WHAT YOU SHOULD KNOW ABOUT THE GDPR

An Osterman Research eBook
Published March 2018

HubStor™

OVERVIEW

The General Data Protection Regulation (GDPR) is a far-reaching and standard-setting piece of regulation focused on protecting personal data. Any organization impacted by its mandates needs to take rapid action to ensure they are appropriately ready by May 2018. Equally, however, is the realization that compliance is not a one-time event nor a journey with an easy destination. It is an ongoing process of learning, analysis, mitigation, and improvement.

However, many organizations are not yet ready for the GDPR starting gun in May 2018 and many need to expend significant resources to become compliant.

Compliance is required, but will bring spillover benefits for customer engagement, competitive positioning, eDiscovery, and regulatory compliance more generally.

BACKGROUND

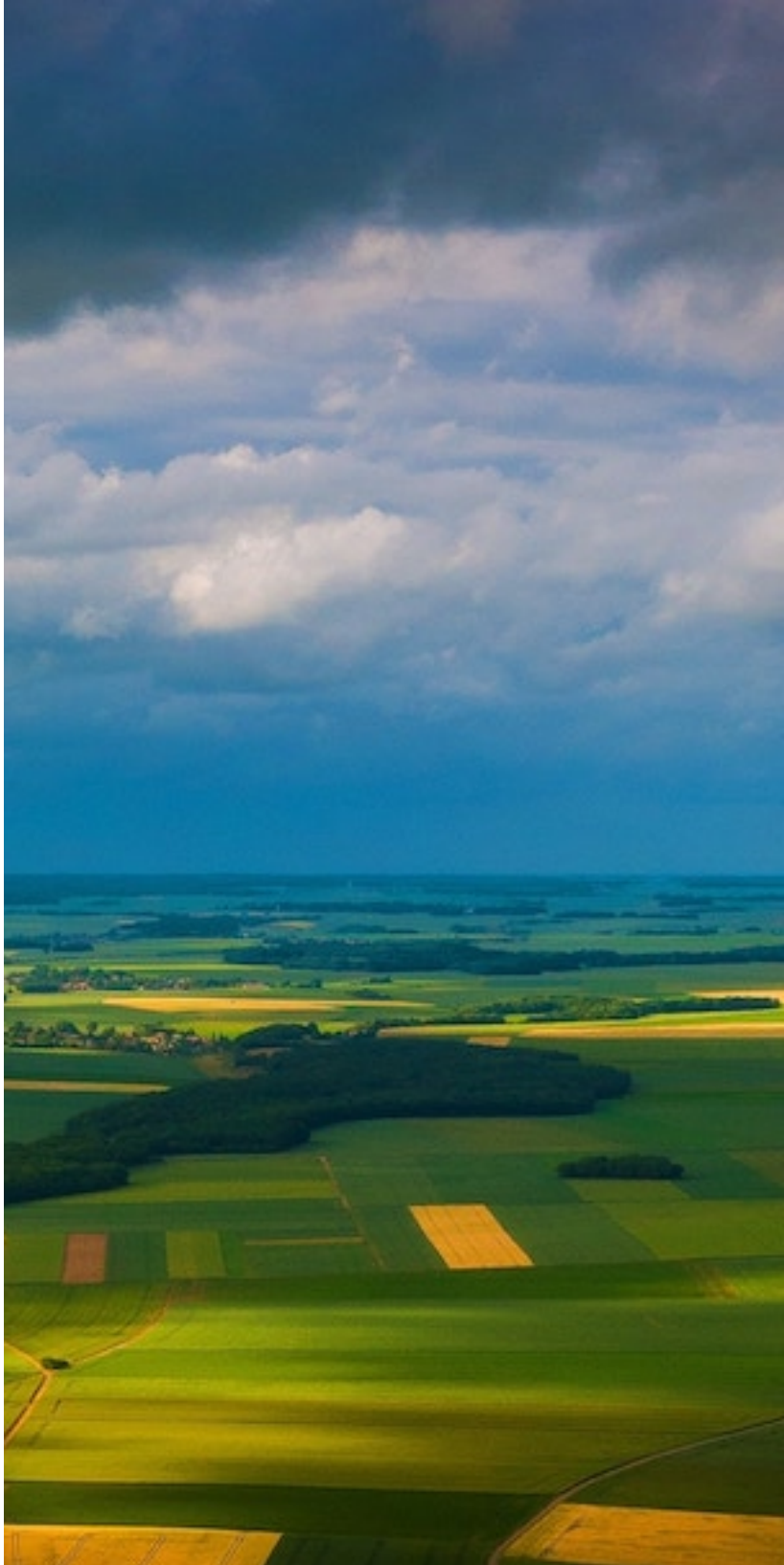
The GDPR continues the data protections afforded under the previous Data Protection Directive of 1995, but strengthens the rights of data subjects, harmonizes the approach to data protection across the European Union, and introduces new responsibilities for data controllers and data processors.

