GDPR: AROUND THE WORLD IN ONE REGULATION

Quest®

GDPR: the regulation heard around the world

The General Data Protection Regulation (GDPR) requires organizations to strengthen data protection and security measures to protect the personally identifiable information (PII) of EU citizens. More specifically, organizations must ensure only people who should have access to PII have that access. Also, reasonable measures must be in place to protect data from unauthorized access as well as prove accountability of those accessing it.

GDPR impacts all organizations, in all industries and regions. Even those outside the EU that collect and store personal information of EU citizens must demonstrate GDPR compliance.

WHY? IMAGINE THESE SCENARIOS:

Your healthcare information, which houses your medical history, is now in jeopardy following a massive data breach.

Your personal data, including phone numbers and email addresses, has been stolen out of a cloud network following a cyberattack.

Your financial information, like tax forms and bank statements, has been unintentionally exposed by an administrator who was given improper access permissions at your last employer.

WHO'S RESPONSIBLE FOR THIS? AND WHY SHOULD OUTSIDE INFLUENCES IMPACT YOUR RISK?

The amount of sensitive information being collected by various applications, systems, and organizations has reached a staggering level, leaving many to wonder who exactly is accountable for ensuring its appropriate use and protection.

As technological advances and cybersecurity threats continue to mount, data protection becomes increasingly important to both organizations and individuals.

The GDPR, which became enforceable on May 25, 2018, sets rules for how personal data of European Union citizens can be collected and processed. But this set of regulations is cascading around the world. Countries are beginning to adopt similar legislative frameworks. Organizations are considering the impact to their operations and adopting new practices.

Let's take a quick tour around the world to see how the GDPR has been influencing organizations globally.

Quest

Getting the Facts Straight

Myth

The GDPR does not apply to businesses located outside of the EU.

The GDPR is not a big deal, and organizations can get by with encrypting their data or using pseudonymization

Organizations are immune from the GDPR because their cloud service provider (CSP) is wholly responsible for managing their stored data.

Fact

100%

of all data stored in the cloud or on-premises must be GDPR compliant, as long as EU citizen information has entered the database at any point in time.

79%

of organizations using SharePoint do not believe existing tools are “very effective” at protecting sensitive content from accidental exposure or a targeted breach.

68%

of organizations do not have sufficient visibility into where sensitive data is located within SharePoint.

Quest

North America

UNITED STATES

Entered into formal operation in August 2016, the Privacy Shield enables U.S. businesses subject to the jurisdiction of the Federal Trade Commission or Department of Transportation to transfer personal data from the EU to the US, given they have registered with the Department of Commerce. This policy provides seven principles with which companies must comply, and has been determined by the European Union as providing adequate safeguards for the transfer of data. But it's only applicable to that piece of the GDPR. Organizations still have to determine if the GDPR applies based on the information they are collecting and processing, and then comply accordingly.

US organizations appear to be taking the new regulations seriously, with half of all US multinational corporations stating that GDPR compliance is their top data protection priority. Funding for compliance activities is mounting and it is clear that information security enhancement in the US is a growing trend catalyzed by the GDPR.[1]

1 https://www.adweek.com/brand-marketing/84-of-u-s-companies-expect-to-be-ready-for-europes-new-data-regulations/

Quest

CANADA

Canada's PIPEDA Act (Personal Information Protection and Electronic Documents Act) may bring businesses closer to GDPR compliance, but they will still need to address comprehensive privacy policies and update breach notification protocol and penalties.

Larger corporations have started rolling out security and information governance strategies that address GDPR, but many SMBs are reportedly still at risk of noncompliance.

MEXICO

Mexico's Federal Data Protection Law is close to adhering to the EU's requirements for the protection of individuals with regard to the automatic processing of personal data (Convention 108), but its current regulation still presents risk to consumer privacy.

Businesses reportedly are focusing on introducing new technologies that can help mitigate security risk and protect personal data.

$1,000,000: Minimum budget most businesses are setting aside for GDPR preparations.[2]

2 https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html

Europe

UNITED KINGDOM

Under the context of Brexit, former Prime Minister Theresa May had publicly stated that the UK will prioritize GDPR, especially since it becomes enforceable while the UK is still part of the European Union. Though up to 24 percent of London businesses have demonstrated low awareness into the regulation,[3] UK organizations began to revamp their compliance strategies in 2018.

