Microsoft

Journey to GDPR Compliance

Contents

Introduction

At Microsoft, we are deeply committed to privacy. In 2000, we established our first corporate privacy function, laying the foundation of people, process and technology investments for what is now a broad privacy governance program across Microsoft.

The General Data Protection Regulation (GDPR) is an important step forward for clarifying and enabling individual privacy rights. The GDPR will take effect on May 25, 2018, and Microsoft has been investing to be compliant across its entire business for nearly two years leading up to this date, building upon this foundation and history of our commitment to privacy.

This e-book addresses our own journey to GDPR compliance. We share our approach to global regulations and standards like the GDPR, what we've been doing to drive compliance within Microsoft, and key lessons we've learned along the way. We hope this e-book will be helpful to you regardless of where you are in your own efforts around GDPR compliance, and will give you a window into the level of investment we have made.

Brendon Lynch,
Microsoft Chief Privacy Officer

Our framework

Since Microsoft operates in nearly every country in the world, we are subject to, and must operate consistent with, a multitude of laws, regulations, codes of conduct, industry-specific standards, and compliance standards. Microsoft also wears many hats—as a large international employer, as a provider of consumer products and services, and as an enterprise-class software and service provider. For privacy regulations, the following framework helps describe the compliance investments we've made to our organizational structure, and processes:

Assessing and managing our compliance risk through tools such as extensive personal data store inventorying, data protection impact assessments and privacy reviews, and processes for the monitoring, measurement, and enforcement of privacy compliance.

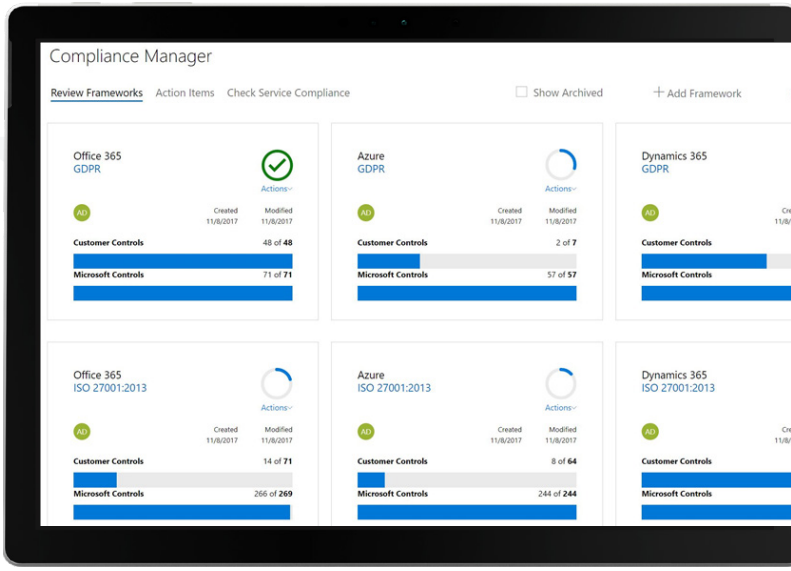
Protecting personal data with built-in, intelligent security capabilities that work together to more effectively secure personal data (including employee data).

Streamlining our processes to empower our consumer users to access and manage their data, help our commercial customers meet their own compliance obligations, and train our employees, partners, and vendors on privacy readiness.

Assessing and managing our compliance risk

To meet our compliance obligations, we thoroughly examine relevant regulations, laws, industry best practices, standards, certifications, codes of conduct, and other rules and guidance applicable to Microsoft in all its roles. We also review similar sources that are generally applicable to our customers. We then create controls against which we can test our compliance with these requirements. It is a massive exercise given the global nature of Microsoft's operations and that of its customers. But through this process we have developed the confidence, experience, and expertise that has enabled us to more nimbly address new regulations such as the GDPR.