Even though the requirement for GDPR compliance commences in May 2018, compliance will be an ongoing effort that will continue indefinitely after May 2018.

GDPR may impose major penalties for organizations that violate the rights of EU data subjects: €20 million or four percent of total global turnover for a list of serious offenses, and €10 million or two percent of total global turnover for less serious ones.

Only five percent of the organizations surveyed by Osterman Research believe they will be "completely ready" for compliance with the GDPR by the deadline of May 25, 2018.

Every communication and collaboration technology and practice will be impacted by the GDPR, including email, storage, managed file transfer, encryption, security, archiving, closed-circuit television, printer solutions, scanning solutions, media, fax processes, photos, paper-based processes, etc. Organizations will need to carefully evaluate each of their current solutions and vendors to ensure that they will be compliant with the GDPR.



WHAT IS THE GDPR?

The General Data Protection Regulation (GDPR) is the very-soon-to-be-enforced new data protection law for all 28 Member States in the European Union. While it builds on and extends the principles in the earlier 1995 directive on data protection (Directive 95/46/EC), unlike the directive it applies Europe-wide as a unified regulation.

The GDPR:

- Applies not only within the European Union, but extraterritorially. Any organization that controls or processes data on living people in the European Union must comply with the data protection provisions of the GDPR, even if the organization does not have a physical presence in any European Union member state.

- Changes the answer to the question of "who owns my personal data?", giving ownership to the individual data subject and not the organization.

- Affects global data processes and data transfers, because personal data cannot be transferred outside of the EU to another country or region that lacks equivalent data protections unless Binding Corporate Rules, Model Contracts or other programs like Privacy Shield are in place.

- Requires notification of a data breach to the relevant Supervisory Authority and every affected data subject directly if the breach is likely to result in a risk to data subjects' rights and freedoms.

WHY THE GDPR?

- To modernize data protection regulations in Europe for new technological and communication advances such as the Internet, digital marketing, social networks, the Internet of Things, and pervasive data tracking capabilities, and to harmonize regulations across Europe to provide a unified pan-European approach.

- The harmonization driver flows from a European Commission priority of creating a Digital Single Market in Europe, by tearing down regulatory differences between national markets to create one unified market with common and consistent rules for all. Organizations will no longer have a differing set of data protection regulations to comply with per national market, but rather one unified compliance framework.

- To create a level playing field for every organization controlling or processing personal and sensitive data on EU data subjects, rather than allowing non-residence in the EU to provide an exemption from good data protection practices.

- To elevate the importance of good data security and data protection for personal and sensitive personal data.

- To re-center the locus of data protection in a global and interconnected world, putting the emphasis on the personal and sensitive data of people located in Europe regardless of where the organization collecting or processing that data is physically located.

SOME HISTORY

Over the past century in Europe (and undoubtedly before that too), personal data has been used against European citizens – think of secret police organizations in some countries and their meticulous filing system on the activities of millions of citizens at home and abroad. In creating a new standard for a new Europe, the European Convention on Human Rights (1953) guaranteed a right to privacy in Article 8, for private and family life, and correspondence; this right was based on the earlier Article 12 in the Universal Declaration of Human Rights (1948). The more recent EU Charter of Fundamental Rights (2000) carries forward the rights in the 1953 convention, and includes data protection as a fundamental right too.