NORWAY

Following the recent healthcare data breach that impacted 50 percent of the country's population, Norwegian organizations are responding by implementing automated breach prevention measures into their security strategy and working towards GDPR compliance.[4]

GERMANY

Heralded as the first EU member state to align the new BDSG regulation with the GDPR, Germany has already exceeded GDPR requirements by imposing additional domestic

3 https://www.computerweekly.com/news/252433545/Almost-a-quarter-of-London-businesses-unaware-of-GDPR

4 https://www.computerweekly.com/news/252433538/Norwegian-healthcare-breach-alert-failed-GDPR-requirements

Quest

regulations, including penalties for non-compliance and video surveillance rules in public.

In addition to BDSG and GoBD, German organizations are decreed to GDPR compliance requirements, meaning the country will continue to incorporate a highly sophisticated regime for sensitive data security and notification.

AUSTRIA

Austria is the second EU member state to implement the GDPR, and organizations met the GDPR compliance enforcement date.

NETHERLANDS

The Netherlands' strict domestic data protection regulation (AVG) mandates organizations to report data breaches to the privacy watchdog, which could accelerate the ability of many Dutch organizations to meet GDPR requirements.

Multinational corporations (like Facebook, Apple and Uber) that host data in the Netherlands must adhere to privacy policies across country borders, in addition to the GDPR regulation.

SWITZERLAND

Swiss organizations have a legal basis to adopt the GDPR following the Federal Council's decision to adopt a domestic law requiring GDPR compliance, which includes penalties for the unlawful infringement of personal data.

Asia-Pacific

AUSTRALIA

With more than 1.5 million Australian citizens born in the EU, Australia faces a unique challenge to ensure GDPR compliance. The Office of the Australian Information Commissioner (OAIC) strongly recommended businesses implement all necessary steps to ensure compliance before the commencement.

All Australian businesses that provide goods and services for euros or pounds (or host German or French language websites) are liable for GDPR compliance.[5]

SOUTH KOREA

Though South Korea enforces one of the world's most globally advanced privacy regimes (Personal Information Protection Act), more than half of the country's businesses are reportedly still at risk of GDPR noncompliance.

Up to 21 percent of Korean organizations are concerned that GDPR noncompliance will result in revenue losses outside of GDPR-imposed penalties.[6]

JAPAN

Though Japan strengthened its data protection regulation following the reform of the Japanese Act on the Protection of Personal Information, the country still needs to implement the regulation nationwide. The estimate is that up to 60 percent of Japanese businesses did not meet the GDPR compliance enforcement date.[7]

SINGAPORE

Singapore reportedly stands with less than 10 percent GDPR readiness, even with a majority of the city-state expressing concerns around general data protection and privacy.[8]

5 https://www.cso.com.au/article/626299/australia-filled-eu-citizens-will-meet-your-gdpr-obligations-them/

6 https://www.zdnet.com/article/singapore-japan-korea-among-least-prepared-for-new-eu-data-laws/

7 https://www.zdnet.com/article/singapore-japan-korea-among-least-prepared-for-new-eu-data-laws/