We're now providing the benefits of this hard-earned experience and expertise to our customers via the Microsoft Compliance Manager—a new solution that our customers can use to manage their own compliance with key regulations and standards from a centralized dashboard. The Compliance Manager provides you with a real-time risk assessment of deployed Microsoft Azure, Office 365 and Dynamics 365 cloud



services, and a compliance score to help you understand your exposure to risk for specified compliance and data protection standards, regulations, or laws. Assessment results combine the detailed documentation of controls implemented by Microsoft to comply with requirements, as well as provide prescriptive guidance and recommended customer actions for your organization to take to improve compliance posture.

Protecting personal data

Compliance with regulations like the GDPR requires that organizations take appropriate technical and organizational measures to protect personal data from loss or

unauthorized access or disclosure. Protecting personal data in today's complex threat landscape requires a comprehensive approach to data security.

Microsoft invests over $1 billion in security annually. It's a massive investment that is required to outpace the criminal innovation, bring cybercriminals to justice, and deliver innovative, world-class security for our employees and customers. Our security investments take a platform approach that looks holistically across all the critical end points of today's cloud and mobile world:

Identity and access management. We use capabilities like Microsoft Azure Multi-Factor Authentication, conditional access in Active Directory, and biometric verification in Windows 10 to protect user identities, control access to resources, enable fast and secure logins, and prevent pass-the-hash attacks.

Information protection. We use the protection capabilities of Azure Information Protection, Office 365 Data Loss Prevention, and Enterprise Mobility + Security solution to detect and prevent data leakage, restrict unauthorized data sharing, classify and retain data, protect data on lost and stolen devices, and monitor and manage device and applications on mobile devices.

Product spotlight:

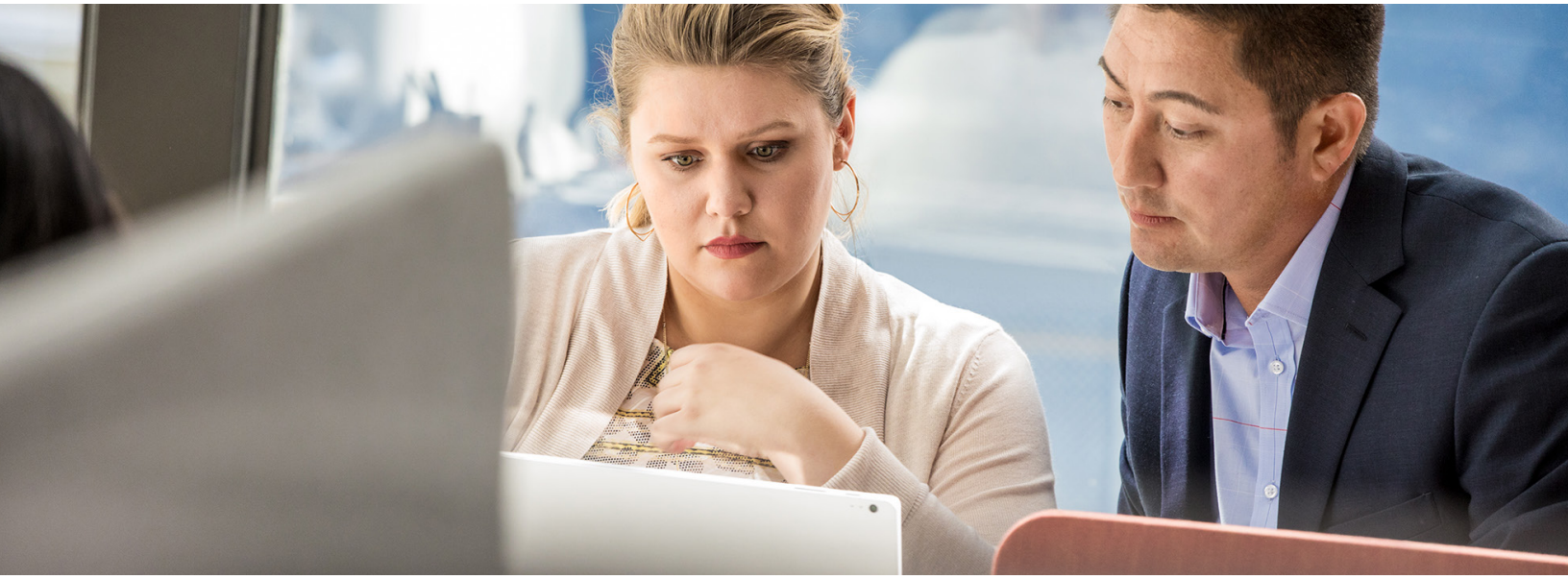
With **Office 365 Data Loss Prevention (DLP)**, we can identify, monitor, and automatically protect against inadvertent disclosure of data such as credit card numbers, social security numbers, and health information. We use this technology across Exchange Online, SharePoint Online, and OneDrive for Business, and it even helps prompt employees about the DLP policy.

