WHITE PAPER

The GDPR Deadline Has Passed: What Should You Do?

An Osterman Research White Paper
Published May 2018

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond • Washington • 98010-1058 • USA
+1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

Executive Summary

The General Data Protection Regulation (GDPR) is the European Union's (EU's) latest attempt to protect the privacy of sensitive data for residents of the EU, and it goes much further than the current Data Protection Directive (DPD) in that regard. The importance of the GDPR cannot be understated in two important respects: 1) it goes much further than the DPD in terms of the rights it affords to data owners and the obligations it imposes on those who control and process this data; and 2) it will be implemented on May 25, 2018, meaning that any entity that holds data on EU residents must be ready to comply very soon. In short, if you have data on residents of the EU (and you most likely do), you have very little time to comply with the GDPR.

KEY TAKEAWAYS

- The GDPR can be viewed as both a negative and a positive for any entity that holds data on residents of the EU, but in many ways compliance with the GDPR will yield significant, spillover benefits for any organization that complies with it.

- The GDPR confers numerous rights on residents of the EU and, for all intents and purposes, gives them near complete control of their own data. Among these rights are the rights of data ownership, the right of access to any data that any entity maintains on them, the right to have errors in this data corrected, the right (within limits) for this data to be expunged by those who maintain it, the right to receive data in a standardized format, the right to control how their data is used, the right to learn if their data has been breached, and the right to object to the manner in which their data is processed, among others.

- As with any set of rights that is given to one group, a set of obligations is imposed upon others. Among the obligations that is imposed by the GDPR upon data controllers and processors are the following:

    - The requirement to maintain very good records about the data of EU residents is processed.

    - The requirement to provide any resident of the EU with any and all data held about them, in most cases at no charge.

    - The obligation to enable data protection "by design and default" in all systems that process or maintain data.

    - The obligation to report most data breaches within 72 hours after their discovery.

    - The obligation to prove that data subjects have provided their consent to have their data held and processed.

    - The requirement to maintain strict confidentiality about EU data residents, especially for highly sensitive information, such as their political opinions, union member and sexual orientation.

    - The obligation to cooperate with other data controllers and ensure that all third parties are compliant with the GDPR.

    - The obligation to implement solutions and technologies that will enable compliance with the GDPR to be established and maintained.

    - The appointment of a Data Protection Officer that will be charged with managing compliance with the GDPR.

The GDPR can be viewed as both a negative and a positive for any entity that holds data on residents of the EU.

ABOUT THIS WHITE PAPER

This white paper was underwritten by Druva; information about the company is provided at the end of this paper.

A Quick Background on the GDPR

LOOKING AT BOTH SIDES OF THE GDPR

There are two ways of looking at the GDPR:

- **The negative view**
  The GDPR is yet another onerous regulation that adds red tape, increased cost and the potential for enormous fines if the key provisions of the requirement are violated. Like most laws, the GDPR includes some level of vagueness so that it may be interpreted after its implementation, further complicating decision makers' planning about how best to address the key requirements of the law.

- **The positive view**
  The GDPR is about earning and retaining the trust of EU and non-EU customers by organizations that will maintain the integrity of their sensitive data, including their preferences, past purchases and their willingness to engage with them going forward. A competence in data protection may bode well for competence in other commercial aspects, and organizations properly positioned will earn greater freedoms and privileges in the future to serve customers than those that cannot get their data protection act together.

WHAT EXACTLY IS THE GDPR?

The General Data Protection Regulation (GDPR) is the new data protection law for all 28 Member States of the European Union (EU). The GDPR is an extension of the principles in the 1995 directive on data protection (Directive 95/46/EC), but unlike its predecessor, the GDPR applies as a unified regulation across all of the EU. In short, the GDPR is a unified data protection law that simplifies the regulatory environment for all organizations doing business with European residents. While there are a few areas where national law can change the regulation, giving a member-state specific interpretation, these are few and far between.

The GDPR does a variety of things:

- It provides a direct answer to the question of data ownership, giving ownership to individual data subjects and not the organizations the control or process this information. An individual may give an organization the right to store and use their personal data and sensitive data, but if consent is the legal basis for processing, data subjects own the right to revoke their consent at any time they wish. Organizations must be very clear about the legal basis on which they rely for storing and using personal data, and transparency with data subjects regardless of the legal basis.