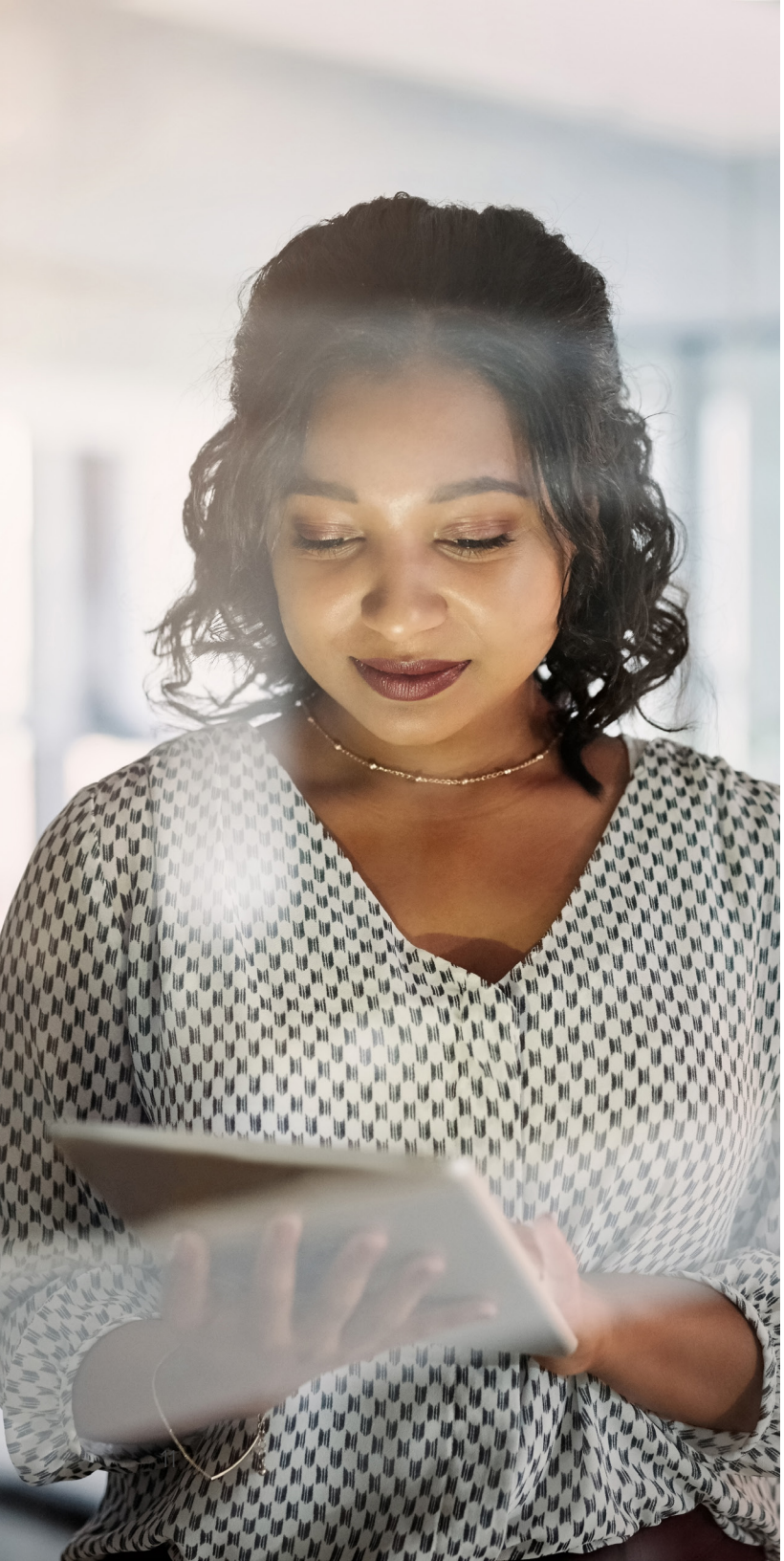
8 https://www.computerweekly.com/news/252435773/Singapore-firms-unprepared-for-GDPR?src=5719333

Protecting critical information

The threat of sensitive information falling into the wrong hands or being inadvertently disclosed is a constant concern. Yet, protection is only half the battle. Your organization is still at risk of considerable harm if processes do not enforce compliance of pertinent laws, government regulations and mandates. Data protection regulations, like GDPR, make persistent protection of your sensitive data more complex than ever before — and imperative to properly manage.

Check SharePoint off of your GDPR “To Do” list and break through the limitations of standard tools with a customizable solution that’s tailored to your information security and governance needs, yet flexible enough to address multiple regulatory landscapes.

Quest® Metalogix® solutions can help you implement a tailored solution that solves for the complex compliance challenges of SharePoint and Office 365.



Quest is here to help

Your compliance program is only as strong as your weakest link. See how Quest Metalogix solutions can help your organization locate personal data, manage governance policies, protect against threats and audit existing systems for security gaps.

See how Metalogix ControlPoint and Sensitive Content Manager can help bring you closer to GDPR compliance.

- ControlPoint enables permissions, auditing, reporting and governance policies for SharePoint so that you can confidently manage permissions and automate SharePoint governance and content cleanup, while protecting against data breaches and suspicious user behavior.
- Sensitive Content Manager raises the bar for SharePoint data loss prevention. It lets you confidently scan, detect and classify sensitive data and PII. Enforce policies leveraging the full range of SharePoint permissions management, auditing and user activity.

Conclusion

Organizations around the world face a variety of unique and distinguishing business challenges, but the GDPR is poised to impact all global entities — regardless of industry, size or revenue.

Despite the variances in how countries are responding to the GDPR, the need to manage sensitive information is consistent across the board. And even with highly enforced security strategies, organizations are still at risk of noncompliance, meaning they will have to reconsider their information governance and identify where their gaps reside.

Quest

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. We're a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we've built a portfolio of solutions which now includes database management, data protection, identity and access management, Microsoft platform management and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.

Ebook-GDPR-US-GM-41044

Quest