IMPERVA®

SOLUTION BRIEF

Five Ways Imperva Helps You with GDPR Compliance

Imperva helps simplify preparation for GDPR and address data discovery and classification, pseudonymization, security of processing, breach detection, and data transfer requirements

Overview

The new EU General Data Protection Regulation (GDPR) adopted in 2016 will soon make a significant impact across the world, as enforcement starts on May 25, 2018. It requires all organizations that do any business in the EU or that collect or process personal data originating in the EU to comply with the regulation. Organizations are not exempt from the GDPR simply because they do not have a physical office in the region or do not process personal data in an EU member country. Those that fail to comply can face very strict fines- as much as $22.3 million or up to four percent of total worldwide revenue for the preceding financial year, whichever is higher.

While the GDPR is a lengthy 88-page document, Imperva has summarized the key requirements that pertain to data security:

- Article 25: Data protection by design and by default
- Article 32: Security of processing
- Article 33: Notification of data breaches to the appropriate regulator
- Article 35: Data protection impact assessment
- Article 44: General principle for data transfer

To help you get started, we have created a whitepaper GDPR: New Data Protection Rules in the EU illustrating detailed requirements under each article. Imperva data protection solutions can help organizations address key GDPR data security requirements. This solution brief explores five ways Imperva can will help ensure the GDPR compliances.

Data Discovery and Classification

The GDPR emphasizes that organizations should exhibit commitment to individuals' data privacy by implementing a *Data Protection by Design*[1] approach, implying organizations need to build privacy and protection into their products, services, and applications. GDPR requires that organizations create and maintain a detailed inventory of personal data, and then classify that data by assigning a risk profile and priority.

To achieve this requirement, the first step is to understand **where** databases are located and **what** type of information they hold. Imperva SecureSphere finds both known and unknown databases by automatically scanning enterprise networks. You can easily create custom data discovery policies to scan any part of your network. SecureSphere also enables automated, scheduled scans, as it is critical to ensure continuous discovery to include new data in security and protection efforts. Automated, scheduled scans allow you to develop and maintain an updated inventory of data scattered across your organization.

[1] General Data Protection Regulation Article 25

Once the databases are identified, SecureSphere provides visibility into what personal data your organization holds and processes. It locates various data types by default, such as financial transactions, credit card numbers, Personally Identifiable Information (PII), system and application credentials, and more. Imperva leverages multiple methods to classify sensitive data and assign risk profile, enabling rapid and holistic identification of sensitive data. Knowing what personal data lives in which databases also helps determine what systems are in scope for GDPR, allowing you to accelerate compliance with several GDPR obligations.

Masking or Pseudonymizing Personal Data

The GDPR requires organizations practice data minimization, which means they collect and use data limited to only what is necessary for a specific purpose, retain it no longer than necessary and limit access to a need-to-know basis. As an example[2], if an insurance company collects personal information for the purposes of issuing a policy, and they now want to analyze this data collected from their clients to improve pricing of policies, they would not be able to do it because the personal data collected for one purpose (e.g., issuing a policy) cannot be used for a new purpose (e.g., creating a database for pricing analysis). However, if the data is pseudonymized or anonymized via data masking, then they could use the masked database for pricing analysis.

Pseudonymized data, according to the GDPR, is data that has been de-identified such that the data cannot directly identify the subject. Imperva Camouflage pseudonymizes or anonymizes personal data through data masking.

Data masking replaces real data with realistic fictional data that is functionally and statistically accurate. For example, the original data contains a record of John Smith who is 60 years old, and his SSN is 123-44-5555. After the data is masked, it might become Tom White, 56 years old, with a SSN of 747-88-9999. Data masking facilitates processing of personal data beyond original collection purposes. It also limits the spread of personal data beyond "need-to-know" and reduces risk of data breach.

[2] Chapter 6: Data Protection Principles – Unlocking the EU General Data Protection Regulation, White & Case, July 2016

Security of Processing

Making sure that personal data is secure is the cornerstone of the GDPR. It mandates that those handling data, such as data controllers and data processors, need to introduce appropriate technical and organizational measures to secure the data. For instance, some of these measures should include systems and processes to ensure that data remains confidential and protected. Imperva SecureSphere helps you protect data by identifying database vulnerabilities and monitoring database activity.

Database Vulnerability Assessments

The GDPR requires ongoing protection and regular testing and verification of technical and organizational measures used to ensure security of processing. Continuous database vulnerability assessments identifies risks to personal data. Imperva SecureSphere finds those security holes in your databases that attackers can exploit. With a library of over 1,500 pre-defined tests, SecureSphere scans database servers and their OS platforms for vulnerabilities and misconfigurations such as missing patches, default passwords or misconfigured privileges. Custom assessments can also be created. Assessment reports provide concrete recommendations to mitigate identified vulnerabilities and strengthen the security posture of a scanned database server. Additionally, the Imperva RiskSense Vulnerability Manager add-on generates a risk score based on the severity of vulnerabilities and on the sensitivity of the data. Together, you can easily track and manage identified vulnerabilities and prioritize remediation efforts that represent the greatest risk.

