverage of such rules and protection mechanisms.

Does encrypting everything exempt me from having to comply?

No. Encrypted data usually leads to pseudonymization rather than truly anonymous data. A data breach involving encrypted information should still be monitored, because reidentification and decryption are still a risk. Gartner advises clients to consider reporting data breaches on encrypted personal data to the regulatory authority as well. Where a postbreach impact assessment demonstrates a risk to the subject, that individual must be informed as well. Note that "anonymization" is the deletion or changing of personal data in such a way that this personal data can no longer be assigned to a certain or ascertainable individual or can only be assigned with a disproportionately high effort in terms of time, cost and work.

Pseudonymization, instead, is the replacement of an individual's name and other identifiable characteristics with a label to prevent identification of the individual by unauthorized parties or to render such identification substantially difficult. Pseudonymization techniques include certain levels of masking, redaction, tokenization and/or encryption of personal data. These are ways to enhance security, but they do not necessarily create data that is out of scope for the GDPR.

How is masking useful?

There are two main reasons to use data masking. The first is that personal identifiable data can only be used for designated purposes. Testing, for example, is not a processing purpose that data subjects usually consent to. Moreover, testing environments are often less protected than operational environments. In such cases, anonymous information should be used rather than live data. The second reason is that masking reduces risk/impact from a data breach. Similar to other pseudonymization (tokenization or encryption — either SaaS or done on-premises), the impact of a data breach on individuals (subjects) is reduced. It's a proper preventative measure.

How does cloud technology relate to the GDPR?

A data controller is responsible for the conduct of any of its data processors. Noncompliance with regard to GDPR on the vendor side reflects on the compliance of the end-user organization. There are ways to retain control from an end-user perspective (see "CISO Playbook: How to Retain the Right Kinds of Control in the Cloud"), and service providers are encouraged to adjust their products equally (see "Adapt Your Cloud Hosting Proposition Now for Imminent GDPR European Privacy Regulations"). Moving to the cloud may add to the security aspects of the processing activity, but could also lead to residency concerns. If the risk appetite of the end-user organization requires additional controls, a CASB service may be helpful (see "Market Guide for Cloud Access Security Brokers"). Alternatively, data protection in hybrid or on-premises operations is increased by adoption of DCAP products. These products monitor and respond to malicious or inappropriate user access behavior with data stored pervasively across on-premises or cloud silos (see "Market Guide for Data-Centric Audit and Protection"). A collateral benefit is that privacy compliance is demonstrated by mapping, dashboarding and logical control application.

Are mobile devices covered by the GDPR?

Yes, as is every technology used for the processing of personal data. Mobile devices are sensitive endpoints and are part of the data processing chain. Though these devices are used to process personal data, the risk is twofold since they also process information on the user. Data breaches occur when mobile devices are lost, resulting in unintended loss of control over data processed.

Enterprise mobile management (EMM)/DLP/mobile device management (MDM) and similar technology should only be in scope depending on the risks assessed to increase compliance with GDPR requirements for "adequate security." Bring your own device (BYOD) initiatives may require a choose your own device (CYOD) alternative if the employee doesn't consent to his personal device being monitored. After all, consent has to be freely given. As indicated in Question 6, employee consent to bring an owned device under monitoring may not be considered valid.

Evidence

Gartner has taken more than 5,800 inquiries on privacy matters in between publication of the 2016 and 2017 Hype Cycles for Privacy, a 45% increase over the previous period (between the 2015 to 2016 Hype Cycle publications). More than 1,000 inquiries pertained primarily to the GDPR since the term was coined mid-2016.

Additional resources for this research include:

"Model Contracts for the Transfer of Personal Data to Third Countries." (http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm) European Commission.

"Overview on Binding Corporate Rules." (http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm) European Commission.

"Data Protection Officer." (https://ec.europa.eu/info/departments/data-protection-officer_en) European Commission.

"Guidelines on Data Protection Officers ('DPOs')." (http://ec.europa.eu/newsroom/document.cfm?doc_id=43823) Article 29 Data Protection Working Party.

"Opinion 05/2014 on Anonymisation Techniques." (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf) Article 29 Data Protection Working Party.

"Regulations." (http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf) Official Journal of the European Union.

"Guidelines on the Right to Data Portability." (http://ec.europa.eu/newsroom/document.cfm?doc_id=44099) Article 29 Data Protection Working Party.

"Privacy Impact Assessment (PIA)." (https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/privacy-impact-assessment-pia) The Personal Data Authority.

"Opinion 15/2011 on the Definition of Consent." (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf) Article 29 Data Protection Working Party.

"General Data Protection Regulation." (https://gdpr-info.eu/)

[1] Article 8 of the European Convention on Human Rights (http://www.echr.coe.int/Documents/Convention_ENG.pdf) ; Article 12 of the UN Universal Declaration of Human Rights (http://www.un.org/en/universal-declaration-human-rights/) ; Article 17 of the UN International Covenant on Civil and Political Rights (http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx) ; The Fourth Amendment of U.S. Constitution (https://www.usconstitution.net/xconst_Am4.html) .

[2] In TRUSTe Privacy Index, 2015, Consumer Confidence Edition, 91% of people surveyed said they would avoid doing business with companies that do not protect their privacy.

[3] "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries." (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm) European Commission.

Note 1
Data Breach Example evidence

A one-year model (see "Analysis: How Data Breaches Affect Stock Market Share Prices" (https://www.comparitech.com/blog/information-security/data-breach-share-price/) from Comparitech and "Post-Breach Share Prices Plummet Below NASDAQ Average" (https://www.infosecurity-magazine.com/news/share-prices-plummet-below-nasdaq/?mkt_tok=eyJpIjoiWmpFd1pUa3dNR1kwWW1GaiIsInQiOiIrSmh1RFBqTWp5Ykd5Q3BLV0d6VnZ5cWVieHVJSUhBZzVYMU9UMVlcL29DSythbGR5T3dsQXlyS2xmWnBlOV from Infosecurity Magazine) showed that share prices experienced an immediate 2.84% drop versus the Nasdaq average, and took 38 market days to recover. The stocks then outperformed the Nasdaq until day 175, at which point they started falling again. Three years after a breach, share price had fallen 42% relative to the Nasdaq baseline.

these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. (/technology/about/ombudsman/omb_guide2.jsp)"
