THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

May 2018 is the compliance moment
Make no mistake, the GDPR sets a new and higher bar for privacy rights, for security, and for compliance. And while your journey to GDPR may seem challenging, Microsoft is here to help all of our customers around the world.

Brad Smith
President & Chief Legal Officer, Microsoft
Table of contents

03 Executive summary
04 GDPR compliance and government implications
07 Promise of technology
10 Drawing additional value from GDPR compliance
13 Your quick start journey begins here
**Executive summary**

European governments and commercial organizations doing business in Europe must each comply with the General Data Protection Regulations (GDPR), but governments have unique GDPR obligations. As a regulator, you must deliver a consistently secure privacy experience for your citizens, in addition to educating the private sector community on compliance. While your compliance is legally required, adherence to the GDPR establishes you as a role model for commercial organizations; especially since many of them depend on information provided by, or shared with government. We believe at Microsoft that technology can help you lead by example to meet your security requirements, your operational objectives, and build trust and transparency with citizens.

GDPR compliance can be a force-multiplier. In addition to protecting and securing your citizens’ data, your GDPR journey will enable you to optimize your business procedures and modernize your legacy systems. Aided by automation, lower-value processes can be redesigned – empowering your first line workers to focus on higher-value assignments.

The GDPR reflects that your citizens want to manage their own lives, and how they engage with you. As a byproduct of your GDPR-compliance efforts, not only will your citizens have greater control over their data, but they’ll enjoy more personalized and secure engagements with you through the deployment of citizen-centric GDPR-compliant services.

There are additional benefits in being GDPR compliant. The AvePoint study on Organizational Readiness for the European Union General Data Protection Regulation identifies 3 positive impact areas:

- Implementing a data strategy and data governance strategy and system
- Managing the contractual relationships with customers and suppliers to ensure compliance across the data chain
- Implementing a security strategy and a notification system as proactive mechanism of control

This will allow you to offer Citizen Centric Services and ensure strong security of infrastructure through cyber security resilience.
GDPR compliance and government implications

The GDPR imposes new rules on entities that offer goods & services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

The GDPR is structured around six principles:
1. Requiring **transparency** on the handling and use of personal data.
2. Limiting **personal data processing** to specified, legitimate purposes.
3. Limiting **personal data collection and storage** to intended purposes.
4. Enabling individuals to **correct or request deletion of their personal data**.
5. Limiting the **storage** of personally identifiable data for only if necessary for its intended purpose.
6. Ensuring personal data is protected using appropriate security practices.

Government agencies collect and manage huge amounts of citizen’s personal and sensitive data. As processor of such information, they are required to comply with the regulation. At the same time government organizations are also important employers, managing data for thousands of employees.

Therefore, many government agencies play a multiple role, both as a **data controller** and a **data processor**. GDPR applies to both data controllers and data processors. Data controllers must only use data processors that take measures to meet the requirements of the GDPR.

Under the GDPR, data processors face additional duties and liability for noncompliance, or acting outside of instructions provided by the controller, as compared to the Data Protection Directive. Data processor duties include, but are not limited to:

- Processing data only as instructed by the controller
- Using appropriate technical and organizational measures to protect personal data
- Assisting the controller with data subject requests
- Ensuring sub processors are engaged to meet these requirements

The implications for Governments are wide. Very soon, all public-sector organizations will need to have consent or one of five other specific legitimate reasons to hold and process individuals’ data, including all legacy data.
Right to Rectification and Portability - Public organizations will need to ensure appropriate IT systems and data governance processes are in place to deal with the right to erasure, restriction of processing and data portability. The right to data portability gives individuals the right to move their data elsewhere and to receive assistance in doing so. Complying with these new data portability requirements will force public organizations to ensure they can bring all customer information together and manage it from a single place. Let’s examine a scenario: The accounts and credentials created to electronically file and pay taxes are not the same as those used to inquire about other social services. As a result, personally identifiable information about citizens is not centralized within government agencies and is often duplicated across line of business systems. Within the context of GDPR this creates challenges for government agencies as citizens will want to review their data, correct it as necessary, and where possible erase it. We’ve explore on the next slide how we can use a Federated Identity Management (FIM) solution to solve some of these challenges.

Big data and “citizen segmentation” - In the last few years, government agencies have been gathering as much data as they can to leverage its value across citizen experience and business operations. However, now they will have to re-examine their data strategies. In the case of most personal data, they’ll have to limit the amount of data they gather and store, and for how long, to meet compliance requirements. Additionally, the GDPR specifically imposes constraints on “profiling” which it defines in GDPR Article 4(4) as “any form of automated processing of personal data … to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.” This means agencies will have to re-examine their processes governing the use of predictive analytics to deliver personalized services. As the demand for personalization increased, retailers will need to find a way to continue big data and personalization of the eGovernment experience in a way that is GDPR compliant.