- It applies not only within the European Union, but also worldwide for any organization that controls or processes data on living people in the European Union. These controllers and processors must comply with the data protection provisions of the GDPR, even if the organization does not have a physical presence in the EU. Such personal data can be related to offering goods and services to data subjects in the European Union, or monitoring the behavior of people that happens within the EU for the purposes of profiling, analyzing and/or predicting preferences, behaviors, and attitudes. Organizations that control the personal data that is captured and used are clearly accountable under the GDPR, but accountabilities now apply to any organization processing data on behalf of a data controller.

- It affects global data transfers and processes because personal data cannot be transferred outside of the EU to any other geography that lacks equivalent data protections unless Binding Corporate Rules, Model Contracts or other programs like Privacy Shield have been established. For example, even though the United Kingdom is likely to leave the EU, it is adopting the GDPR into its national laws to ensure that the same protections and rights apply within the UK and between the UK and EU member states.

- It requires notification of a data breach to data subjects directly and to the relevant Supervisory Authority if the breach will likely result in a risk to data subjects' rights and freedoms. If data is breached in the absence of adequate protections being in place, organizations that commit such breaches must have a robust response and mitigation plan for any breaches if they are likely to result in a risk to data subjects' rights and freedoms.

- It excludes protections for the personal data of EU data subjects who are involved in criminal proceedings.

After many years of development, the GDPR was published in the *EU Official Journal* in early May 2016, and it will be enforced beginning May 25, 2018. This means that, as of the publication of this white paper, the GDPR will be enforced in less than a month's time.

WHY WAS THE GDPR PUT IN PLACE?

The key drivers for the development and implementation of the GDPR were:

- To modernize data protection regulations in Europe to accommodate advances in technologies like the Internet, social networks, digital marketing, the Internet of Things, and pervasive data tracking capabilities. The GDPR was also established to harmonize the various regulations across Europe so that a unified, pan-European approach could be put in place. The earlier data protection directive was introduced before the Internet became commonplace, and it was increasingly out-of-touch with modern data challenges. The driver of harmonization flows from a European Commission priority of creating a Digital Single Market in Europe, which will effectively remove the regulatory differences between national markets so that one unified market with common and consistent rules for all can be created. Organizations will no longer have a differing set of data protection regulations with which to comply for each national market, but rather one unified compliance framework.

- To establish a more level playing field for every organization that processes or controls EU residents' personal and sensitive data, rather than allowing non-residence in the EU to provide an exemption from good data protection practices – this could and did happen under the previous Data Protection Directive. Since we live in a more highly connected world with the ability to sell goods and services easily to people anywhere around the world without a local physical presence, the playing field had to be re-defined based on the location of data subjects, not the organizations that sell to them.

- To heighten the importance of good data security and data protection for EU residents' personal and sensitive personal data. Just as new technologies have created digital markets where data can flow quickly and easily, new technologies have been created to protect that data since the established of the original Data Protection Directive. Consequently, the GDPR mandates many stronger protections both organizationally and technically to restore the appropriate balance.

- To place the emphasis on the personal and sensitive data of people located in Europe regardless of where the organization processing or collecting their data is located physically. This will have a significant impact on global legal frameworks by demanding that any organization, region or country that wants to trade within

The playing field had to be re-defined based on the location of data subjects, not the organizations that sell to them.

the EU market has equivalent or adequate data protection standards, rights, and obligations. Every organization that controls or processes personal data on EU data subjects will need to assess the requirements of GDPR on its data processes. Moreover, multi-national firms that have a presence in Europe may find it ends up being easier to establish the requirements of the GDPR as their standard and best practice for data protection anywhere they do business.

Data Subjects Have Numerous Rights

Under the GDPR, data subjects are given a substantial set of rights over their personal data:

- **Data subjects own their data and have the right to request it**
  Article 4 of the GDPR defines personal data as "any information related to an identified or identifiable natural person" (called a "data subject" in the GDPR text). The direct identifiers for this information include name, ID number, and online identifiers like an email address, as well as indirect identifiers like 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, such as religious or philosophical beliefs, racial or ethnic origin, political opinions, genetic and biometric data that can be used to identify a person, and data about a natural person's sexual orientation or sex life. All personal data must be protected and special categories of personal data carry additional prohibitions and constraints.

- **Data subjects have the right to have their data rectified**
  Data subjects have the right to rectification (Article 16) – the right to have inaccurate or incomplete data about them corrected. A data subject has the option of supplying additional information to facilitate the rectification process.

- **Data subjects have the right to be "forgotten"**
  The right to erasure of personal data (Article 17) obligates a data controller to erase a data subject's personal data on request. For example, if the data subject withdraws their consent for processing of their data, and consent is the only legal basis for the processing of that data, the data controller must remove all instances and copies of the personal data from its systems.

