European Union General Data Protection Regulation (GDPR) FAQ

Disclaimer

This FAQ is a commentary on the GDPR, as Microsoft interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled.

As a result, this document is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this white paper for your internal, reference purposes only.

Published Oct 2017

Version 1.0

Contents

Version 1.4 – October 2017

Fast FAQ

What is the GDPR?

The General Data Protection Regulation (GDPR) is a comprehensive new privacy law that gives residents of the European Union (EU) greater control over their "personal data" and requires organizations to maintain appropriate security of personal data. Failure to comply with the GDPR could result in significant penalties.

Who needs to know about the GDPR?

The GDPR applies to companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU or that collect and analyze data tied to EU residents. The GDPR applies no matter where personal data is processed.

When will the GDPR come into effect?

The European Parliament approved and adopted the GDPR in April 2016 and enforcement will begin May 25, 2018.

How will the GDPR affect my company?

The GDPR imposes a wide range of requirements on organizations that collect or process personal data, including a requirement to comply with six key principles:

- ***Transparency, fairness, and lawfulness*** *in the handling and use of personal data.* You will need to be clear with individuals about how you are using personal data and will also need a "lawful basis" to process that data.
- *Limiting the processing of personal data to* ***specified, explicit, and legitimate purposes***. You will not be able to re-use or disclose personal data for purposes that are not "compatible" with the purpose for which the data was originally collected.
- ***Minimizing the collection and storage of personal data*** *to that which is adequate and relevant for the intended purpose.*
- *Ensuring the* ***accuracy*** *of personal data and enabling it to be* ***erased or rectified***. You will need to take steps to ensure that the personal data you hold is accurate and can be corrected if errors occur.
- ***Limiting the storage*** *of personal data.* You will need to ensure that you retain personal data only for as long as necessary to achieve the purposes for which the data was collected.
- *Ensuring* ***security, integrity, and confidentiality*** *of personal data*. Your organization must take steps to keep personal data secure through technical and organizational security measures.

You will need to understand what your organization's specific obligations are to the GDPR are and how you will meet them, though Microsoft is here to help you on your GDPR journey.

COMPREHENSIVE FAQ

What rights must companies enable under the GDPR?

The GDPR provides EU residents with control over their personal data through a set of "data subject rights." This includes the right to:

- Access information about how personal data is used
- Access personal data held by an organization
- Have incorrect personal data deleted or corrected
- Have personal data rectified and erased in certain circumstances (sometimes referred to as the "right to be forgotten")
- Restrict or object to automated processing of personal data
- Receive a copy of personal data

How much can companies be fined for noncompliance?

Companies can be fined up to €20m or 4% of annual global turnover, whichever is greater, for failure to meet certain GDPR requirements. Additional individual remedies could increase your risk if you fail to adhere to GDPR requirements.

How do I know if the data that my organization is processing is covered by the GDPR?

The GDPR regulates the collection, storage, use, and sharing of "personal data." Personal data is defined very broadly under the GDPR as *any* data that relates to an identified or identifiable natural person.

Personal data can include, but is not limited to, online identifiers (e.g., IP addresses), employee information, sales databases, customer services data, customer feedback forms, location data, biometric data, CCTV footage, loyalty scheme records, health and financial information and much more. It can even include information that does not appear to be personal – such as a photo of a landscape without people – where that information is linked by an account number or unique code to an identifiable individual. And even personal data that has been pseudonymized can be personal data if the pseudonym can be linked to a particular individual.

You should also be aware that the processing of certain "special" categories of personal data – such as personal data that reveals a person's racial or ethnic origin, or concerns their health or sexual orientation – is subject to more stringent rules than the processing of "ordinary" personal data.

This evaluation of personal data is highly fact-specific, so we recommend engaging an expert to evaluate your specific circumstances.

My organization is only processing data on behalf of others. Does it still need to comply with the GDPR?

Yes. Although the rules differ somewhat, the GDPR applies to organizations that collect and process data for their own purposes ("controllers") as well as to organizations that process data on behalf of others ("processors.") This is a shift from the existing Data Protection Directive, which applies to controllers.

How would my company be impacted if I share EU personal data with a company that is not GDPR compliant?

Under the GDPR, your organization can only share data with another organization for processing if it enters in to an agreement that provides guarantee they will "implement appropriate technical and organizational measures" such that the rights of data subjects are protected and the processing requirements of the GDPR are satisfied. See Article 28 of the GDPR for additional requirements.

What specifically is deemed personal data?

