Asigra.

Recovery is Everything™

Datasheet

Worried About the GDPR? Are you Ready to Comply?

What is the General Data Protection Regulation (GDPR)?

The GDPR is a new set of rules designed to shape, enhance, standardize and centralize unstructured data governance in the EU member states. First proposed in 2012 and adopted in 2016, companies now have slightly over two years to adapt and comply with the new regulation before the deadline of May 2018. Research from content management company Metalogix shows IT professionals in many countries aren't prepared for this new regulation.

Considered now to be the most stringent privacy mandate worldwide, it affects organizations, IT administrators, controllers as well as IT appliances, processors and networks, regardless of their location, that are involved or engaged in data processing activities related to people in the EU.

For Companies who have an Internal IT department:

Under the GDPR, companies are under extreme pressure to keep an inventory of the data they handle – both in-flight and at-rest to ensure that personal data is protected. Whether you're using G Suite, SharePoint or any other cloud SaaS application, make sure data is accessible at any time as failed audits can have devastating effects on companies of any size.

For Companies who use a Managed Service Provider (MSP):

Businesses need to take a much stricter approach when dealing with MSP's as they need to ensure that potential contractors handle data privacy and cyber security in a way that is compliant to the new regulations. As an organization, do your due diligence and question their data handling practices, how they store data, who has access, their encryption policies – essentially anything relevant to how unstructured data is handled and processed.

Asigra.

Recovery is Everything™

Here are some key elements that will have significant impacts on your organization:

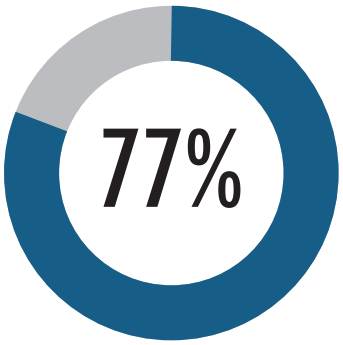
- **Increased Territorial Scope:** GDPR applies to all companies who deal with personal data, regardless if business is conducted physically in the EU.
- **Data Breach Notifications:** The new regulation requires all organizations to report a data breach to Data Protection Authorities within 72 hours/three days of detection.
- **Consent (Rights of Individuals/Data Subjects):** Under the new rules of GDPR, consent must be given before any data collection on websites is performed.
- **Clear and Succinct Communication:** Organizations will have to write their terms and conditions in easily understandable language, not legalese.
- **Penalties/Fines:** Organizations that breach the GDPR can be fined up to four per cent of annual global turnover or €20 Million (whichever is greater).

How Does the GDPR Affect North American Businesses?

To think that GDPR does not apply to non-EU providers and contractors would be a mistake. Globalization has allowed businesses and services to operate across several borders, which means the GDPR is more wide reaching than within the EU territory. It's expected with this new regulation that all organizations who manage their data flows, transfers and processes, have clear documentation and align their business practices to the new regulation.

Many of the new requirements under GDPR are in tandem with the PIPEDA and CASL. If you're a compliant organization, you may already have appropriate practices and policies in place. However, with the sanctions and fees being so high, McMillian LLP states that organizations should:

- Review consent forms for EU
- Review all contracts with Data Processors
- If you don't have a Chief Protection Officer (CPO), hire one and ensure their policies align with GDPR requirements
- Review privacy and data protection policies that apply to personal data in the EU
- Review internal policy to determine if adjustments need to be made
- Consult with legal counsel to understand and know obligations.



77 per cent of IT professionals in Germany, Austria and Switzerland are three times as concerned as the rest of the world about the implications of the GDPR.

Worried About the GDPR? Are you Ready to Comply?

Asigra.

Recovery is Everything™

How Asigra Addresses Compliance Requirements.

The IT compliance requirements for most of regulations/standards can be categorized into four key sections. The table below shows how Asigra addresses each one of them.