The **Intelligent Security Graph** synthesizes a vast amount of security signals from more than 200 services using advanced analytics technologies and artificial intelligence to deliver self-learning, actionable security insights in near real time. These insights are shared across all our security solutions, making them smarter, better at protecting, and capable of stopping attacks before they happen.

Threat protection. To combat increasingly sophisticated cyberthreats, we created the Microsoft Intelligent Security Graph (ISG), which enables our solutions to bring in unified preventative measures that improve the efficiency of protecting, detecting, and responding to security incidents. We also use Office 365 Advanced Threat Protection (ATP) and Windows Defender ATP to protect our environment from malicious files and links, detect anomalous behavior, isolate potential threats, automate breach response.

Streamlining our processes

Regulatory obligations can be a forcing function to streamline and improve internal processes. Our privacy program has evolved over time and the GDPR provided an impetus to continue that evolution. GDPR requirements have driven further automation of data governance processes; the evolution of privacy tools, programs, and processes; changes to our internal privacy standards; and a variety of organizational changes designed to improve the consistency and efficiency of our privacy outcomes. As a result, we've been able to reduce unnecessary data processing, standardize our contracts with partners and vendors, and improve the collaboration between our engineering, privacy, and compliance teams.



Our approach for the GDPR

Like our customers, Microsoft must ensure we have appropriate technical and organizational measures in place to meet our specific GDPR obligations and support the GDPR needs of our customers. The following sections share key parts of the approach we took with regard to the GDPR, some of our learnings, and examples of how we scaled our implementation efforts.

Defining scope

Once the GDPR was officially adopted on April 27, 2016, it was important to translate the GDPR's legal requirements into business requirements that were specific to Microsoft and more digestible for our privacy, compliance, and IT leaders. Our Corporate, External, and Legal Affairs team completed a significant legal analysis of the regulation to develop business requirements, called Business Implementation Requirement Documents (BIRDs), that our privacy experts and IT leaders could translate into controls, milestones, and workstreams.

Due to the GDPR's scale, prioritizing efforts and preventing workstream fragmentation were ongoing challenges. It was critical to envision and explicitly define an end

> "It was imperative that our legal experts translate the GDPR's requirements into business requirements that our business and engineering teams could run with."
>
> –Alison Howard, Assistant General Counsel, Privacy & Regulatory Affairs, Microsoft

state for our compliance to drive consistency across our workstreams and help our teams prioritize their implementation efforts. This led us to focus on a number of investments:

- Launch a self-service privacy portal for consumers to request copies of and delete their personal data used in our cloud services.
- Building a comprehensive data inventory that accurately maps out the flow of personal data across our entire business.
- Implementing a common infrastructure that standardizes data schema, enables automation, and enforces privacy policies.
- Reviewing and standardizing data retention policies across our businesses, systems, and partners/ suppliers.
- Updating our technical documentation and processing contracts to deliver our commercial customers the information and assurance needed for their own compliance obligations.
- Reviewing our Data Privacy Requirements for our vendors and building compliance requirements into our procurement process.

While this is not an exhaustive list, it represents a significant portion of our compliance efforts.

