SOLUTION SHEET

DIGITALGUARDIAN®

Digital Guardian for EU GDPR Compliance

7 DATA PROTECTION CHANGES THAT NEED ATTENTION NOW

The EU General Data Protection Regulation (GDPR) is the most significant new regulation involving a private residents personal information to emerge in many years. The regulation provides the basis for how multi-national organisations and government agencies must protect sensitive consumer data and defines how organisations can derive value from that data.

EU regulators finalized the General Data Protection Regulation (GDPR) in May of 2016 and will begin enforcement in May 2018. No more changes in the law are coming, so there are no more reasons to delay. Here are the changes that security professionals should understand and start addressing now.

1 GLOBAL SCOPE

Any organisation that processes data of EU residents must comply, no matter where they are located or data is stored.

2 BIG FINES

Fines of up to 4% of an organisation's global turnover or €20 million, whichever is higher. This requirement alone is making GDPR compliance a board-level issue.

3 MANDATORY BREACH NOTIFICATION

Data protection authorities must be notified of a breach within 72 hours of its discovery. Where the breach is likely to impact the rights and freedoms of individuals, data subjects must be notified without undue delay. Most security teams will have to react much faster than they do today to meet this requirement.

4 DATA PROTECTION OFFICER

A data protection officer (DPO) must be appointed by companies "engaged in processing of customer data in the regular course of business." Security teams will have to work closely with the DPO to ensure efficient compliance.

5 PRIVACY BY DESIGN

Security can no longer be implemented after the fact or even mid-stream. Security must be built-in, intrinsic—from the ground up.

6 DATA PROTECTION IMPACT ASSESSMENTS

Where data processing could put personal data at high risk, organisations must conduct a data protection impact assessment (DPIA) prior to processing. Security teams will have to detail the security measures and safeguards put in place to ensure compliance.

7 EVIDENCE OF MITIGATION MAY REDUCE FINES

The amount of the fine may be reduced if appropriate measures have been implemented. The ROI on data protection best practices has never been clearer.

DIGITALGUARDIAN®

For more information, visit
www.digitalguardian.com

GDPR COMPLIANCE REQUIRES DATA LOSS PREVENTION

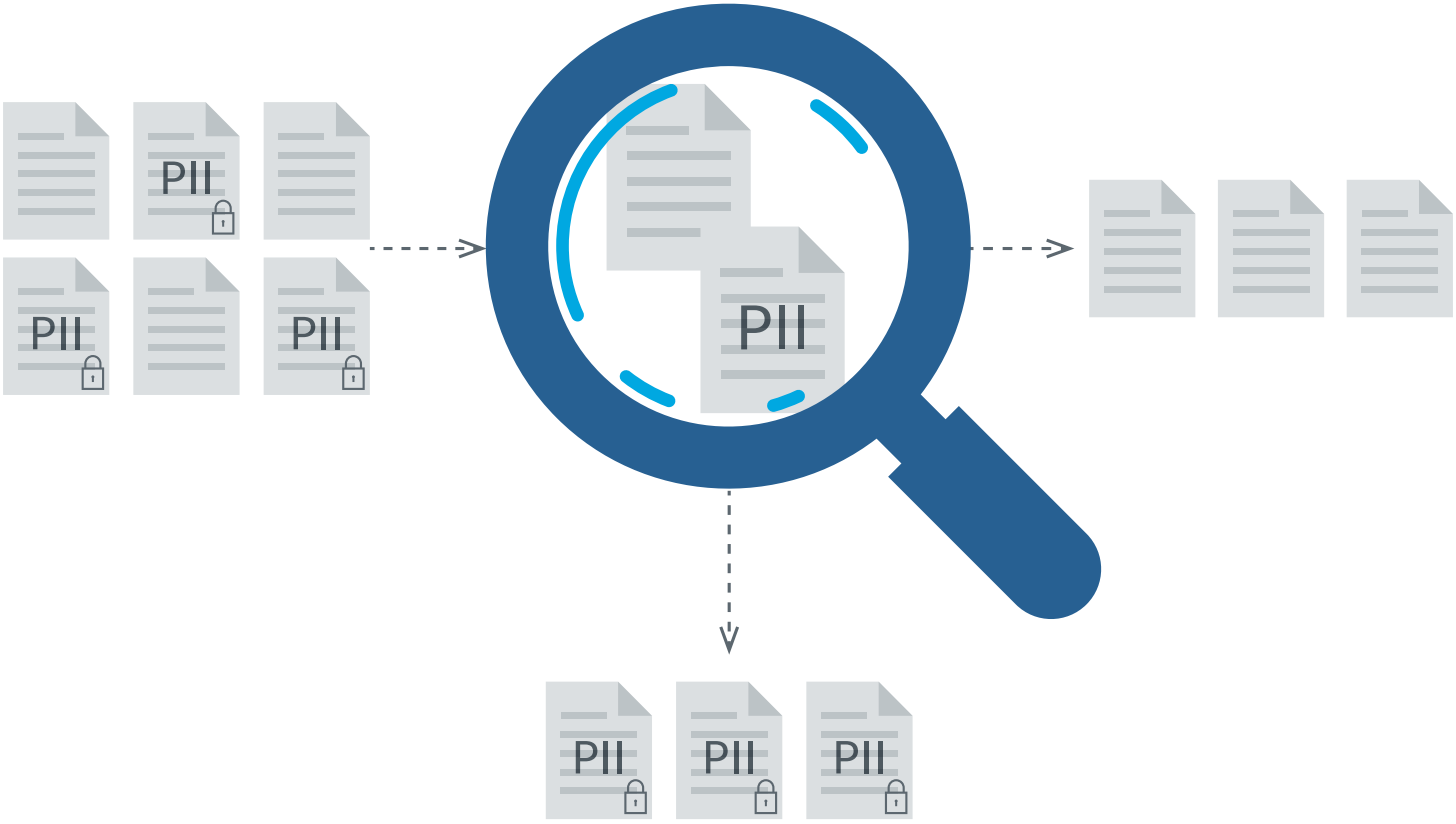
GDPR is not very prescriptive in regard to security technology. It doesn't mention data loss prevention (DLP) anywhere, but logically it requires enterprise DLP to meet the "integrity and confidentiality" principle. Here's why.

