ALERT LOGIC®

SOLUTION BRIEF:

ALERT LOGIC® FOR GDPR

INTEGRATED SECURITY FOR GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR FOR THE ORGANIZATION

If your organization collects, controls or processes personal information of citizens in European Union (EU) countries, you must comply with the GDPR.

Any organization that processes EU citizen data—even those without a business presence in the EU—are subject to GDPR rules and penalties of non-compliance.

Organizations not in compliance are subject to penalties of up to €20 million or 4 percent of global annual turnover, whichever is higher.

GDPR FOR THE SECURITY PROFESSIONAL

Most of the GDPR requirements concern processes, policies, and documentation. Unlike mandates such as PCI DSS or ISO-27001, there are no prescriptive, detailed security controls. For security planning, the GDPR provides a risk-based approach to ensure that measures implemented provide a level of security appropriate to the risks.

Most security professionals will focus on Article 32, which represents the main provision requiring technical measures for data protection. Other GDPR Articles to address include Articles 24, 25, 33, 34 & 35 that establish risk-based design principles, and security related obligations and processes enabled by Article 32.

HOW ALERT LOGIC CAN HELP

Alert Logic® Cloud Defender® makes it easy for security professionals to implement the GDPR technical control requirements found in Articles 24, 25, 32, 33, 34 & 35 with an integrated suite of security capabilities combined with 24x365 managed detection and response services.

SAVE MONEY

Single Integrated Solution
Suite of Security Capabilities
One Monthly Subscription

STAFFING RELIEF

Our Experts are Included
24x7 Threat Monitoring
15-Min Live Notifications

START FAST

Ready-to-Use Services
Expert Onboarding Assistance
Personal Tuning & Training

INTEGRATED SECURITY FOR THE GENERAL DATA PROTECTION REGULATION (GDPR)

The integrated services that make up Alert Logic® Cloud Defender® help you implement the technical measures needed to comply with GDPR Articles 24, 25, 32, 33, 34 and 35 to help you:

- Reduce your attack surface to prevent unauthorized access by finding vulnerabilities and risky configurations before your adversaries do
- Ensure encryption of personal data is in force by identifying and alerting on missing, disabled, misconfigured encryption mechanisms
- Receive 15-minute personal notifications on high- and critical-incidents that threaten the confidentiality, integrity, and availability of protected data from analysts in our 24x7 Security Operations Center (SOC)

ARTICLE 24

Responsibility of the controller

WHAT IT SAYS

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

WHAT IT MEANS

The controller is responsible for implementing and documenting what they are doing to comply with GDPR (policies, training, procedures, technical controls.

HOW WE CAN HELP

From day one, Cloud Defender enables your team with reports and documentation that:

- Establish the scope of technical measures included to secure protected data included with Alert Logic services (scope of service, service description, overview of environments included), service escalation plans for high- and critical-events
- Service activation documentation
- Executive and detailed threat and vulnerability reporting to demonstrate implementation of security technical measures, incident responses, remediations and more

ARTICLE 25

Data protection and design by default

WHAT IT SAYS

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

WHAT IT MEANS

Using process, design, and technology strategies, you should protect personal data at the at the earliest stages of the design process. For example:

- Only the data necessary should be processed, and it should be stored for a short period of time, with limited and controlled access
- Data that is used should be encrypted and/or pseudonymized (replaced with realistic fictional data while maintaining usefulness and accuracy)

HOW WE CAN HELP

Help your team use assessment, detection, and alerting capabilities included with Cloud Defender to identify systems that fall out of compliance with designed protections such as:

- Identify encryption issues in your applications and deployments
- Check access controls and privilege settings for excessive permissions and unusual changes
- Continuously monitor outbound traffic that might contain personal data

ARTICLE 32

Security of processing

WHAT IT SAYS

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.