Subject access requests - Public organizations should be aware that there will likely be an increase in access requests, and there may be a need for increased administrative resources to deal with same. They will be obliged to respond to access requests within one month unless they are “manifestly unfounded or excessive” or a national legislative measure allows access to be refused. It remains to be seen whether the motive for the access request can be taken into consideration by a controller when responding to requests.

Trust and public perception

Consent and digital communication/marketing – The GDPR will require explicit opt-in for all electronic and automated marketing. This includes email, SMS and automated calling. Explicit consent will mean no more pre-checked boxes, automatic opt-ins from order forms, etc. Therefore, children under the age of 16 will need parental / guardian consent. Additionally, B2B customer and prospect data is no longer excluded for unincorporated companies.

IoT device data - The GDPR requires that privacy protection is built into IoT devices by default. This means data-sharing should be limited to the specific purposes that have been presented to the individual concerned.

Expanded scope - Because of the wider reach in terms of processing data, government agencies can expect a few changes to the way they collect, store, process, and secure their personal data. The GDPR now specifically lists genetic data and biometric data as sensitive personal data and permits Member States to introduce further conditions around the processing of biometric, genetic, or health data

Lawful processing – Public organizations will need to document and prove their legal basis for processing personal data. Government departments and public companies must be able to demonstrate that consent has been given, procedures must be in place for recording consent. Data access requests such as Freedom of Information requests will regularly test this compliance.

GDPR is ultimately setting a course for citizen trust. As our partner Soprasteria highlights the objective is to restore the trust of individuals in the processing of their data. This renewed trust is a real business issue for Governments and businesses on the way to GDPR compliance. No viable digital economy exists without trust, however 72% of Europeans fear the improper use of personal data as per ex-European Commissioner for Justice Fundamental Rights and Citizenship, Viviane Reding.

By developing citizen trust Public administrations will improve their image and position themselves as agents of trust. At the same time citizen trust contributes to citizen compliance when it comes to tax obligations for example. (OECD 2013 Cooperative Compliance)
Public procurement implications

**Government Tenders/Procurement Agreements** – During the course of procuring goods or services from vendors, government agencies may collect, process, and manage personal information relating to a vendor’s owners, employees, or contractors. Governments must manage such procurement processes in a way that complies with the GDPR. A “Digital Public Procurement” platform can help public organizations meet their compliance obligations.

**Proof of concepts/pilots** – Certain proof-of-concept pilots conducted by software vendors rely on “production” data that contains personal information. To benefit from the use of production data, government agencies should leverage GDPR-compliant ICT platforms to assist such agencies with their GDPR compliance obligations.

**Awarded Contracted** – Suppliers may routinely process or otherwise come in contact with government data that is projected under the GDPR (e.g., employee data, personal citizen information). Agencies need to establish a GDPR compliance process to manage and track suppliers that come into contact with GDPR-protected data.

GDPR compliance may have a positive impact in helping to reduce the vulnerability of cyber attacks

**Privacy by design** – The GDPR sets a new standard of privacy by design and by default, requiring data privacy to be embedded into data governance processes, systems, and products. The GDPR also states that organizations must conduct data protection impact assessments to predict the privacy impacts of projects and employ mitigations as needed.

**Data security and breach notifications** – The GDPR will require retailers to secure personal data in accordance with its sensitivity. In the event of a data breach, data controllers must generally notify the appropriate authorities within 72 hours. Additionally, if the breach is likely to result in a high risk to the rights and freedoms of individuals, organizations will also need to notify affected individuals without undue delay.
Microsoft: The promise of technology

In February of this year, we announced that Microsoft cloud services will comply with GDPR by May 25, 2018—across Office 365, Dynamics 365, Azure, including Azure data services, Enterprise Mobility + Security, and Windows 10. The Microsoft Cloud also has a range of compliance controls, audited by third parties. Through these investments, we will also help you validate that when you are using the Microsoft Cloud, you are using services compliant with the GDPR. To further demonstrate our commitment to you, we’ve backed this up with our contractual commitments that provide key GDPR-related assurances about our services.

Microsoft: The promise of technology

In the new GDPR world Microsoft helps you respond to many of your customers’ questions, including:

- Do you know where your data resides and who has access to it?
- How do you control who has access to your data and how it is used based on risk assessment in real-time?
- Can you classify, protect and apply policy-driven actions to your data, on devices, between apps, in any location, at rest and in transit?
- Can you automatically detect a data or identity breach? And are you able to respond adequately to a breach?
- Do you continuously review and update your data protection policies and practices?