Training our people

After defining the GDPR's scope for our organization, it was evident we needed to ensure our affected people had a strong understanding of privacy and how the GDPR's requirements would affect the way we processed personal data. We expanded our corporate privacy training significantly to help educate our employees, partners, suppliers, and vendors about upcoming privacy requirements affecting their roles, and how we would approach compliance. Our core internal training and GDPR readiness investments include:

- Internal webinars, workshops, online training courses, and reference materials to train our employees, partners, and vendors on the GDPR's requirements, privacy program updates, and security requirements.
- Train-the-trainer programs to empower subject matter experts to lead specialized trainings in their local hubs and divisions.
- Abbreviated technical and privacy documentation for our customers, detailing our compliance with GDPR, and guides to help enable secure and compliant use of our products and services.

Our investments in training resulted in better privacy program execution not only by ensuring our people understood the new GDPR requirements, but also by enabling us to scale our implementation efforts more effectively.

"Our legal team engaged in routine "office hours" to support engineering and compliance teams in addressing complex interpretation questions. Answers to these questions were cataloged for use by other teams and to ensure consistency of application."

–John Payseno, Assistant General Counsel, Microsoft

Enhancing our privacy processes

Our privacy program starts with a bedrock of accountability spread across each corporate entity to drive program ownership. At Microsoft, this bedrock of accountability is implemented through a centralized privacy team and divisional groups that spread across our engineering and business groups. Our centralized privacy team includes legal, privacy, engineering, and compliance professionals. This central team is tasked with defining the privacy compliance rules and companywide program strategy for addressing privacy regulations.

Privacy accountable executives in each of the groups build compliance programs tasked with meeting the requirements set out by the central team. Each divisional group cascades that accountability down from their accountable executive through privacy program owners, privacy managers, and engineering leads. The central team supports those teams with a common unified privacy policy framework, training on new requirements, and process and other programmatic support.

To achieve GDPR compliance across our diverse business groups and engineering divisions, we launched a companywide initiative called Next Generation Privacy (NGP). Our NGP

initiative provides a comprehensive framework that includes policies, processes, technical infrastructure, and customer experiences to address privacy at all levels of our organization and deliver the standardization needed for compliance. Within this framework, we identified accountable executives in each of our engineering, business, and specialized organizations that are responsible for GDPR compliance in their group.

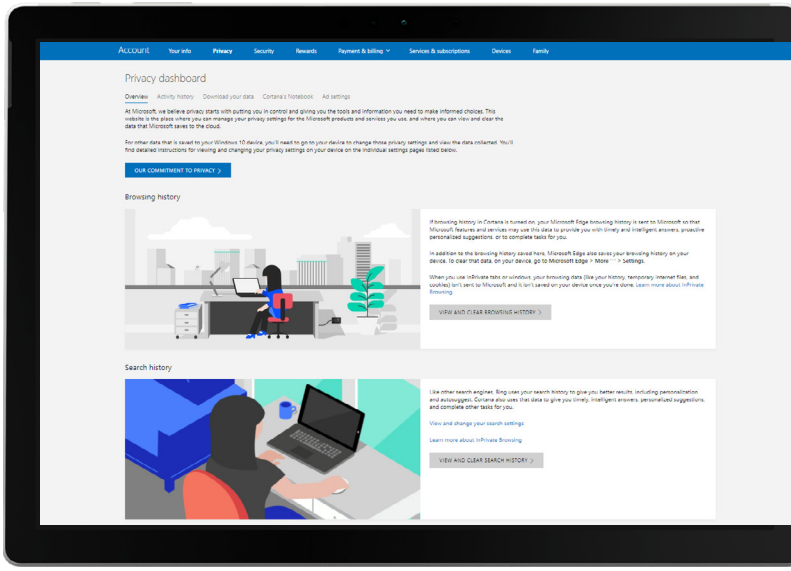
To ensure we are compliant by May 25, 2018, we needed to verify our compliance during the implmentation phase and establish mechanisms for ongoing verification of compliance. Using the standards, policies, and documentation provided by NGP, our compliance and internal audit teams are

completing technical and process reviews to verify our compliance—providing consultation and identifying improvement opportunities.