At its core, the law requires impacted companies to protect personal data of EU residents against data breaches. For security teams this means you must put in place measures that stop personal data from leaking out - without slowing down business processes.

GDPR REQUIRES A TECHNOLOGY THAT CAN:

- Analyze the content of data transmitted, used or stored in any IT system processing personal data
- Determine which of that data is personal data (PII) that must be protected and classify it as such
- Permit the non-restricted, free flow of all other data
- Apply real-time controls to make sure designated personal data is always safeguarded

CONTENT ANALYSIS



DIGITALGUARDIAN®

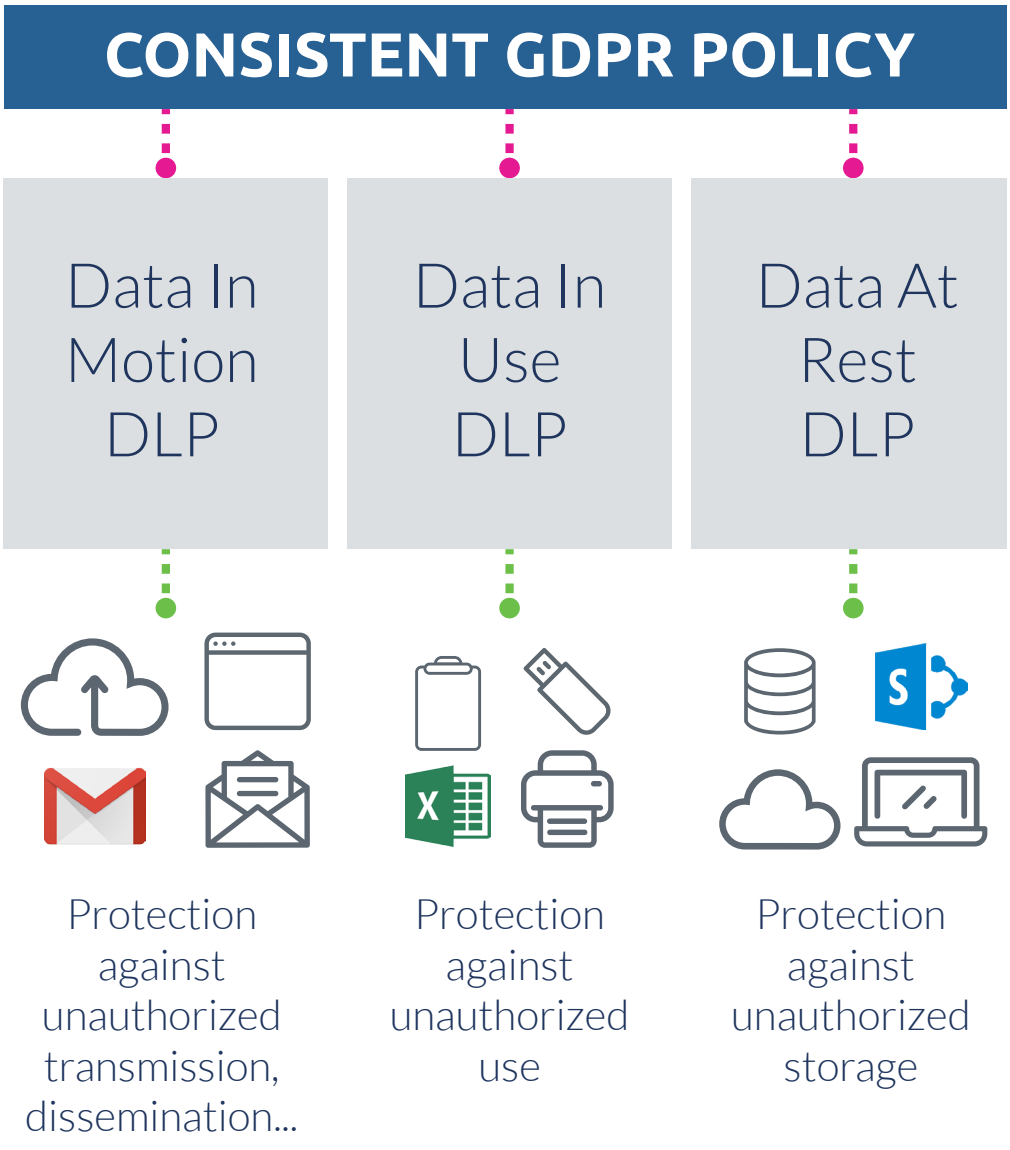
For more information, visit
www.digitalguardian.com