The pre-GDPR practical outworking of the data protection ethos in Europe was the 1995 Directive on data protection. This, however, was not a common regulation for all of Europe, but a proposed standard from the European Commission that individual Member States should pay attention to and adopt within their own national laws. This created a complex compliance environment for any organization working across member states, as the very definition of personal data could differ by state, notifications of data breaches had to be made separately to the supervisory authority in each state, and data transfers between states had to be undertaken with special care. GDPR solves the variation with a single regulation for all of Europe, and for any organization that controls or processes data on EU data subjects, regardless of where the organization is based.

PERSONAL DATA

Article 4 defines personal data as "any information related to an identified or identifiable natural person" (called a data subject more generally in the GDPR text). Direct identifiers include name, ID number, and online identifiers such as an email address, and indirect identifiers include location data and various types of identity. The key test is whether a direct or indirect identifier, alone or in combination with others, can be used to uniquely identify a natural person. Article 9 adds a second layer to the definition of personal data, by separating out "special categories" of personal data, including data that reveal racial or ethnic origin, political opinions, and religious or philosophical beliefs, genetic and biometric data for identifying a person, and data about a natural person's sex life or sexual orientation. All personal data must be protected, and special categories of personal data carry additional prohibitions and constraints.

GDPR introduces new and expanded rights for data subjects, including the right of access (Article 15), right to erasure under specific circumstances (Article 17, also called the right to be forgotten), and the right to data portability (Article 20). These three articles in combination redefine the question of ownership of personal data, putting that power squarely in the hands of individuals and not the organizations that control or process information about them.

PENALTIES

GDPR has two tiers of administrative fines for non-compliance (Article 83), which can be levied by a supervisory authority based on the type of infringement, rather than on a first, second, and subsequent infraction basis:

- The fine for lower level infringements is up to €10 million or up to two percent of the total worldwide annual turnover from the preceding financial year, whichever is higher. Infringements at this level include failing to enact data protection by design and by default (Article 25), failing to keep adequate records of processing activities (Article 30), and not ensuring appropriate security of processing (Article 32), among others.

- The higher level of fines is up to €20 million or four percent of total worldwide annual turnover, whichever is higher, and is for infringements such as failing to comply with the basic principles for processing, including conditions for consent (Article 5-7, and 9), not providing data subjects with their rights (Articles 12-22), and unauthorized or inappropriate transfers outside of the EU (Articles 44-49), among others.

These administrative fines do not prevent a data subject from also seeking financial damages through a civil court against any organization that fails to process their personal data properly, does not ensure their rights are met, and fails to ensure adequate organizational and technical safeguards are in place to protect their personal data.

YOUR OBLIGATIONS

- Data can be processed (which includes just about any action performed on data, including storage) only if there is a legal basis for doing so (Article 6). These include direct consent from the data subject, necessity for performing a contract with the data subject (or getting ready to do so, on request from the data subject), complying with a legal obligation, to protect the vital interests of the data subject or another natural person, and in line with the legitimate interests of the controller or a third party.

- Both data controllers and data processors are required to maintain a record of processing activities under its responsibility (Article 30). Think of this as a data governance blueprint for all data processes that touch personal data.

- Data subjects have the right under Article 15 to ask any data controller for confirmation whether personal data concerning him or her are being processed.

- In what will create significant challenges for organizations with legacy data systems and legacy data archives, data protection must be "by design and by default" (Article 25).

- A data controller must notify the supervisory authority of a personal data breach within 72 hours of becoming aware of the breach, and data processors must notify the data controller of a personal data breach "without undue delay" after becoming aware of the breach (Article 33).

DATA SUBJECTS' RIGHTS

Data subjects, not data controllers or processors, are the owners of their personal data. The GDPR gives data subjects ownership by virtue of the following rights:

- The right of access (Article 15).
- The right to rectification (Article 16), for rectifying incomplete or inaccurate data about a data subject.
- The right to erasure (Article 17), so a data controller must erase a data subject's personal data on request.
- The right to restriction of processing (Article 18), when the data subject contests the accuracy of their personal data, when the processing is unlawful, or when the controller no longer requires the personal data but the data subject does not want it erased for use in legal claims.
- Data controllers have the responsibility to notify each recipient with copies of personal data when handling a data subject's request to rectify, erase, or restrict the processing of his or her data (Article 19), unless this is impossible or too difficult.
- The right to data portability (Article 20), whereby a data controller must supply a data subject with their personal data, on the condition that they provided it to the controller. This must be delivered in a "structured, commonly used and machine-readable

format," and be able to be transferred to another data controller. The data subject can even request the data controller to transmit their data directly to another data controller.