Investing in new technology

Lastly, we needed to invest in new technology to scale and drive consistency. These investments included the implementation of new compliance solutions; working with our partners to develop new compliance capabilities; creating connections between systems that use personal data; and updating the code of our internal IT, consumer, and commercial products and services with compliance controls to enable our teams to meet compliance obligations.

Our primary investment came from NGP's Technical Foundation Framework, which



outlines the technical requirements, approaches, and areas in which our engineering groups needed to invest to support privacy requirements. In order to deliver on our data subject request obligations, we needed to implement a common infrastructure that standardizes our data governance and enables us to more easily build automation into our systems.

"We had to implement a unified data strategy for the entire company. You can't exercise and scale data subject request execution when products and services are using inconsistent data identifiers and types or in some cases, not even aware of the data they possess."

–Nitesh Bakliwal, Principal Lead Program Manager, Microsoft

We then built a master repository of personal data sources (including employee data), personal data types and identifiers, and third-party systems requesting access to this personal data. To help us scale these efforts, we used machine learning to query select systems for personal information and catalog the in-scope data. Once the data was registered in the data repository, we created an API that integrated actions across our systems—such as automatic encryption, indexing, export, lookup, and selective delete.

As a result of these efforts, we created the consumer Privacy Dashboard—a centralized place for consumers to view and control their personal data across the Microsoft services they use. GDPR includes the right for data subjects to request access to their personal data or opt out of processing. For Microsoft, fulfilling this requirement means enabling data subjects to view how Microsoft consumer services are using their data, call for its removal, download a copy of it, or request to opt out of processing altogether.

While creating a common infrastructure and implementing a unified data strategy requires a significant investment, we believe it will positively change how we handle personal data, increase transparency with our consumers, and enable us to meet the evolving privacy requirements of governments and industry.

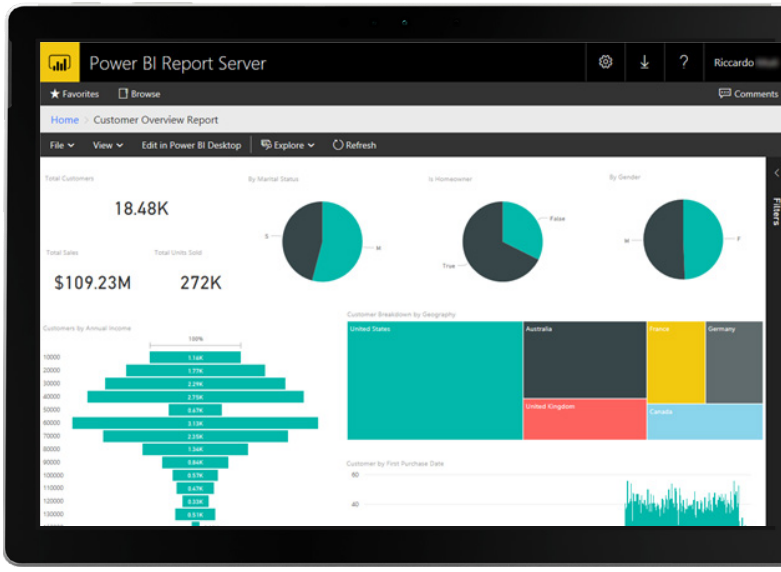
"Our employee data is almost as expansive as our customer data. We not only had to identify all the areas we store HR data, but also where we had personally idenfiable information—like on user devices, in building security logs, dining services, CRM, and Office."

–Damon Buono, Principal Program Manager, Microsoft

Implementation examples

The following examples are some of the key implementation workstreams that are focused on bringing Microsoft into compliance with the GDPR.