Our extensive portfolio of solutions provide you with a holistic set of capabilities to help meet your GDPR obligations. These capabilities operate across our platforms and core products, enabling you to utilize compliant solutions for all aspects of your organization.
A community of experts to guide your journey

We recognize that GDPR spans technology and business policy. To this end, we’ve brought the Microsoft partner ecosystem together to help you. In the Microsoft Tech Community privacy forum you can discuss GDPR issues and learn from experts.

We’ve collaborated with consulting firms with deep policy knowledge of privacy and GDPR, and working together, who can help you plan and implement process and technology to be GDPR compliant. And finally, we’re sharing best practices from our own privacy experts.

GDPR is part of our holistic cloud compliance investments

We are committed to our principles of cloud trust – across security, privacy, transparency and compliance. We have a broad portfolio of cloud services that address the rigorous security and privacy demands of our customers, who comprise over 90 percent of Fortune 500 companies. As the GDPR enforcement begins, here is what else you can expect from us:

• Technology that meets your needs – You can leverage our broad portfolio of enterprise cloud services to meet your GDPR obligations for areas including deletion, rectification, transfer of, access to and objection to processing of personal data. Furthermore, you can count on our extensive global partner ecosystem for expert support as you use Microsoft technologies.

• Contractual commitments – We are standing behind you through contractual commitments for our cloud services, including timely security support and notifications in accordance with the new GDPR requirements. In March 2017, our customer licensing agreements for Microsoft cloud services will include commitments to be GDPR compliant when enforcement begins.

Sharing our experience – We will share Microsoft’s GDPR compliance journey, so you can adapt what we have learned to help you craft the best path forward for your organization.
The value of Microsoft Enterprise Services

GDPR requires a holistic approach to security and data management—resulting in a secure, modern enterprise. While Microsoft cannot certify compliance against any specific regulation, we can help you simplify your GDPR journey through proactive modernization of IT environments.

Microsoft Services’ Security Risk and Data Management program consists of two components that will help simplify and streamline your GDPR journey: a Discovery and Planning workshop to educate and develop a clear roadmap, and our rich set of Security Risk and Data Management solutions to modernize your IT environment. Following this approach, we help you establish a foundation for digital privacy and data protection. We can also work with your preferred compliance partner to provide technology-based services to complement their GDPR-related services to support your end-to-end GDPR program.

Discovery & Planning Workshop

Microsoft will review the maturity of your existing data privacy program, your data security and risk management investments, and the location and correlation of personal data that is processed through your business processes and technical capabilities. Furthermore, infrastructure, cloud, and identity security measures will be reviewed and compared with Microsoft’s current architecture recommended practices and designs. This information is consolidated and analyzed to develop a roadmap of short-, mid- and long-term actions mapped to technology capabilities and solutions, that resolve identified gaps and achieve desired objectives.

The next step is to modernize your IT environment across Cloud, Security, Identity, and Data platforms to prepare for your GDPR Program. Microsoft Services has well established and effective platform modernization solutions.

- **Modern cybersecurity foundation**: mitigate against cyber threats.
- **Modern data platform foundation**: know where your data is and how to manage it effectively.
- **Hybrid cloud foundation**: use the Cloud’s advanced data and security capabilities.
- **Modern workplace**: optimize end user productivity, collaboration and security.
Drawing additional value from GDPR compliance

As a regulator, you must deliver a consistently secure privacy experience for your citizens, in addition to educating the private sector community on compliance. While your compliance is legally required, adherence to the GDPR establishes you as a role model for commercial organizations, especially since many of them depend on information provided by, or shared with government. Microsoft believes that technology can help you lead by example to meet your security requirements with trusted technology solutions that secure data you collect and process, increase operational efficiencies, as well as create trusted relationships with your citizens.

Citizens benefit from personalized "made-for-me" service delivery experiences supported by a single interface, with a single identity to access all government social services and programs. This personalized and secure experience helps enable citizen engagement and access to services – anytime, anyway and with any device. Ultimately, this creates a continuous service consumption and citizen feedback loop that drives continuous government service delivery and improvement.

Personalized citizen service

The GDPR reflects citizens desire to manage their own lives, their data, and how they engage with government. As a byproduct of your GDPR-compliance efforts, not only will your citizens have greater control over their data, but they’ll enjoy more secure and personalize engagements with you through the deployment of citizen-centric GDPR-compliant services.

