GDPR takes effect in May 2018

Is your nonprofit ready?

What is GDPR? The General Data Protection Regulation is Europe's new privacy law that raises the bar for the protection of personal data, which is any data that can be linked to an individual.

What does this mean to the average person or organization in simple terms?

The GDPR imposes new rules on companies, government agencies, nonprofits, and other organizations, regardless of their location, that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The average person will have more explicit rights under GDPR to know who stores, processes, and has access to his/her personal data. Under GDPR, EU residents can request access to and rectification and deletion of his/her data.

Organizations need to review their data governance practices, get rid of legacy systems that store unnecessary data, and delete data not collected as prescribed under the new rules of the GDPR. They also need to document appropriate technical and organizational measures and work only with reliable vendors or face high financial and reputational risks.

How will GDPR impact my organization based in the US?

For many organizations in the US that do not operate or have business in the EU or process information of individuals in the EU, the GDPR will not have an immediate impact. However, many other countries around the world are looking at the GDPR to be a basis for their own privacy laws and regulations. Microsoft believes compliance with the GDPR standard can be a best practice in data management of personal information.

Why did the EU put GDPR into place?

In Europe, privacy is a fundamental right and the EU is dedicated to protecting it. Its operational philosophy is built on the concept that personal data belongs to the individual. This is different than how the United States operates, whereby information collected on an individual is seen as the property of the organization that collects it. Data breaches have become part of our everyday life, and Europe wants to lead the way internationally to require companies to be more principled and transparent around data use and to invest in security and data protection. Any company or agency collecting or utilizing personal information may do so only if it has a lawful basis to process the information.

Will other countries follow the EU and put similar regulations in place?

The GDPR applies to anyone who provides goods or services to residents in Europe. Other countries are considering similar laws with some variations, because they consider GDPR to be overly prescriptive.

Who will monitor GDPR compliance?

The Data Protection Authorities in the member states, as well as the European Data Protection Board, will monitor GDPR compliance.

When does GDPR take effect?

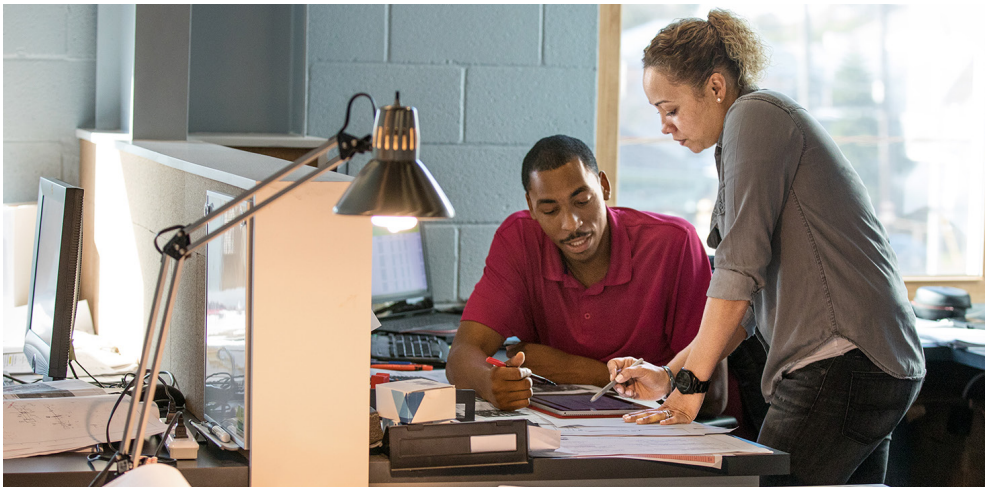
May 25, 2018. It has been made clear that there will be no enforcement grace period, as companies received two years' notice to prepare for the new regulations.

What are the main requirements of GDPR?

The GDPR requires enhanced security, data protection, appropriate technical and organizational measures, transparency, recordkeeping, accountability, and support for data subject requests. It also requires that data controllers notify authorities about personal data breaches within 72 hours. Responsibility for data protection will be shared within organizations and with vendors, establishing a shared responsibility model. Organizations must know what and how personal information is collected and processed in their internal systems. This requires executive awareness of how this takes place and cannot be considered an IT or legal issue alone. Internal awareness and training will be key.

How do I know if GDPR applies to my organization?

GDPR applies to any organization which operates within the borders of the European Union or processes the personal data of any person in the European Union. What are risks to my organization if it doesn't comply? Failure to comply will expose the organization to legal and financial penalties from privacy regulators in the EU plus legal claims from individuals.



Can Microsoft help us meet the requirements of GDPR?

The final responsibility for GDPR compliance lies with the organization. It's up to nonprofits to determine what data will be collected, how it will be used, which people in the organization are responsible, and how individuals can request their personal information and request rectification and deletion.

However, Microsoft does provide a suite of tools to assist with meeting requirements. Our Azure cloud infrastructure has been designed with GDPR in mind and has the systems in place to assist with compliance. Our Office 365 E3 and E5 licenses allow for ease of data tagging and automatic identification of sensitive information even if the user does not know it to be sensitive. Finally, we have launched a GDPR compliance dashboard that can be used by organizations to monitor their own compliance.

You can also visit the GDPR webpage on our new Microsoft Trust Center website to learn more about how the features and functionality of Azure, Dynamics 365, Enterprise Mobility + Security, Office 365, and Windows 10 will enable you to meet GDPR requirements.

Next steps

- Review the Nonprofit Guidelines for Cybersecurity and Privacy white paper
- Determine the owner for GDPR compliance and identify next steps to ensure compliance.
- GDPR compliance will not happen overnight with a final endpoint, it's a continuous journey.

Additional resources

Security and Compliance Information for Nonprofit Organizations

Microsoft Trust Center – GDPR

Andrea Simandi

Andrea Simandi was appointed to the role of European Data Protection Attorney for Microsoft in February 2017. As part of Microsoft's European Commercial legal team, she supports the company's enterprise customers in complying with the requirements of the General Data Protection Regulation and accelerating their digital transformation.

Cameron Birge

As the Microsoft Philanthropies Humanitarian Response Manager, Cameron has the responsibility for coordinating across the company the provision of resources to external agencies providing humanitarian relief during sudden-onset humanitarian disasters. As with others on the team, he also has a portfolio of other engagement areas with nonprofits that include awareness on data privacy and cybersecurity issues.