- **Data subjects have the right to obtain their data in a standardized format**
  Data subjects have the right to data portability (Article 20) and this data must be provided to them in a "structured, commonly used and machine-readable format". Moreover, this data must be in a form that will allow it to be transferred to another data controller. The data subject can even request that the data controller transmit their data directly to another data controller.

- **Data subjects have the right to control how their data is used**
  Data subjects have the right to restriction of processing of their personal data (Article 18), such as 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 subjects have the right to learn their data was breached**
  Data subjects have the right to learn if their personal data was breached and is likely to cause them harm (Article 34). While this is not stated as a "right" of the data subject per se, it is a communication responsibility of the data controller and so the effect is the same.

- **Data subjects have right to object to processing of their data**
  Data subjects have the right to object to the processing of their personal data in accordance 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, processor or a third party (Article 21). Before a data controller can resume processing of a data subject's personal data, the controller or processor 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.

What Must You Do as a Data Controller or Processor?

The rights conferred upon data subjects in the EU creates a number of essential obligations for data processors and controllers:

- **You must maintain very good records**
  Both data controllers and data processors must maintain a record of processing activities under their responsibility (Article 30). You can consider this a data governance blueprint for all data processes that impact personal data. Required information that data controllers must retain include the name and contact details of the controller (and representative and Data Protection Officer), the categories of data subjects and personal data, the purpose of the processing, the time limits for erasure of the different categories of data, the categories of recipients who can access the results of the processing, and a general description of the technical and organizational measures for protecting personal data.

  Data processors have a similar, but slightly shorter, list of requirements. Records must be maintained in electronic or paper form, and these records must be made available to the Supervisory Authority on request. Organizations with fewer than 250 employees are generally excluded from these record-keeping requirements, but there are some instances where this exclusion does not apply, such as processing special categories of data.

- **You must respond to SARs in a timely manner**
  Under Article, 15, data subjects have the right to ask any data controller for confirmation whether personal data concerning him or her are being processed. If data is being processed, data subjects must be given access to their data plus contextual information, such as the categories of personal data being processed, the purposes for the processing, the recipients or categories of recipients who have access (especially recipients in third countries or international organizations), the length of time the data is stored, where the data came from if not from the data subject, and the presence of any automated decision making that takes place on that data.

  Data subjects must also be notified of their rights of erasure, rectification, restriction of processing, and complaint to a supervisory authority. This must be provided free of charge, and promptly – data controllers have only 30 days to provide this information under normal conditions (90 days in some cases). The current Data Protection Act the requirement is 40 days, and so existing processes must now change to meet the new requirements.

  SARs are a critical issue that could quickly overwhelm any organization lacking exceptional data management practices and the technologies to support them. The ability to effectively see all instances of personal data regarding an individual and to know the lineage of each instance will be essential, not only for the ability to fulfill the access requirements of Article 15, but also the flow-on rights of rectification, erasure, and limitation of processing. GDPR attempts to prevent an

The rights conferred upon data subjects in the EU creates a number of essential obligations for data processors and controllers.

abuse of the subject access request right by virtue of a fee mechanism for second and subsequent requests from the same data subject, but any organization suddenly facing a large number of first time access requests will need to have very good response mechanisms in place.

- **You must enable data protection "by design and default"**
  Data protection must be "by design and by default" (Article 25), which will create significant challenges for many organizations with legacy data systems and legacy data archives. This requirement has been established to minimize the damage to the rights and freedoms of data subjects, and it includes the mandate for both organizational and technical measures. Pseudonymization – one method of obfuscating personal data values and discussed below – is specifically mentioned, as is the principle of data minimization so that personal data that is not necessary to a particular processing is never collected. The analysis of these measures is to be undertaken when the data processing method is initially designed and when the processing actually takes place. In short, data protection is not just a point-in-time requirement; it is a continual mandate.

  To achieve compliance with the "by design and default" aspect of the GDPR, organizations should carry out a risk assessment of all processes that might process personal data and, if deemed to be a high risk, a Data Protection Impact Assessment (DPIA) must be conducted every six months, since a DPIA is a per-process evaluation. New processes or changes to existing processes are then evaluated using a DPIA. Unless a formal risk assessment is carried out, it is difficult or impossible for decision makers to know for which processes a DPIA must be carried out. Further, without such a risk assessment, it is difficult or impossible to know if all processes are captured, documented and understood.