- The right to object to the processing of their personal data in line with specific legal bases, namely the performance of a task carried out in the public interest, in exercising official authority, or necessary for the legitimate interests of the controller or a third party (Article 21). Before the data controller can resume processing of the personal data, they must demonstrate that they have the grounds to continue doing so. This right to object also applies to processing for direct marketing purposes, which the data controller cannot override.

- The right to not be subject to a decision that is based solely on automated processing, including profiling, where that decision creates legal or similarly significant effects for him or her (Article 22). There are some situations where this right is not available, but if these exclusions are used, the data controller must at least offer the ability for human intervention, allow the data subject to express his or her view, and offer the ability to contest the decision.

- Finally, data subjects also have the right to learn if their personal data was breached and is likely to cause them harm (Article 34), although this is not stated as a "right" of the data subject as such, but rather a communication responsibility of the data controller. The effect, however, is the same.

CONSENT IS KING

If consent is used for collecting and processing personal data, there are specific requirements the data controller must meet. These include:

- The ability to prove that the data subject has given consent (Article 7(1)). This requires that you maintain good records on how and where consent was gained.

- The request for consent, if provided as one part of a written document, must be "clearly distinguishable from the other matters" in the document and easy for the data subject to read and understand (Article 7(2)).

- The ability for a data subject to withdraw his or her consent at any time, using a process that must be as easy as giving consent (Article 7(3)).

- Being very careful to ensure that only the personal data required for performing a contract or providing a service is requested from the data subject where consent is used as the legal basis (Article 7(4)).

- For children under the age of 16, consent for information society services must be given or authorized by whomever holds parental responsibility for the child (Article 8(1)).

MAINTAINING PRIVACY

Data controllers and data processors hold responsibilities to ensure the rights and freedoms of data subjects are maintained and their privacy respected. Specific responsibilities include:

- Avoiding the processing of special categories of personal data – for determining racial or ethnic origin, understanding political opinions, religious or philosophical beliefs, determining trade union membership, uniquely identifying a natural person through genetic or biometricU data, health data, or data about a person's sex life or sexual orientation – but there are exceptions (Article 9).

- Appointing a data protection officer who has expert knowledge in the field of data protection in order to inform and advise the data controller or processor about their data protection obligations (Articles 37-39). He or she must not be dismissed or penalized by the controller or processor for carrying out the required tasks.

- Working jointly and transparently where two or more data controllers are determining the purposes and means of processing. This includes being very clear about which responsibilities each holds under GDPR (Article 26).

- Ensuring that any data processor used by a data controller is compliant with the GDPR (Article 28), and that appropriate technical and organizational measures are implemented by the processor to ensure data protection.

PRESENCE IN THE EU

Every data controller and data processor that is not established in the EU must appoint a representative based in one of the Member States in which relevant data subjects are located (Article 27). This applies when processing activities relate to offering goods or services to data subjects in the EU, or monitoring of data subjects' behavior that takes place within the EU (Article 3(2)). The representative must be designated in writing, and be available for communication and interaction with supervisory authorities and data subjects on issues related to processing in light of the compliance mandates of the GDPR. This role of representation is not the same as a data protection officer; the representative must be based in the European Union, while a data protection officer is best located close to the operations of the data controller. Article 27 lists two exclusions to the need to appoint a representative based in the EU.

TECHNOLOGY SOLUTIONS

GDPR requires that each data controller and processor "implement appropriate technical and organizational measures" to ensure data protection of personal data. These should be done in light of an assessment of the risks to rights and freedoms of natural persons based on the personal data processed. Here is a list of technical measures that you are highly likely to require in your journey of protecting personal data and achieving GDPR compliance:

- **Archiving and backup**
  Archiving tools offload outdated and less frequently used data into secondary systems, reducing the volume of current data in production systems, while still providing a mechanism for authorized individuals to access the relevant data in the context of their day-to-day work. Archiving systems must still be compliant with GDPR, however, including the ability to discover personal data on a data subject under an access request, rectify any data that is incorrect, and erase data under a right to be forgotten request if the conditions for erasure are met.