Monitoring Data Access Activity

The GDPR requires organizations maintain a secure environment for data processing, making data activity monitoring critical. To comply with GDPR, you need to be able to answer these questions- **Who** is accessing the data? And **how** is data being used?

SecureSphere is a proven data protection solution that provides complete visibility into data activity. It continuously monitors and analyzes all database activity, including local privileged user access and service accounts, in real time. Monitoring and auditing database activity helps ensure that personal data is being used appropriately and being accessed by authorized users. Data monitoring also helps prevent data theft from external attacks like SQL injections and protect against insider threats– malicious, careless, or compromised users. By keeping a watchful eye on the data, you can identify and block suspicious or unauthorized data access before they become breaches.

Additionally, with SecureSphere, you can easily configure custom policies for your environment. Pre-defined compliance and security policies allow you to apply common policy across databases, Big Data, cloud environments and more. SecureSphere monitors all activity without impacting system performance. Its centralized reporting capability enables you to generate and maintain compliance reports across the entire data environment.

Breach Detection and Incident Response

In the event of a personal data breach, the GDPR dictates that data controllers must notify the supervisory authority *"without undue delay and, where feasible, not later than 72 hours after having become aware of it."* If notification is not made within 72 hours, the controller must provide a reasoned justification for the delay.

The biggest challenge is that security teams are overwhelmed with large volume of incident alerts and that truly worrisome incidents get lost in the noise. Imperva CounterBreach leverages advanced machine learning and peer group analysis to prioritize data access incidents that require immediate attention – without security teams needing deep knowledge of the data environment. It analyzes user behavior and data access activities to identify truly worrisome (or dangerous) incidents, reducing the window of exposure.

In order to meet the "72-hour window" requirement, you need to continuously monitor your data environment. SecureSphere monitors data access and collects granular data access details. It documents details that can be used to investigate incidents and breaches – *what happened, when did it happen, what data was compromised, who took/misused the data*. It allows you to produce the necessary information for breach reports to the proper Data Protection Authority (DPA), notify affected data subjects appropriately, and comply with GDPR breach requirements.

Enforcing Cross-Border Data Transfer Policies

The GDPR imposes restrictions on the transfer of personal data outside the European Economic Area (EEA) to ensure that data protection and privacy requirements outlined in the regulation are not undermined. Article 44 of the GDPR prohibits the transfer of persona data beyond the EEA, unless the recipient country can prove adequate data protection.

SecureSphere helps you to enforce requirements outlined in model contracts and Binding Corporate Rules (BCRs). Ongoing database discovery and classification scans ensure new databases and personal data are cataloged and protected. Policies can be created to inspect the database traffic. When policy violations occur, such as unauthorized access, blocking user connections or terminating a transaction can help ensure appropriate cross-border data access and use.

Case Study- Data Across Borders Enforcement

Customer:

A global payment technology solution company

Customer Challenges:

- Have datacenters and DBAs around the world
- New datacenter in Germany is subject to the German Federal Data Protection Act
- Need to control access to German PII and perform PII discovery

Imperva Solution:

- SecureSphere Data Security Solution

Benefits:

- Protect PII from access by DBAs outside Germany
- Satisfy Data Protection Act requirements
- Provide meaningful and actionable data
- Schedule PII scans for ongoing data discovery and classification

Table: Mapping Key GDPR Requirements to Imperva Data Security Solutions

ARTICLE	WHAT IT MEANS	REQUIREMENTS FOR DATA SECURITY	IMPERVA SOLUTION
25: Data protection by design and by default	Implement technical and organizational measures to show consideration and implementation of Data Protection Principles and appropriate safeguards	• Data minimization • User access limits • Limit period of storage and accessibility	Camouflage SecureSphere
32: Security of processing	Implement appropriate technical and organizational security controls to protect personal data against accidental or unlawful loss, destruction, alteration, access or disclosure	• Pseudonymization and encryption • Ongoing protection • Regular testing and verification	Camouflage SecureSphere CounterBreach
33 and 34: Data breach notification	72 hour notification to Data Protection Authority following discovery of data breach, and notification to affected individuals	Breach report that includes: • what happened • numbers of affected individual • what data was breached	SecureSphere CounterBreach
35: Data protection impact assessment	Assessment of the purpose, scope and risk associated with processing personal data	Inventory of personal data across organization, access rights to data, and risk associated with that access	SecureSphere
44: Data transfers to third country or international organization	Permit transfers only to entities in compliance with GDPR regulation	Monitor and block access to entities or regions that do not meet requirements	SecureSphere

Summary

Without doubt, the GDPR will impact much of the organization– from IT, legal, marketing, customer service, to even HR. While the scope of impact may be large, there is still time for you to prepare for the new regulations. Imperva can help you accelerate compliance with several GDPR obligations, including data discovery and classification, data minimization and pseudonymization, security of processing, breach detection and notification, and data across borders enforcement. With Imperva, you have the visibility into who is accessing what data, and when.