



The GDPR— data just got personal

What it is, what it means –
and how it affects you

The **GDPR** is a game-changer for organizations holding, and protecting, personal, identifiable data on EU citizens.

Because the financial penalties for those failing to uphold data protection, or suffering a breach are so huge, data cyber-risk is no longer ‘just’ an IT problem. The whole organization must prepare – and take responsibility for – data compliance.

This Quick Reference Guide is a topline walkthrough of the key points of the GDPR and its consequences. More help is available.

What is the GDPR?

New rules are needed to protect our increased life online. The new EU General Data Protection Regulation (GDPR) is a big step up from previous legislation.

It means that EU citizens can expect more control of their personal data, and easier access to it. But GDPR compliance means increased assessment and detective controls, and improved data security principles for those holding data.

A brief glossary

IAM	Identity and Access Management
EU	European Union
GDPR	General Data Protection Regulation
IGA	Identity, Governance, and Administration

Why is it happening?

Our life online means our personal data often travels further than we do. When it goes beyond EU borders, the legal lines are blurred. GDPR will bring conformity and increase protection of a valuable commodity that could be worth €1 trillion annually by 2020.

When does it begin?

The GDPR will be enforced from 25 May 2018. The two year implementation period has already begun and local Data Registrars can already impose fines for breaches.

Who does it affect?

- Every EU organization holding personal data.
- Organizations within the EU processing data.
- Any organization, anywhere, holding information on EU citizens.
- Any organization offering goods or services to EU individuals.

But Brexit...?

...will make no difference. The GDPR deadline precedes any potential move and will not relieve companies of their responsibilities.

What's changing?

An overarching principle of stronger protection of personal data. This manifests as increased assessment, preventive, and detective controls, and improved data security principles.

More accountability. Organizations must:

- prove compliance – documenting/recording the principles behind processing decisions.
- implement comprehensive, proportionate governance measures, such as privacy impact assessments and 'privacy by design'.
- report data breaches 72 hours after becoming aware of a data breach

Big penalties for non-compliance or direct breaches.

They include:

- €10 million or 2% of total worldwide annual turnover, whichever is greater, for serious breaches
- €20 million or 4% of total worldwide annual turnover for very serious breaches, whichever is the greater.

What does a data breach look like?

Under the terms of the GDPR, a data breach is a security lapse leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. For example, a hospital could be liable under the terms of the GDPR if a patient's health record is inappropriately accessed due to a lack of appropriate internal controls. For the GDPR, inappropriate data access is as important as loss.

Are you ready?

Probably not. This survey* identified that data protection is not yet a high priority for some organizations. While 67% of organisations said that regulatory and legal compliance was a major driver for investing in privacy, a worrying 63% of respondents admitted their privacy maturity – or readiness – was only at the early or middle stages. The two year implementation period for GDPR has begun, and local Data Registrars can already impose fines for breaches.

Uh oh

A worrying 97% of organizations have no plan to address GDPR and 50% are 'not confident' they will be ready for GDPR in 2018.

While 89% of organizations feel their approach to data security will need to change because of the GDPR, only 8% feel they are already compliant.

The Micro Focus response

Doing nothing is not an option. So use the GDPR as an opportunity – a framework for establishing, or reinforcing, robust data protection and integrity. Successful management of the GDPR transformation is part technology, and part process.

We can help with an expert analysis of your data protection setup. While it does not guarantee compliance it represents a useful pre-GDPR healthcheck that assesses your organization's Identity and Access Management strategies and protections.

It is a useful preparation for the detailed GDPR Data Protection Impact Assessment (DPIA). This will identify any potential personal privacy risks to individuals in processing their data.

GDPR compliance combines knowledge, strategy and technology. Each stage must be addressed chronologically and the correct technology implemented at the right time. Anything less could leave an organization short of their compliance goals.



Micro Focus Identity-Powered Security Capabilities

Security Capabilities	Manage & Govern Rights								Enforce Access Controls					Monitor User Activity					
	Identity Lifecycle Mgmt.	Request Management	Role Management	Access Recertification	SoD Control	Dormant, Rogue & Orphaned Account Control	Active Directory Delegation	Privileged Account Mgmt.	Federation	Single Sign On	Risk-Based Authentication	Multi-Factor Authentication	Super Users Privilege Mgmt.	Shared Account Password Mgmt.	File Integrity Monitoring	Privileged Session Mgmt.	User Activity Monitoring	Security Incident and Event Mgmt.	Reporting and Analytics
Example questions																			
How do you confirm on an ongoing basis that a user's access to personal data is appropriate?			●	●													●		●
How do you know that individuals who do not need access to personal data cannot access it?	●		●	●	●										●		●		●
How do you prevent individuals who do not need access to personal data from accessing it?	●		●					●				●							
How do you protect personal data from the risk of exploited insider credentials?						●					●	●							
How do you protect personal data from inappropriate access by privileged user credentials such as system administrators?								●					●	●		●			

Knowledge:

Our assessment will highlight areas of concern. Addressing them is an important and positive move towards GDPR compliance. Questions might include:

- Can you answer with certainty who has access to personal data?
- How do you distinguish between appropriate users and those with privileged credentials such as systems administrators?
- What personal data do you have, where is it stored – and who can access it?
- Is every user's access to personal data still appropriate – and how do you check?
- Beyond the password and user rights, what controls are protecting personal data?
- How do you protect personal data from exploited insider credentials?

Strategy:

For the purposes of the GDPR, data protection and IAM are almost interchangeable. The basic principle behind the GDPR is data protection, and the strength of an organization's IAM will determine how compliant they are.

An internal decision-making process decides what must be done, and when. It attributes resources to the plan. The Identity Powered Security (IPS) strategy must focus on three key points:

- 1. Manage and Govern Rights:** Micro Focus IGA tools ensure that individuals only have the rights they need. We work with customers to review their compliance on an ongoing basis.
- 2. Enforce Access Controls:** Insider credentials are coveted by hackers¹ So our IAM tools create the right access controls to effectively protect personal data – perhaps with stronger authentication methods
- 3. Monitor User Activity:** Another key consideration is ensuring that users are accessing what they should. Are your privileged users accessing data that they wouldn't normally see? How about everyone else?

Solution:

Protection of personal data is fundamental to GDPR, and can only be delivered when underpinned with effective Identity and Access Management (IAM). IAM is recognised to consist of a number of well-defined and understood capabilities. The table above maps these capabilities to the example questions that organisations need to ask themselves regarding their ability to effectively protect personal data, and comply with GDPR.

Next steps

There is no one-size-fits-all plan or magic bullet that resolves every organization's GDPR obligations. But an integrated strategy harnessing our expertise and product set could future-proof your IT infrastructure from strategic fines that could affect business growth. The first step towards improving your readiness is to check the current status of your IAM infrastructure. Our free Data Protection Assessment will check your processes and technology against the requirements of the GDPR.

^{*}Joint IAPP-EY Annual Privacy Governance Report 2015




¹Source: 2015 Black Hat Hacker Survey



For further information contact us:
Freephone +44 (0) 1635 565 200

Visit our websites
microfocus.com
suse.com

Find us on Social Media

-  facebook.com/microfocuscorp
-  twitter.com/microfocus
-  linkedin.com/company/micro-focus