Zaperon

WHITEPAPER

GDPR Cybersecurity Compliance Made Easy With Zaperon



Introduction

As businesses undergo digital transformation, the urgency for businesses to implement rigorous personal data protection measures has intensified. According to a Gartner report, an estimated 75% of data breaches in organizations result from inadequate management of identities, access, and privileges to IT systems that manage personal data of people, a significant increase from 50% in 2020. The **General Data Protection Regulation (GDPR)** was launched in May 2018 as a result to safeguard the personally identifiable information (PII) data of EU citizens and is now a global standard for how organizations handle data security.

GDPR outlines stringent requirements to secure individuals' privacy rights, urging organizations to adopt robust measures against data breaches and unauthorized access. Non-compliance can result in hefty fines of up to 4% of global annual turnover or €20 million, whichever is higher, making it one of the strictest privacy laws globally. GDPR mandates organizations to obtain explicit consent from people before collecting their personal data, ensure data protection by design and by default, and report data breaches within 72 hours.

75%

of data breaches in organizations result from inadequate management of identities

Source: Gartner Report



Understanding GDPR

GDPR is an EU law that enhances data protection and privacy for individuals. Enacted in May 2018, it gives people more control over their personal data and imposes strict rules on how organizations collect, store, and use their data. With its 99 articles, the GDPR sets comprehensive standards for data protection. These articles are organized into several key chapters, each addressing different aspects of data protection.

Amid rapid technological advancements, the GDPR's seven core principles ensure a more rigorous and ethical approach to handling personal data, fundamentally changing how organizations manage and protect information.

7 CORE PRINCIPLES OF THE GDPR

PRINCIPLE	DESCRIPTION
Lawfulness, Fairness, and Transparency	Process data legally, fairly, and transparently.
Purpose Limitation	Collect data for specified, legitimate purposes only.
Data Minimization	Collect only necessary, relevant, and adequate data.
Accuracy	Keep data accurate and updated, correcting inaccuracies promptly.
Storage Limitation	Retain data only as long as necessary for intended purposes.
Integrity and Confidentiality	Ensure data security against unauthorized access and damage.
Accountability	Demonstrate compliance with all GDPR principles.

Who Needs to Comply?

OPERATE WITHIN THE EU

Any company or organization, regardless of its size, that processes personal data of individuals residing in the EU is required to comply with GDPR. This regulation applies broadly to all entities, including businesses of any scale, non-profit organizations, public authorities, and other types of organizations that handle personal data.

SERVE EU RESIDENTS

Companies based outside the EU that offer goods or services to individuals within the EU or monitor their behavior, such as through website tracking, are also subject to GDPR. This includes various types of companies, such as e-commerce businesses, social media platforms, and any other organizations that interact with EU citizens or residents.



Consequences of Non-Compliance

FINANCIAL PENALTIES
Fines up to €20 million or 4% of Global Turnover.

REPUTATIONAL DAMAGE
Tarnished reputation and lost trust.

LEGAL CONSEQUENCES
Risk of litigation and Compensation Claims.

LOSS OF DATA SUBJECT RIGHTS
Organizations May Lose the Ability to Process Personal Data.

BREACH NOTIFICATIONS
Mandatory Notifications Incur Additional Costs.

OPERATIONAL RESTRICTIONS
Limitations on Business Activities.

In May 2023, the Irish Data Protection Commission (DPC) imposed a historic **€1.2 billion** fine on Meta for transferring European users' personal data to the US without adequate protection.

Meta

Marriott INTERNATIONAL

The British ICO fined Marriott International **€20.4 million** for a data breach exposing 339 million guest records, including seven million from the U.K., exposing names, email addresses, phone numbers, passport numbers, and more.

GDPR Compliance with Zaperon's Identity Protection Platform 2.0

Zaperon's Identity Protection Platform 2.0 provides a robust framework, ensuring GDPR compliance that is crucial for protecting personal information.