- **You must report data breaches within 72 hours**
  Data controllers must notify the Supervisory Authority of a personal data breach within 72 hours after becoming aware of the breach. Moreover, data processors must notify the data controller of a personal data breach "without undue delay" after becoming aware of the breach (Article 33). Data controllers are also obligated to advise data subjects "without undue delay" if a breach is likely to result in a high risk to the rights and freedoms of natural persons (Article 34).

  Interestingly, notification is not necessary if there is no risk to the rights and freedoms of natural persons, such as when the data was encrypted and so is rendered unreadable by unauthorized parties. Common examples of breaches include the loss of unencrypted computers or mobile devices, insecure disposal of personal information, and hackers accessing a database and encrypting it for a ransom. Detecting breaches requires having a very good handle on where personal data exists, as well as the state of data protection in real-time.

- **You must prove that data subjects have given you their consent**
  A critical provision of the GDPR is that 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 bases include direct consent from the data subject, to protect the vital interests of the data subject or another natural person, 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, and in line with the legitimate interests of the controller or a third party. Clarity on the legal basis for each collection and processing is essential because of the follow-on implications and linked requirements. For example, if the data subject requests erasure at some point in the future, this must be accommodated unless the legal basis for the original collection and processing overrides the erasure request. Similarly, any additional processing beyond the original purposes requires a contextual balancing of interests between the data subject and data controller.

- **You cannot reveal sensitive data about individuals**
  Data controllers and processors must avoid processing of special categories of personal data, such as understanding political opinions, determining racial or ethnic origin, determining religious or philosophical beliefs, determining trade union membership, health data, uniquely identifying a natural person through genetic or biometric data, or data about a person's sex life or sexual orientation unless one of ten exclusions apply to the general prohibition (Article 9). These exclusions include ensuring rights of employees, explicit consent, protecting vital interests, and when the data in question has clearly been made public by the data subject, among others. If any of these special categories of personal data will be processed, a DPIA is likely to be required (Article 35), the supervisory authority may need to be consulted in advance (Article 36), and the Data Protection Officer for the organization should be explicitly involved (Articles 37-39). In short, the processing of special categories of personal data is prohibited unless an exclusion is used.

- **You must play nice with other data controllers**
  Data controllers and processors must work jointly and transparently when determining the purposes and means of processing. This includes being very clear about which responsibilities each holds under GDPR (Article 26). Data subjects can be informed of any arrangements, but they retain full rights against each controller separately.

- **You must ensure that your partners are also compliant with the GDPR**
  It is essential 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 adequate data protection. Data processors now have direct specific obligations under GDPR, but data controllers cannot avoid their obligations if things go awry. A contractual agreement between the data controller and processor must be put in place.

- **You must pseudonymize and encrypt personal data**
  Data controllers must protect personal data using appropriate organizational and technical measures, informed by a risk assessment to the processing of that personal data. Pseudonymization and encryption are two of the specific approaches mentioned in the GDPR that offer strong (albeit not failsafe) data protection. These approaches are recommended, but not required, along with other measures like processing system confidentiality, integrity and resilience, and a regular program of testing the designated security measures (Article 32).

- **You must have a Data Protection Officer**
  You must appoint a Data Protection Officer who has expert knowledge in the field of data protection. This personal must be able to inform and advise the data controller or processor about their data protection obligations (Articles 37-39). He or she is to be involved in all issues related to protecting personal data, be available to data subjects for the exercise of their rights, and be accessible to the Supervisory Authority as a liaison for the organization. Specific tasks of the Data Protection Officer include:

  - Informing and advising the organization and employees involved in processing of their responsibilities under GDPR.
  - Monitoring compliance.
  - Providing advice on data protection impact assessments.
  - Cooperating with the Supervisory Authority (Article 39).

  The Data Protection Officer must have the freedom to carry out his or her responsibilities without interference, and is to report to the highest management

It is essential that any data processor used by a data controller is compliant with the GDPR.

level of the controller or processor (Article 38). He or she must not be dismissed or penalized by the controller or processor for carrying out their required tasks.

- **You must have a representative in the European Union**
  Data controllers and processors 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 requirement 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)). This individual must be designated in writing, and he or she must 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.

What if You Don't Comply With the GDPR?

The GDPR has two tiers of administrative fines for non-compliance (Article 83) with key provisions of the law. These 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 violations of the GDPR 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 larger fine is up to €20 million or four percent of total worldwide annual turnover, whichever is higher, and is reserved for infringements like 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 private right of action against any organization that fails to process their personal data properly, does not ensure their rights are met, or fails to ensure adequate organizational and technical safeguards are in place to protect their personal data.