- **Data Classification**
  Mission-critical sanctioned corporate systems that hold personal data in structured formats are much easier to understand in terms of data protection than the mass of unstructured data and unsanctioned applications in use. Data classification tools offer an automated method for analyzing all data stores and sources in the organization, to identify personal data and classify what is discovered. This extends into the usually difficult-to-find data

locations like copies, exports, backups, and shadow IT cloud services that employees are using. Data classification tools map what personal data is actually in place across the organization, so that appropriate mitigations can be developed (e.g., protect in place, migrate, delete). Another important consideration is the selection and use of review tools that will help decision makers to sift quickly through large volumes of information.

- **Managed File Transfer Solutions**
  File transfer solutions of various types, from consumer-focused tools to high-level managed file transfer solutions, are commonly used to send and receive information, including personal data. Many current of these solutions provide inadequate security and other controls and will not be compliant with the GDPR. At a minimum, any file transfer solution should integrate with identity management solutions, maintain tight user controls, integrate with DLP solutions, encrypt data when it is being transferred and when at rest, enable non-repudiation of data, enable scheduled deletion of data, and ensure that data transferred outside the EU fall under an appropriate transfer exception.

- **Data Loss Prevention (DLP)**
  DLP tools analyze flows of data in email and other systems to identify the presence of personal data using pattern-matching and other advanced forms of identification and classification. If personal data is identified and appropriate protections are not in place – for example, a spreadsheet attached to an email containing customer names and email addresses that is not encrypted – either the spreadsheet can be automatically encrypted or the message can be blocked or quarantined. DLP tools help

prevent the most common and frequent type of data breaches: employees sending data that should be protected in an unprotected form or to people who are not authorized to receive it.

- **Encryption**
  Encrypting personal data adds a strong level of data protection, by using a mathematical code to scramble alphanumeric characters into an unintelligible string that lacks any meaning and cannot be deciphered without the decryption key. Encryption is explicitly mentioned as a data protection safeguard in the GDPR, because most data breaches can be prevented if encryption is used. For example, if a data breach does happen, a controller is excused from the notification requirements if the risks to personal data are low, which would usually be the case if the data was encrypted when breached.

- **Identity Access and Management**
  Personal data is not protected if any employee can access it. Identity access and management tools introduce an identity system so that employees can be uniquely identified, and thus their access to corporate systems – and personal data – be carefully managed. A strong identity and access management system is essential all the time, but is extremely beneficially for preventing access to corporate systems and personal data when off-boarding an employee out of the organization entirely, or when an employee moves to a new role in the organization with a different set of access rights.

- **Pseudonymization**
  Like encryption, pseudonymization obfuscates personal data values by rendering them unintelligible to anyone without access rights. Unlike encryption, pseudonymization achieves this by replacing personal data values with a code that can be used to look up the original values that ar stored separately in a secured database. Pseudonymization is also explicitly mentioned in the GDPR, although the approach is not without its own risks, such as the unauthorized reversal of the pseudonymized data. However, in production systems, test and development environments, and data archives, pseudonymization offers one recommended way of protecting personal data.

- **Security Tools**
  Security tools analyze the integrity of network resources, endpoint devices, and cloud services to identify unauthorized access attempts, unwanted types of data including malicious threats, and the presence of unauthorized and questionable applications when access to a network or data resource are requested. These capabilities work in combination to reduce the likelihood of data breaches due to nefarious applications working quietly in the background to exfiltrate data, and can provide rapid awareness of an active breach attempt. Security tools can also identify out-of-date and unpatched operating systems and applications that are vulnerable to malicious threats.

  Tools to thwart phishing, ransomware, other types of malware and impersonation in email are critical to prevent malicious code from undermining the integrity, availability and resilience of data

systems. Advanced capabilities are essential and must go beyond simple spam and virus filtering.

