GLOBALCYBER CONSULTANTS

What is the GDPR and How Will it Affect Your Business?

THE GENERAL DATA PROTECTION REGULATION (GDPR) IS A SWEEPING REGULATION DUE TO TAKE EFFECT IN THE EUROPEAN UNION (EU) MEMBER STATES AND THE UNITED KINGDOM IN MAY 2018.

THE GENERAL DATA PROTECTION REGULATION (GDPR) IS A SWEEPING REGULATION DUE TO TAKE EFFECT IN THE EUROPEAN UNION (EU) MEMBER STATES AND THE UNITED KINGDOM IN MAY 2018.

Through the regulation, the EU has outlined protections for every individual citizen's personal data. The new legislation has huge implications for companies around the world that have any kind of market in the EU. Especially businesses that rely on consumer data.

In short, the GDPR introduces new obligations for any organization that handles data about EU citizens, regardless of whether that organization is based in the EU or not. In addition to new requirements for companies when it comes to notifying consumers about data breaches, there will be stricter responsibilities when it comes to managing and protecting personal data.

The EU hopes that these regulations will help streamline how organizations manage, store, process, and share personal data – balancing civil liberties and privacy with economic growth and innovation.

That said, the increased security controls, procedures and requirements set forth in the GDPR's 99 Articles are expected to come at a significant cost for businesses as many organizations will be required to appoint a Data Protection Officer, conduct Privacy Impact Assessments to ensure their organization is in compliance with the regulation and will be subject to substantial fines of up to €20M or 4% of global annual turnover (whichever is greater) for failing to adhere to the regulatory requirements, to name a few.

As businesses worldwide prepare to comply with the new, complicated data protection regulation, we have outlined the key facts that organizations need to know so they can adequately allocate resources to get ahead of compliance before it is too late!

1. THE GDPR AFFECTS ANY COMPANY THAT PROCESSES THE PERSONAL DATA OF EU CITIZENS.

This legislation widens the definition of personal data to include any data that can be used to identify an individual, such as genetic, cultural, economic, mental or social information. As almost all personal data now falls under the GDPR, organizations are faced with an increased demand to answer difficult data accountability questions such as:

– Why are we holding personal data?
– Why was it originally gathered?
– How did we get it?
– How long has it been held?
– Is the data shared with any third parties?
– How secure is the data in terms of accessibility and encryption?

2.ANY COMPANY THAT COLLECTS PERSONAL DATA HAS TO FIRST OBTAIN CONSENT. CONSENT TO COLLECT ANY PERSONAL DATA.

Organizations need to use simple and clear language when informing users about what information will be collected, how the information will be processed, and how it will be used used.

It's critical to note that firms need to be affirmative in obtaining consent to process personal data as silence and inactivity no longer constitutes permission. Without valid consent, any personal data processing activities will be shut down by authorities

3.PRIVACY RISK ASSESSMENTS WILL BE REQUIRED FOR ALL INITIATIVES.

The GDPR mandates Privacy Impact Assessments for identifying and assessing privacy exposures where privacy breach risks are high. This means that before organizations can even begin projects involving personal information, they must conduct a privacy risk assessment to ensure they are in compliance as projects commence.

4. DATA MONITORING MEANS THAT YOU NEED A DATA PROTECTION OFFICER.

The GDPR requires public authorities as well as certain other organizations to appoint a Data Protection Officer (DPO) when the organization's core activities require regular monitoring of data subjects or processing of large amounts of personal data. According to a study by the International Association of Privacy Professionals (IAPP), this requirement means that 28,000 DPOs will have to be appointed in the next two years in Europe alone.

5.ANY DATA BREACHES REQUIRE NOTIFICATIONS.

The GDPR introduces a common data breach notification requirement aimed to standardize the various data breach notification laws throughout Europe and ensure organizations are continuously monitoring for breaches of personal data.
The regulation requires that organization notify their local data protection authority of a data breach within 72 hours of discovering the breach, requiring new technologies, processes and training to ensure that data breaches are properly understood, recognized and handled.

6.ALL SYSTEMS SHOULD BE DESIGNED WITH DATA PRIVACY IN MIND.

The GDPR requires privacy by design in that software, systems and processes must be designed and consider compliance with the principles of data protection. For example, a substantial amount of commercially used software is not currently capable of properly erasing information. As the regulation is rolled out, all software will be required to completely erase data, posing new challenges for software engineers and business decisions at the strategic level.

7. ALL CITIZENS WILL HAVE THE RIGHT TO BE FORGOTTEN.

The GDPR introduces the right to be forgotten and the right of access by the data originator. At an organizational level, this maintains that companies must have the appropriate processes and technology in place to delete data in response from data subjects (i.e. originators). Companies must obtain clear consent before they alter the way in which they are using any data they have collected as these rights give individuals agency over their data and where it may be held, used and transferred.

LOOKING AHEAD

The new, sweeping regulatory requirements that the GDPR imposes will require organizational changes with new resources, processes and procedures for companies worldwide.

The biggest challenge for organizations is not technical, it's organizational. Each business will have to work to understand how people interact with data. While businesses were previously required to protect personal data, there is now an explicit requirement for companies to be overt and transparent about what and whose data they have, what they are going to be using the data for and how it is protected.

Organizations are faced with a fundamental culture shift as all employees from those at the executive level down to administration must be aware of their obligation to protect consumer data across all channels, even over the phone. That said, perhaps the biggest change that will drive transformation across all industries, is that the GDPR puts the customer back at the center and in control over their data. Although there will be many organizational pressures and hurdles to comply, this transformation should be viewed as positive progression towards an economy built upon trust.

About Global Cyber Consultants

At the forefront of digital innovation, Global Cyber Consultants works with worldwide organizations to ensure their assets are best protected while driving innovative change and operational efficiencies to secure sustained success and accelerated growth. With recognized industry expertise across insurance, technology, cybersecurity and finance/strategy, we ensure our clients they have industry leading resources and the intellectual capital required to maintain a competitive advantage within their own operating environment and the ever-changing business landscape.

At Global Cyber Consultants, we have created a standardized assessment that automates the manual processes of traditional risk assessments and allows companies to automate and streamline the IT and Vendor audit process by mapping to several security standards, such as NIST, ISO, HIPPA, PCI and the NY DFS Regulation, through one assessment. In responding to market needs, our platform also continuous insight into a company's cyber risk and their particular exposures, and what steps and the appropriate solutions that should be taken and implemented to better secure themselves with actionable insights and become "cyber competitive."