In addition to the significant penalties for non-compliance with the GDPR, it is important to note that there are also non-financial penalties that can create significant problems for an organization that violates the provisions of the GDPR. For example:

- Any Supervisory Authority has the power to impose restrictions or even stop a particular process, implement a remediation program, and then require frequent audits going forward.

- Investigation by a Supervisory Authority will cause significant disruption in an organization, creating further financial impact, loss of confidence from customers, stakeholders and employees. It may also impact shareholders' support and the share price for a public company. Moreover, there is the added

risk of the auditor finding "other" issues that may require further investigation and remediation.

THE POTENTIAL FOR ABUSE OF THE GDPR

One of the real dangers that organizations face in the context of GDPR compliance is potential abuse of the SAR process. As we have seen following the shooting at Stoneman Douglas High School in Parkland, Florida, or during the Occupy Wall Street movement, activists will sometimes call for boycotts of various organizations or general strikes. It is not inconceivable that an activist or activist organization could seek to harm a target organization by organizing followers into submitting SARs en masse. An organization that received 10,000 SARs on a single day, for example, could be overwhelmed without the proper processes and technology solutions in place, and could run afoul of the GDPR requirement to provide this information in a timely manner.

What Systems and Technologies Should You Deploy?

There are a number of systems and technologies that organizations should deploy to become compliant with the GDPR among which are the following:

ARCHIVING AND BACKUP

Archiving solutions index and migrate data to secondary storage, reducing the volume of current data in production systems, while still providing a mechanism for authorized individuals to access relevant data for purposes of their day-to-day work. Archiving solutions must be compliant with GDPR, 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.

While organizations must continue to follow best practices for backup, the GDPR potentially increases an organization's risk depending on how backups are produced. An integrated archive and backup strategy is essential to ensure that only a single instance of data is stored for both. Moreover, cloud-based archiving and backup solutions may offer some advantages here because of their speed of implementation, an important consideration given that the GDPR will implemented very soon.

There are a number of systems and technologies that organizations should deploy to become compliant with the GDPR.

DATA CLASSIFICATION

Data classification tools offer a method for analyzing all data stores and sources in the organization so that personal data can be appropriately classified. This extends into usually difficult-to-find data locations like backups, copies, exports, and shadow IT cloud services that employees may be (and probably 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., delete, migrate or protect in place). Another important consideration is the selection and use of review tools that will help decision makers to sift quickly through large volumes of information.

DATA LOSS PREVENTION

Data loss prevention (DLP) tools analyze the flows of data in email and other systems to identify the presence of personal data using pattern-matching and other advanced forms of classification and identification. Using DLP tools, data that is not properly protected – such as an unencrypted spreadsheet with sensitive data that is sent as an email attachment – can be blocked, quarantined or forwarded to someone like a compliance officer. 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

The encryption of personal data adds a strong level of data protection by using a mathematical code to scramble content into an unintelligible string that lacks any meaning and cannot be deciphered without a decryption key. Encryption is explicitly mentioned as a data protection safeguard in the GDPR, since most data breaches can be prevented if encryption is used. For example, if a data breach does occur, 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. Similarly, most data breach notification requirements in the United States include a provision that the loss of data encrypted does not constitute a data breach.

IDENTITY ACCESS AND MANAGEMENT

Providing global access to sensitive information is a critical problem in many organizations, since 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 always essential, but is very 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

As with encryption, pseudonymization obfuscates personal data values by rendering them unintelligible to anyone without the appropriate access rights. Unlike encryption, however, pseudonymization achieves this by replacing personal data values with a code that can be used to look up the original values that are stored separately in a secured database. Pseudonymization is another technology explicitly mentioned in the GDPR, although it is not without risk, such as might be the case with unauthorized reversal of the pseudonymized data. However, in production systems, test and development environments, and data archives, pseudonymization offers a recommended way of protecting personal data.

SECURITY

Endpoint, server, gateway and cloud security solutions analyze the integrity of network resources, endpoint devices, and cloud services to identify unauthorized access attempts, unwanted types of data like 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 because of nefarious applications working quietly in the background to exfiltrate data, and can provide rapid awareness of an active breach attempt. The right 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, cryptomining malware 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 in order to satisfy the requirements of the GDPR.

APPLICATION SECURITY TESTING

As noted earlier, the GDPR requires that data protection be "by design and default", and application security testing tools help deliver this mandate by analyzing applications for vulnerabilities. Once identified and cataloged, 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 a system.