- **Ensuring Safe Cross-Border Transfers**
  It is also essential that organizations implement appropriate safeguards when transferring data to nations outside of the EU. The GDPR allows such data transfers under three conditions:

  If the European Commission has determined that the level of personal data protection in the country to which information will be sent meets an acceptable standard.

  If binding corporate rules (discussed in Article 49) or contractual agreements are used to govern the management of the data sent outside of the EU. Moreover, Article 42 allows that "data protection certification mechanisms, seals or marks" may be approved for a maximum of three years "for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation".

  If an exemption is granted in the event that none of the conditions above can be satisfied (discussed in Article 49).

  Unfortunately, the validity of each of these mechanisms – including the Privacy Shield program which enables many organizations to transfer data to the United States – are under a legal challenge and have the potential to be invalidated. Organizations should consider alternative measures to enable compliance if these

mechanism are invalidated, which may include creating or expanding their data center capabilities within the EU.

- **Application Security Testing**
  Data protection must be "by design and by default," and application security testing tools help deliver this mandate by analyzing applications for vulnerabilities. Once identified and catalogued, software developers can rectify or mitigate the weaknesses before damage can be done. Penetration testing, for example, offers a process for analyzing application and system security, in order to elevate the overall security posture of the system.

- **Data Portability Capabilities**
  Data subjects have the right of data portability, where a data controller must supply the personal data the subject has provided in an appropriate format for transfer to another data controller. Tools that enable the export of data provided by data subjects that meet the right conditions will be essential.

- **User Awareness Training**
  Employee training is an organizational measure that has high overlap with the technical measures of protecting data. Employees should be trained on the requirements of the GDPR, their responsibilities to protect personal data, the risks of unsanctioned tools and applications, and the risky actions they should avoid in order to not fall foul of the data protection mandates. For example, sending a spreadsheet containing an export of personal data from corporate systems to their personal email address is a risky and dangerous proposition, the consequences of which

should be explained. Likewise for departing employees, copying data on customers to take to their new place of employment is a breach of GDPR, and should not be done.

- **Other Technologies**
  The above is a list of high-priority technical measures that help with GDPR compliance. Complementary technical measures include:

  - Incident response systems, for quickly being able to contain and respond to a security or data protection incident. We also recommend use of APIs to consolidate logs and forensics from key security systems to help identify, investigate and more quickly remediate threats.

  - The use of data redaction solutions that enable private or sensitive information to be blocked from access when data is transferred to third parties or even when it is stored by a data controller or processor.

  - Mobile device management tools, to remotely wipe or kill a compromised or lost device in order to prevent a breach of data. Such tools also provide a real-time dashboard on the data protection health of the device fleet, and enforce local settings such as encryption and the use of endpoint security software.

  - Behavior analytics to provide early warning of developing patterns that show weird or unsanctioned behavior by employees, that could give early warning signals of a data breach, for example. Such tools can also highlight impossible

valid situations, like an employee being logged into two devices simultaneously on opposite sides of the world (this would signal account credential compromise).

- Privileged account management analysis tools to ensure that only valid actions are undertaken by authorized IT administrators. Privileged accounts often have higher access rights to data systems containing personal data, and are a key attack vector for hackers and other actors with malicious intent.

- Process mapping tools, to document how processes with personal data work, where the data resides, who interacts with it, and how it is shared.

ABOUT HUBSTOR

HubStor is a cloud archive and hybrid cloud storage solution providing enterprise clients with industry-leading data protection, search, data management, and WORM storage on the Microsoft Azure cloud platform. Enterprise clients around the world use HubStor to manage data growth of file systems, protect Office 365 data, meet regulatory requirements, and preserve mission-critical information assets.

HubStor currently serves clients, large and small, across a variety of industries in the United States, Europe, United Kingdom, Canada, Australia, and New Zealand. HubStor is a Microsoft Partner and a member of the Microsoft Enterprise Cloud Alliance.

HubStor, Inc.
515 Legget Drive, Suite 800
Kanata, Ontario K2K 3G4
Canada

+1 855 704 1737

sales@hubstor.net

www.hubstor.net