Driving visibility through a Power BI GDPR Workstream Dashboard

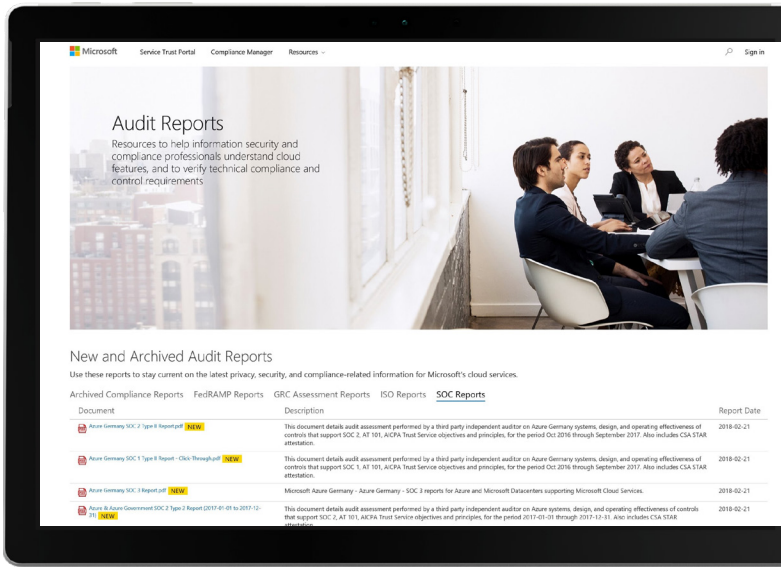


The GDPR represents one of the most complex compliance-focused engineering efforts ever undertaken at Microsoft. Regulatory, compliance, legal, HR, operations, business, and engineering teams have to work together to orchestrate cross-company activities. Keeping everyone in sync, deliverables on target, performance expectations clear, and owners accountable is critical to success. The engineering teams taught the regulatory and compliance teams how to use Microsoft Visual Studio Team Services (VSTS) for project tracking, enabling everyone to work together from a single source of truth. And because VSTS includes Power BI integration and real-time reporting, the separate teams were able to drive transparency, measure progress easily, and collaborate efficiently.

Updating technical documentation in the Service Trust Portal

As a data processor, we have a responsibility to help our customers meet their own compliance obligations. We do this by publishing compliance guides and trust and transparency guides through our Service Trust Portal that demonstrate our compliance with global standards and regulations,

share how we protect customer data, and provide guidance on how to manage cloud data security and compliance across our Microsoft Azure, Office 365, and Dynamics 365 services. To help our customers meet their GDPR compliance obligations, we're updating our documentation to include detailed information on product functionality and controls, product data protection impact assessments, audits, recordkeeping on processing, and information and processes regarding subprocessors.



Scaling engineering efforts with user stories

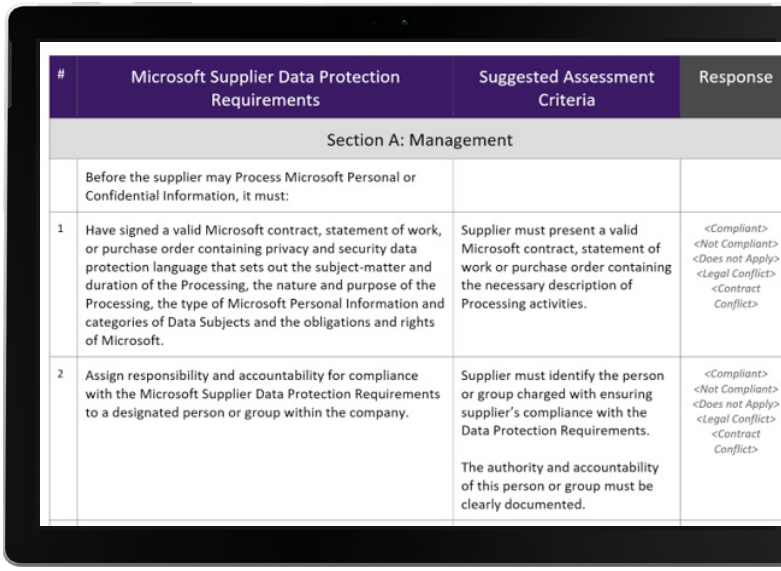
The GDPR's record-keeping requirements call for organizations to be able to demonstrate where personal data is being processed, show what systems have access to that data, and prove a lawful basis for its use. Through the process of understanding everywhere our IT systems are processing personal data and then implementing the necessary data classification and governance controls needed to meet our requirements, we found over 13,000 user stories (data flows from the user experience perspective) that involved in-scope sensitive data. To help scale efforts, our privacy and compliance experts in IT worked with our engineering leads to develop a framework that our implementation engineers could use to map out the data flow of their assigned user stories, identify the needed changes, implement them, and then document inside Visual Studio Online to prove compliance. As a result, we were able to scale our efforts and meet implementation deadlines by tapping into a larger resource pool.