ENTERPRISE DLP FOR CONSISTENT GDPR COMPLIANCE

Enterprise DLP was designed specifically for this purpose – no other technology does it better. And while many security technologies are adding "DLP Lite" functionality, only enterprise DLP can ensure you have consistent, centrally managed GDPR compliant policies across all egress channels – including the cloud.

Enterprise DLP can also play an essential role in meeting the "Privacy by Design" requirement in the law. GDPR "Privacy by Design" mandates that system designers and developers plan for and implement data protection safeguards into any new data processing system that they develop.

With its ability to monitor and control personal data across all elements of a data processing system's architecture – custom applications, IT infrastructure (including general applications, network, email, web browsers, databases, cloud, endpoints) and end-users, Enterprise DLP provides the necessary data protection technology safeguards.



DIGITALGUARDIAN®

For more information, visit
www.digitalguardian.com

WHY DIGITAL GUARDIAN FOR GDPR

Management Console | Data Discovery | Data Classification | Data Loss Prevention | Cloud Data Protection

Digital Guardian believes that data protection products for regulatory compliance don't have to be complex to be effective. Our market-leading DLP solution offers network-based appliances that combine data discovery, data classification and data loss prevention in one powerful, easy-to-manage solution. We can automatically identify GDPR regulated data, which we can then protect in use, in transit and at rest.

1 DEEPEST VISIBILITY ACROSS YOUR ENTERPRISE AND THE CLOUD

Digital Guardian for Compliance enables you to effectively discover, monitor and control EU personal data transmitted on the network, in use on workstations, or at rest in workstations, network servers and cloud storage.

2 ANALYTICS & REPORTING THAT DEMONSTRATE COMPLIANCE

Digital Guardian analytics and reports can provide the key documentation to demonstrate GDPR compliance. Our enterprise wide reporting shows where EU personal data is located, how it's used and what mechanisms you have in place to enforce GDPR data protection principles.

3 FLEXIBLE & AUTOMATED CONTROLS THAT PROTECT DATA WITHOUT SLOWING BUSINESS

Our controls operate silently until needed, then automatically respond to risky behavior. Employees are educated in real-time on the appropriate handling of regulated data via display prompts that request justification for actions that put data at risk. Actions that violate data protection policy are blocked or contained before personal data gets out.

4 EFFECTIVE COMPLIANCE WITH LITTLE OR NO OVERHEAD

Digital Guardian's powerful appliances (physical or virtual) are designed for quick installation and simplified management. Configuration wizards guide you through setup and configuration. Once deployed, our database record matching fingerprinting technology for identifying and controlling personal data is the industry's most accurate, resulting in the lowest false positives. You get full-featured protection with low overhead.

For companies struggling to find the security talent we offer a Managed Security Program for Data Protection Compliance managed by experts who can help you achieve GDPR compliance faster and with greater confidence.

ABOUT DIGITAL GUARDIAN

Digital Guardian's threat aware data protection platform safeguards your sensitive data from the risks posed by insider and outsider threats. By harnessing our deep data visibility, real-time analytics and flexible controls, you can stop malicious data theft and inadvertent data loss.

Gartner®
Magic Quadrant Leader

SHARE