Hewlett Packard Enterprise

GDPR:

7 questions CIOs must answer to achieve compliance

Time is running short. Enforcement of General Data Protection Regulation (GDPR) begins in May 2018 and penalties are severe: Up to **€20 million or 4%** of the preceding year's worldwide turnover. Don't let GDPR compliance slide to the bottom of your priority list.

Here are the top seven questions to ask yourself now:

1.

What is my readiness status?

- Raise internal awareness now to get resources on board for GDPR implementation.
- Launch a group-wide risk assessment to gauge your company's preparedness level, including technology facilities, under existing National and EU regulation.

What information and personally identified information (PII) will fall under these regulations?

GDPR Articles: 5, 24; GDPR Recital 74

- Information in any format must be addressed: hard copy, audio, visual, and alphanumeric.
- You should be able to unify records to provide a 360-degree view of a private customer.
- Understand data flows—where is sensitive data used and moved between databases and applications.

2.

3.

How can I cost effectively respond to legal matters requiring information under my management?

GDPR Articles: 79, 58; GDPR Recital 122, 123, 143

- Ensure legal policies and procedures are in place to meet requirements.
- Evaluate the technology used to isolate information required by in-house counsel as well as compliance and risk officers.
- Determine whether internal or external counsel will handle breach reporting.

How can I best ensure sensitive data is protected, stored and backed up securely?

GDPR Articles: 6, 32, 33, 34, 83

- Evaluate the effectiveness of my total records management.
- Determine whether my existing backup safeguards PII.
- Review my retention policy enforcement for the defensible deletion of data.

4.

5.

How can I identify information for disposition, in accordance with the "right to be forgotten"?

GDPR Articles: 4, 15-22, 24; GDPR Recital 59, 63-71, 74

- Gain legal advice as to how PII is defined.
- Deploy a policy enforcement tool.
- Establish a process that can be monitored and audited for compliance.

Can I report a breach within the timeline required by the EU data protection regulation?

GDPR Articles 33, 34; GDPR Recital 85, 86, 87, 88

- 72 hours is a tough target to reach. A comprehensive and defensible policy and system needs to be in place.
- The security breach alerting mechanism must be provided in the form of technology-assisted monitoring.
- Well-trained compliance staff is needed to use technology and report as required to national Data Protection Regulators.

6.

7.

How can I reduce my overall risk profile?

GDPR Articles: 5, 24; GDPR Recital 39, 74

- Perform a sound and rigorous risk assessment of policy, procedure, and technology.
- Invest in technology as required to achieve risk reduction.
- Establish both proactive defense and post-event handling to protect corporate reputation and avoid both fines and business-limiting criminal enforcement.

Mitigate penalties and safeguard your brand and business reputation. Let HPE help you manage sensitive information in accordance with GDPR requirements.

Learn more at
hpe.com/info/security

a00026999ENW, September 2017