DATA PORTABILITY CAPABILITIES

Also as noted earlier, data subjects have the right of data portability, whereby 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.

OTHER TECHNOLOGIES

The list above include the high-priority technical measures that will help with GDPR compliance. Complementary technical measures include:

- Incident response systems that can quickly 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.
- Mobile device management solutions that can remotely wipe or kill a compromised or lost device in order to prevent a breach of data. These tools also provide a real-time dashboard on the data protection health of the device fleet, and can enforce local settings like encryption and the use of endpoint security software.
- Privileged account management analysis tools 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 an important attack vector for hackers and other actors with malicious intent.
- 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.
- Process mapping tools document how processes with personal data work, where the data resides, who interacts with it and how it is shared.
- Behavior analytics can provide early warning of developing patterns that show unusual or unsanctioned behavior by employees. These tools could give early warning signals of a data breach, for example. They can also highlight impossibly valid situations, like an employee being logged into two devices simultaneously on opposite sides of the world, which would strongly indicate account credential compromise.

Conclusions

The GDPR is a monumentally important data protection requirement that will impact virtually every organization, whether or not they have operations in the EU. There are numerous requirements imposed upon organizations that maintain information on residents of the EU, and these obligations may be difficult to satisfy and onerous to maintain. However, complying with the GDPR will yield enormous benefits for any organization that gets it right and will have spillover benefits in the context of eDiscovery, compliance with other regulatory obligations, proper data management, and overall reduction of risk from data breaches.

The GDPR is a monumentally important data protection requirement that will impact virtually every organization, whether or not they have operations in the EU.

How Druva Enables GDPR Compliance

As only the cloud-native data protection SaaS offering in the market, Druva spends a lot of time thinking about how to solve compliance-related issues like the GDPR by leveraging the power of the public cloud. Here are some **key points to keep in mind when it comes to leveraging Druva Cloud Services to meet your organization's GDPR compliance goals.**

Data Visibility
To secure information and be compliant with GDPR, organizations have to have visibility into where data lives. Druva gives organizations the ability to protect, collect, and monitor data on endpoints, servers, and cloud applications across the global enterprise. This broad visibility provides organizations with an actionable understanding of their overall data-attack surface and delivers real-time information on how best to deploy security mechanisms to be compliant with the GDPR.

Information Governance
GDPR requires a holistic approach to protecting personal data and providing EU residents with access to that data. Traditional governance has focused on forcing data centralization, which only provides visibility into information that is stored centrally. With the decentralization of data creation on mobile device and cloud apps, organizations need to take a different approach to govern that data as part of developing an effective governance process. Druva leverages the cloud to allow organizations to easily centralize data source policy management and enforcement to bring in decentralized data under the control of GDPR compliance.

Regular Data Monitoring
GDPR requires data processors and controllers to monitor the content, location and use of EU resident information no matter where it lives. With Druva, organizations can automate the process of proactively monitoring information for compliance violations whether that data is on a traditional endpoint or in a cloud application.

Secure the Transfer
With GDPR, security must move with the data no matter where it resides. The Druva Cloud utilizes industry-leading standards based on TLS 1.2 and AES 256 encryption with unique keys for each customer as well as simplified and integration key management. Druva can also prevent data from leaving the EU in the event that organizations have not yet established acceptable transfer mechanisms.

Right to be Forgotten (a.k.a. Right to Erasure)
One of the major challenges facing organizations dealing with the GDPR is how to erase information at the request of data subjects in order to purge all data (including backups) and prevent any subsequent processing. According to the GDPR, consent is not permanently binding, and there must be a possibility to withdraw it. While there are some caveats with this provision of GDPR, any lawful requests of erasure have to be processed in a timely manner. Druva provides defensible deletion capabilities to be able to comply with erasure requests, including a robust audit trail to definitively demonstrate that the information was deleted.

Big Takeaways
GDPR is All About the Data Not just protecting data, but actually knowing where all your organizational data resides. It will be critical that organizations manage the full visibility, access, control, and ultimately erasure of all personal information for EU citizens. When it comes to fines and punitive damages, the GDPR does not discriminate between traditional client/server infrastructure versus modern compute capabilities such as cloud applications and mobile devices. Therefore, not knowing where data resides will no longer be a valid excuse, in fact, it may result in a direct violation. Any technology solution that attempts to enable GDPR compliance must focus on being able to see all data, classify all data, and secure all data.

www.druva.com
@druvainc
+1 800 375 0160
info@druva.com