LEAST PRIVILEGE ACCESS

GDPR requires personal data to be minimized and only necessary data collected and processed. Zaperon enforces this by implementing least privilege access that is a core principle of zero trust security, granting users permissions essential only for their roles, thus reducing the risk of unauthorized access. Additionally, **Zaperon centralizes the management of all access and authorization data, preventing data from being stored in multiple locations or copies**. This approach not only facilitates timely deletion of user account information—avoiding risks from orphaned accounts—but also ensures compliance with GDPR's data minimization principles and enhances overall data security.



AUTHENTICATION

Strong authentication mechanisms are crucial for verifying the identity of users accessing sensitive data under GDPR. **Zaperon employs PKI-based passwordless authentication and assigns a unique certificate to each user device, ensuring that only verified identities gain access to sensitive customer data**. By continuously monitoring device posture, Zaperon further adds an extra layer of protection by making sure that only secure devices are used to access corporate resources, aligning with GDPR's data integrity and confidentiality requirements.



ACCURACY

GDPR mandates that personal data must be accurate and, where necessary, kept up to date. **Zaperon ensures this by utilizing real-time synchronization with Active Directory/LDAP databases. This system automatically updates workforce and customer data, minimizing the risk of outdated or incorrect information**. Additionally, Zaperon promptly corrects or deletes any inaccurate data as soon as it is identified, fully aligning with GDPR's accuracy requirements and ensuring data integrity.



STORAGE LIMITATION

GDPR requires that personal data be kept in a form that permits identification of data subjects for no longer than necessary. **Zaperon adheres to this principle by implementing automated alerts for inactive or less active users, prompting administrators to delete or reconfigure misconfigured/inactive accounts**. This proactive approach ensures that personal data is only retained as long as needed for its intended purposes, thereby reducing unnecessary data storage and complying with GDPR's storage limitation requirements.

AUDIT LOGS

Maintaining comprehensive audit logs to track access to personal data is a fundamental GDPR requirement. **Zaperon provides detailed audit logs of application access that record access times and context-based parameters such as location and device used**. These logs are invaluable for detecting unauthorized access and conducting forensic investigations when anomalies are found, ensuring accountability and compliance with GDPR.

MULTI-FACTOR AUTHENTICATION (MFA)

GDPR emphasizes the need for enhanced security measures to protect personal data. **Zaperon Identity Protection 2.0 provides the most secure and phishing-resistant MFA that validates 15+ factors related to device certificates, user behavior, device posture and context, before authorizing access to application data**. This multifaceted approach ensures that the sensitive data remains uncompromised, adhering to GDPR's data protection principles.

INSIDER THREAT MONITORING

According to Verizon's Data Breach Investigations Report, human error is a factor in over 80% of data breaches. With combination of least privilege access, device trust, multi-factor authentication and continuous monitoring of user behavior, Zaperon ITDR eliminates the insider threat. **Zaperon prevents misuse of access and ensures the security of personal data by responding promptly to suspicious activities**. This aligns with GDPR's emphasis on protecting personal data from both external and internal threats.



Zaperon Identity Protection 2.0

PKI-POWERED PASSWORDLESS AUTHENTICATION

Utilizes PKI for secure, password-free access, reducing data breach risks from compromised credentials.

PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION

Implements MFA resistant to phishing attacks, enhancing security with a variety of over 15 factors.

CONTINUOUS ZERO TRUST ACCESS MANAGEMENT

Applies ongoing zero trust policies based on user behavior and device status, ensuring consistent security and compliance.

PROACTIVE DETECTION AND RESPONSE TO IDENTITY THREATS

Proactively identifies anomalies and manages identity threats, minimizing security incident risks.

COMPREHENSIVE IDENTITY SECURITY

Integrates proactive threat detection and response for robust protection of users, devices, applications, and cloud infrastructure.

Zaperon transforms identity protection with its advanced platform, safeguarding organizations against identity-based threats. Using PKI-based passwordless access and phishing-resistant multi-factor authentication, it upholds continuous zero-trust policies informed by user behavior and device posture. With proactive identity threat detection and response, Zaperon ensures robust security for users, devices, applications, and cloud infrastructure.

+1 202 600 5234
+91 8800 170387
sales@zaperon.com
www.zaperon.com
© 2024 Zaperon, Inc.
All Rights Reserved.