WHAT IT MEANS

You should make efforts to keep protected data secure, including:

- Identify and fix vulnerabilities and risky configurations that attackers can exploit
- Encrypt protected data when it cannot be pseudonymized
- Monitor all network traffic to identify potential threat activity
- Inspect all web application traffic to detect suspicious activity
- Collect log data from all systems to identify anomalies, and enable post-compromise forensics

HOW WE CAN HELP

Work with your team to deploy and customize Cloud Defender to protect user data in on-premises, hybrid, and cloud environments with:

- **Continuous vulnerability scanning** to identify software and application vulnerabilities, risky configurations, systems with encryption issues
- **Distributed network intrusion detection systems (IDS)** to identify potential threat activity including: data exfiltration, brute force, privilege escalations, and command and control exploits
- **Automated log Management** collection and analysis to look for indicators of compromise, suspicious behaviors, or support incident response forensics
- **Web application monitoring** to identify and respond to suspicious application transactions, user behavior, and unusual transmission of personal data
- **Managed Web Application Firewall** to block OWASP Top 10 and dozens of other attack classifications—tuned and managed daily by application security specialists (Web Security Manager™ Premier subscription required)

ARTICLE 33

Notification of a personal data breach to the supervisory authority

ARTICLE 34

Communication of a personal data breach to the data subject

WHAT IT SAYS

Article 33 - GDPR requires organizations to report a breach to the supervisory authority within 72 hours of awareness.

Article 34 - When the breach is likely to result in a high risk to data subjects, the data subject must be notified without undue delay.

Taken together, Articles 33 and 34 address the way that organizations should communicate breaches. The notification should include the nature of the breach, measures taken to address the breach and prevent future occurrences.

WHAT IT MEANS

You should have a plan to:

- Detect and respond to threats that could lead to a data breach
- Identify and stop active breaches
- Implement remediations to prevent recurrence of identified breaches
- Report security issues internally
- Notify authorities of verified breaches with details regarding number of users effected and categories of personal data compromised

HOW WE CAN HELP

The Alert Logic® Security Operations Center (SOC)—included with Cloud Defender—augments your team's data security capacity with cyber security expertise to protect EU GDPR personal data across the full stack of your applications and infrastructures, in on-premises, hybrid and cloud environments.

Our experts will investigate and respond to incidents that could lead to breaches of personal data, 24 hours a day, every day of the year—offloading the high costs of an in-house security staff. Our SOC provides:

- **24x7 Monitoring:** GIAC-certified analysts in our SOC monitor your environments 24x7
- **Incident Reports:** Cybersecurity experts review incidents and enrich with additional information and remediation actions
- **Personal Notifications:** Analysts call, text or email you within 15 minutes of high- and critical-priority attacks

ARTICLE 35

Data protection impact assessment

WHAT IT SAYS

Where a type of processing (in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing), is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

WHAT IT MEANS

You should have a plan to run a Data Protection Impact Assessment (DPIA) prior to turning on new services that store or process protected data, especially if it is likely to result in a high risk to the security of the protected data, and if the data will be used to do profiling/filtering based on that data.

HOW WE CAN HELP

Help your team use assessment, detection, and reporting capabilities included with Cloud Defender as part of your DPIA security testing and analysis:

- **Continuous vulnerability scanning** to identify software and application vulnerabilities, risky configurations, and systems with encryption issues
- **Configuration Assessment** to inspect pre-production AWS workloads and services for misconfigurations or overly permissive access that could expose protected data to attack or unauthorized access
- **Intrusion Detection System (IDS) & Log Management** for data-flow and access activity to help produce a systematic description of the processing operations
- **Security and threat reporting** to analyze and document the security posture of tested environments including risk levels, threat details, potential impact and remediation recommendations

Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and maintains strict compliance with internal and external regulatory requirements for our IT operations and services, including: PCI DSS 3.2 Level 2 Audit, AICPA SOC 1 & 2 Audit, and ISO 27001-2013 certification for UK Operations.

ALERT LOGIC®