Regulation/Standard	What does it mean?
▪ Privacy/confidentiality of information – Protect data from unauthorized disclosure. – Implies technologies such as encryption and access control to restrict access to data.	▪ Data is encrypted (AES 256, 196, 128-bit), before being transmitted over the WAN. ▪ Data stored in the DS-System and/or BLM is encrypted. ▪ Encryption is FIPS 140-2 certified ▪ Access control to data with full audit trail and reporting logs
▪ Integrity of data – Protect data from unauthorized modification ensuring its accuracy. – Implies technologies such as encryption and access control (authentication). – Integrity checks. – Audit trails (logging system events and physical access).	▪ Data is encrypted (AES 256, 196, 128-bit), before being transmitted over the WAN. ▪ Data is stored encrypted. ▪ Encryption is FIPS 140-2 certified ▪ Access control to data with full audit trail and reporting logs ▪ Data integrity validation through Autonomic Healing and ▪ Restore Validation
▪ Availability of information – Ensure that information is available when needed through business and service uptime assurance. – Data protection. – Business Continuity and Disaster Recovery technologies and plans	▪ N+1 and grid architecture ensures high availability through failover in case of system disruptions ▪ Disk based retention for fastest recovery ▪ Automated and verifiable backup/recovery process with built-in SLA module for reporting and auditing purposes. ▪ Built-in data replication capability for DS-System and BLM storage enables emergency plans for business continuity ▪ Asigra's architecture implements fast and reliable backup/recoveries at off-site location for DR purposes. ▪ Asigra's Value Beyond Software provides best practices and support for Business Continuity plans and Disaster ▪ Recovery Drills implementation and auditing purposes.
▪ Retention – Preservation of information in an unalterable form for specified periods of time. – With or without requirements for data destruction. – Ability to set policies and manage the lifecycle of data.	▪ Asigra's BLM provides long term disk based retention with data destruction certificate. ▪ Intuitive GUI makes it easy to implement and manage retention rules and policies. ▪ Long term data is stored encrypted.

Asigra's comprehensive backup, recovery and archiving solution gives you the stability and control you need to meet the GDPR requirements. Here's how Asigra's solutions can guarantee you remain compliant:

FEATURES	BENEFITS
Meet Corporate Governance and Regulatory Compliance Mandates	Our backup uses NIST FIPS 140-2 validated encryption for all back up data to adhere to specific retention periods.
Remotely Wipe Data and Schedule Periodic Cleansing with Selective Data Destruction	Wipe any outdated data from unauthorized locations from any endpoint device to comply with mandates and adhere to requests from data subjects to quickly locate their personal and contact information if they wish to be removed.
Eliminate Data Breaches	Ensure data remains safe, anywhere, at any time and on any endpoint device.
Easily Recover Data	Recover any data, anywhere, and at any point in time to be able to recover business critical data for any regulatory compliances.
Encryption	Data is encrypted in-flight and at rest.
Geo-locate Devices with Your Data	Obtain visibility into data anywhere and on any endpoint device to be able to identify and report on locations and sensitive data information.
Agentless	Our agentless technology protects and supports all files, databases, email systems, mailboxes, and operating systems with unlimited storage and petabytes.

About Asigra

Trusted since 1986, Asigra provides organizations around the world the ability to recover their data now from anywhere through a global network of partners who deliver cloud backup and recovery services as public, private and/or hybrid deployments. As the industry's first enterprise-class agentless cloud-based recovery software to provide data backup and recovery of servers, virtual machines, endpoint devices, databases and applications, SaaS and IaaS based applications, Asigra lowers the total cost of ownership, reduces recovery time objectives, eliminates silos of backup data by providing a single consolidated repository, and provides 100% recovery assurance. Asigra's revolutionary patent-pending Recovery License Model provides organizations with a cost-effective data recovery business model unlike any other offered in the storage market. In 2015, Asigra Cloud Backup was named the **Top Enterprise Backup Solution** and achieved silver in Storage Magazine's **Products of the Year**.

More information on Asigra can be found at www.asigra.com

Asigra.

© 2017 Asigra Inc. Asigra, the Asigra logo, Asigra Cloud Backup, Recovery is Everything, and Recovery Tracker are all trademarks of Asigra Inc. Recovery License Model is a registered trademark of Asigra Inc. All other brand and product names are trademarks of their respective owners. [03/17]