Building our partner ecosystem

Our partner ecosystem is critical to helping our customers attain compliance. Fifty-six percent of Microsoft-surveyed partners requested

both online training and product guidance specific to GDPR requirements. Our sales and marketing teams worked with more than 260 partners to help develop their GDPR solutions, including technical, advisory and consulting, and application development capabilities. We've helped our partners prepare for the GDPR by hosting training events, providing GDPR readiness materials through our Microsoft Partner Network, developing through-partner marketing materials, and partnering to help develop GDPR-specific offerings.

Extending GDPR compliance to our suppliers



#	Microsoft Supplier Data Protection Requirements	Suggested Assessment Criteria	Response
	Section A: Management		
	Before the supplier may Process Microsoft Personal or Confidential Information, it must:		
1	Have signed a valid Microsoft contract, statement of work, or purchase order containing privacy and security data protection language that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Microsoft Personal Information and categories of Data Subjects and the obligations and rights of Microsoft.	Supplier must present a valid Microsoft contract, statement of work or purchase order containing the necessary description of Processing activities.	<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>
2	Assign responsibility and accountability for compliance with the Microsoft Supplier Data Protection Requirements to a designated person or group within the company.	Supplier must identify the person or group charged with ensuring supplier's compliance with the Data Protection Requirements. The authority and accountability of this person or group must be clearly documented.	<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>

The GDPR's broad applicability means we need to ensure our suppliers are compliant as well. We started by updating our supplier Data Protection Requirements (DPRs) to include the personal data handling requirements outlined in our Business Implementation Requirement Documents (BIRDs). All in-scope suppliers were then required to complete a self-attestation documenting their compliance with our DPRs. We also require some suppliers to take additional steps to be compliant—such as independent audits or providing industry certifications—based on the type of data they handle. To enforce compliance, suppliers must be compliant before any data can be transferred or work can start. And to build consistency and rigor into our process, we incorporated this process directly into our procurement process across the entire company. We did this by implementing a third-party risk management solution into our purchase order system, standardizing workflow across the company and providing the needed visibility to our privacy teams to conduct their privacy reviews.

Looking ahead

We have learned a lot on our journey to GDPR compliance, and our business and processes are stronger than ever. We've increased the effectiveness of our data governance program, enhanced our privacy and security programs, and reduced our risk and that of our customers.

The GDPR is one example of the evolving regulatory landscape in the digital age. We will continue to evolve and refine our products, practices, training, and documentation to ensure that we meet all applicable future compliance requirements and ensure we maintain the trust of our customers, employees, and shareholders.

Microsoft has a long history of helping our customers comply with complex regulations. Our cloud services offer the most streamlined way for our customers to take on their GDPR compliance efforts. With a global datacenter footprint, an industry-leading certified compliance portfolio, and services architected to be highly secure by design, Microsoft cloud services provide customers with a simplified and complete approach to the governance of their data and data policies. Lastly, you can count on our extensive global partner ecosystem for expert support as you use Microsoft technologies.

- **Take our free online GDPR assessment**
- **Begin to evaluate your compliance with Compliance Manager**
- **Explore how Microsoft can help you prepare for GDPR today at microsoft.com/gdpr**


Microsoft