Innovative technologies like cloud and AI are optimal, helping you establish trusted and secure GDPR-compliant experiences – employee and citizen experiences. It will help drive better decision making, and potentially lead to creation of digital government processes and services when managing and providing social services programs for the greater good. Complying with GDPR helps government foster citizen trust and confidence that their personal data will be protected, access to manage, edit and remove their personal data as their needs evolve.
Protection against the most prevalent and damaging threats

A Digital Protection program provides you with solutions to help minimize and mitigate attacks, protecting your organization and citizen data, and while managing digital identities and access. Based on your business priority, you can define your protection journey.

Minimize and mitigate attacks

Today’s corporations operate in an environment where information breach is almost inevitable. Cybercriminals know where to go inside your network to target the highest value assets—finance, operations, and citizen data. Add to that the challenge of aging infrastructure that makes it difficult to expand your organization, maintain relevance, and secure the organization and data in compliance with regulations and market expectations. In today’s digital world it’s impossible to prevent all attacks, so rapid detection and response capabilities are essential to protecting any government organization.

Protect organization and citizen data

Data is any organization most valuable asset. If financial data, and other proprietary assets, or operational processes were stolen, it could jeopardize the financial stability of any organization. Additionally, citizens need to trust government organizations with their personal data, and know it is secure. Developing secure modern data protection processes can help protect your organization’s most valuable assets.

Manage digital identities and access

You need to know that access to your organization and your citizens’ data are not compromised by the policies and technologies you have in place. And, your organization needs to be able to support and comply with a modernized identity platform.

Benefits

A Digital Protection Program is an important step to a more secure transformation. In order for a Digital Protection Program to be successful, it should cover three critical components:

- **THREAT PROTECTION**: Mitigating cyberattacks with modern protection, early detection, and rapid response to better keep malicious threats out of your organization.
- **INFORMATION PROTECTION**: Protecting organization and citizen data and other digital assets.
- **IDENTITY & ACCESS MANAGEMENT**: Managing digital identities and access enables greater efficiency and innovation to be able to stay ahead of citizen needs and market trends.
Your quick start journey begins here

These are the three steps we recommend in your quick start compliance journey with Microsoft:

1. Go to Microsoft.com/GDPR to learn more about GDPR and explore our resources.
2. Take the GDPR Assessment to identify resources toward simplifying and strengthening compliance.
3. Use this e-book as a resource reference to dive deeper into recommended capabilities.

A recent issue of the Economist explained, “How to manage the computer security threat.” Their top recommendation was that both government and product regulations must lead the way.

Without a doubt, GDPR needs to be seriously addressed as a top priority on the agenda of every Government agency now and beyond May 2018. This is a continuous commitment to security and privacy. By becoming more regulated through GDPR, providing a framework to better protect personal data, and giving tools to implement security controls for protecting, detecting and responding to threats, we will fight our best fight against cyber crime. Microsoft stands ready to work with you to raise awareness, empower and ensure access to the resources available now and in the future.

Resources

Microsoft.com/gdpr


New Microsoft 365 features to accelerate GDPR compliance blog post.

GDPR assessment tool - this 20 questions survey provides customers with guidance on where they are on their GDPR journey and how to use our products to help them with their compliance efforts.

GDPR eBook - this e-book provides a rollup of the content from the assessment tool.

Compliance manager preview: Manage your data protection and compliance posture from one place.
What’s next?
No matter where you are on your digital transformation roadmap, Microsoft Enterprise Services can help.

Engage your citizens
Through connected mobile services to increase satisfaction and participation

Empower your employees
to do their best work by leveraging the power of mobility

Optimize government operations
to ensure cost and operating efficiencies with trusted cloud services

Transform your services
and better utilize data to produce actionable analysis and enable better decision making

Credits
Many subject-matter experts from various groups at Microsoft contributed to the conceptualization and articulation of the story contained in this document.

Steve Rosenboro
Senior Attorney, Commercial Industry and WW Government Industry CELA Lead

Valentina Ion
Sr. Manager Government Industry, Microsoft Europe Middle East and Africa

Lina Mongrand
Sr. Business Program Manager, Government Industry Solutions, Enterprise Services, Microsoft

Binil A Pillai
Director, Cybersecurity & Identity Solutions Strategy, Enterprise Services, Microsoft

Contributors
Susie Kalousis
Digital Engagement and Experience Lead, Government, Enterprise Services, Microsoft

Daniel Grabski
Executive Security Advisor, EMEA, Microsoft

Jason Payne
Chief Architect – Government Industry, Worldwide Public Sector, Microsoft
Microsoft Enterprise Services empowers organizations to accelerate the value realized from their digital experiences.


microsoft.com/services