COMPLIANCE GUIDE

How Zero Networks Helps with GDPR Regulation Requirements

Organizations operating within the EU or handling the personal data of EU residents must comply with the General Data Protection Regulation (GDPR) by implementing strong technical and organizational safeguards to protect data privacy and security. Zero's identity-informed microsegmentation empowers organizations to meet these requirements by delivering precise, context-aware access controls and enhancing the ability to audit data access and activity.

GDPR Requirement	Description	How Zero Helps
Article 5 & 32: Security of Processing	Organizations must process personal data in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organizational measures.	Zero Networks' automated, identity-informed microsegmentation enforces strict access controls and network segmentation, ensuring only authorized users and devices can access sensitive data. Identity-based policies dynamically adapt to user roles and behaviors, minimizing the risk of unauthorized access or data breaches by restricting lateral movement and limiting the attack surface.
Article 25: Data Protection by Design and by Default	Organizations must implement data protection measures into processing activities and information systems from the outset, ensuring that, by default, personal data is not accessible to an indefinite number of people.	Zero enforces the principle of least privilege, isolating personal data and restricting access based on user roles, attributes, and operational needs. This supports "data protection by design and by default" by ensuring only necessary access is granted and automatically adapting as user roles change.
Article 33: Notification of a Personal Data Breach	In the event of a personal data breach, organizations must notify the supervisory authority without undue delay and, where feasible, within 72 hours.	By instantly containing breaches within specific network segments and only providing asset access to predetermined identities who pass MFA, Zero Networks greatly limits the scope and impact of incidents. This, combined with detailed audit trails, enables organizations to quickly assess, respond to, and report breaches as required by GDPR.
Article 28: Processor Security	Organizations must ensure that any third-party processors implement appropriate technical and organizational measures to meet GDPR requirements.	Zero enables organizations to automatically create and enforce security policies that control and monitor third-party access to network assets with granular identity-based controls. This ensures processors only access essential resources and that all access is logged and auditable, supporting GDPR's processor accountability requirements.
Article 30: Records of Processing Activities	Organizations must maintain records of processing activities, including details on data access and security measures.	Zero Networks provides granular, identity-based audit trails for every access attempt to assets, which supports comprehensive record-keeping and facilitating compliance with GDPR's documentation requirements.

Article 24: Responsibility of the Controller	Controllers must implement appropriate technical and organizational measures to ensure and demonstrate that processing is performed in accordance with GDPR.	Zero's automated, policy-driven, identity-informed microsegmentation demonstrates proactive data protection and risk management, helping organizations fulfill their accountability obligations under GDPR.
Article 29: Processing Under Authority of the Controller or Processor	Personal data must only be processed on instructions from the controller, including ensuring that persons authorized to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.	Zero ensures that only authenticated and authorized users can access or process personal data, with dynamic enforcement of access policies based on identity, role, and context. This supports strict adherence to controller instructions and confidentiality requirements.
Article 35: Data Protection Impact Assessment (DPIA)	Organizations must assess the impact of processing operations on the protection of personal data, especially when using new technologies.	Identity-based microsegmentation provides detailed visibility into data flows and user access, supporting effective DPIAs by demonstrating how access is restricted and monitored, and by providing evidence of risk mitigation measures.

Key Zero Capabilities that Support GDPR Compliance:

- **Identity-Informed Microsegmentation:** Zero segments the network based on user, device, and application identity, enabling context-aware access controls that adapt to changing roles and behaviors.
- **Granular Access Controls:** Enforces least privilege and prevents unauthorized lateral movement within the network, with policies dynamically tailored to identity attributes.
- **Comprehensive Audit Trails:** Logs all access attempts and user actions for compliance and forensic investigation, providing clear evidence for audits.
- **Rapid Incident Containment:** Limits the impact of breaches and supports timely breach notification by containing threats at the identity and host level.
- **Third-Party Access Management:** Controls and monitors access by processors and service providers with identity-based policies, ensuring GDPR alignment.
- **Dynamic Policy Adaptation:** Zero continuously reviews and updates access rights as user roles or organizational needs change, reducing the risk of stale permissions and privilege creep.
- **Enhanced Support for DPIA and Accountability:** Provides detailed visibility into who accesses what data, when, and under what circumstances, supporting DPIA and demonstrating GDPR compliance.

Connect with the Zero Networks team to discover how automated, identity-informed microsegmentation can streamline your GDPR compliance and strengthen your data protection posture.

Request a demo

ZERO Networks