Personal data is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. Personal data can include:

Examples of personal data include:

Identity

- Name
- Home address
- Work address
- Telephone number
- Mobile number
- Email address
- Passport number
- National ID card
- Social Security Number (or equivalent)
- Driver's license
- Physical, physiological, or genetic information
- Medical information
- Cultural identity

Finance

- Bank details / account numbers
- Tax file number
- Credit/Debit card numbers
- Social media posts

Online Artifacts

- Social media posts
- IP address (EU region)
- Location / GPS data
- Cookies

How does the GDPR apply to children?

The GDPR includes specific protections for children. It generally provides that the consent of children must be "explicit." GDPR set the age of consent, in the online context, at 16. But Member states may individually set the age of consent anywhere between 13 and 16 years old.

Do we need to ask for consent to collect, store and process personal data from my employees and my customers?

Organizations must have a legal basis for processing personal data, which could include:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

My company has offices and personnel outside Europe. Do I only need to cover personnel in Europe?

The GDPR applies more broadly than might be apparent at first glance. Unlike privacy laws in some other jurisdictions, the GDPR is applicable to organizations of all sizes and all industries.

Specifically, the GDPR applies to:

• processing of *anyone's* personal data, if the processing is done in the context of the activities of an organization established in the EU (regardless of where the processing takes place);

• processing of personal data of individuals who reside in the EU by an organization established *outside* the EU, where that processing relates to the offering of goods or services to those individuals or to the monitoring of their behavior.

The EU is often viewed as a role model on privacy issues internationally, so we also expect to see concepts in the GDPR adopted in other parts of the world over time.

Am I allowed to transfer data outside of the EU?

Yes, however the GDPR strictly regulates transfers of personal data of European residents to destinations outside the European Economic Area. You may need to set up a specific legal mechanism, such as a

contract, or adhere to a certification mechanism in order to enable these transfers. Microsoft details the mechanisms we use in the Online Services Terms.

Under what basis does Microsoft facilitate the transfer of personal data outside of the EU?

Personal data is not restricted to Europe under GDPR, but there are requirements an organization must satisfy to transfer personal data outside of Europe. The GDPR requires that organizations that move data outside of Europe have a lawful basis to do so and use "appropriate safeguards."

The EU has defined a number of "appropriate safeguards" for the transfer of personal data, including:

- Model Clauses—a standard contract, the content of which is defined by the EU, that is entered into between service providers and their customers.
- EU-US Privacy Shield—the subject of an agreement between the EU and the US, it creates a process for companies to self-certify to key protections for data.
- Binding Corporate Rules (BCRs)—a complex process that involves entering into an agreement with relevant data protection authorities in the EU.
- Determination that the receiving country has equivalent data protections to those in the EU. The list of countries can be found here.

Microsoft has long used the Model Clauses as a basis for transfer of data for its enterprise online services. These clauses are incorporated into all of our volume licensing agreements via the Online Services Terms. The EU has specifically validated our approach with Model Clauses. And when the EU-US Privacy Shield became available a year ago, Microsoft was the first company to sign on.

Customers can find Microsoft's certification to the Privacy Shield here (and via the Online Services Terms)..

If I host my data in a datacenter in the EU, even though I do not have a business presence there, do I need to comply with the GDPR?

The GDPR applies to companies, government agencies, non-profits, and other organizations established in the EU as well as organizations, wherever located, that offer goods and services to people in the EU or that collect and analyze data tied to EU residents, including employees.

The determination if GDPR applies is factually and scenario specific so it is impossible to state with certainty. You would need to consult with your legal counsel to make that determination. Microsoft does not distinguish between commercial customers who are, or are not, subject to GDPR. Instead, we provide the benefit of GDPR's elevated protections to all commercial customers, regardless of where they are located. If your personal data are subject to GDPR and Microsoft is acting as a processor or subprocessor, you will automatically get the benefits of Microsoft's GDPR commitments and protections set out in our Online Services Terms.

My company is solely based in the UK. What does that mean in the context of Brexit?

Companies based in the UK should assume that they will be subject to a GDPR-like law upon the exit of the UK from the EU. The UK Government has released a Statement of Intent outlining its adoption of a Data Protection Bill, which is founded on the GDPR.

What are Processors and Controllers?

A controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Does the GDPR apply to both processors and controllers?

Yes, the GDPR applies to both controllers and processors. Controllers must only use processors that take measures to meet the requirements of the GDPR.

Under the GDPR, processors face additional duties and liability for noncompliance, or acting outside of instructions provided by the controller, as compared to the Data Protection Directive. 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 subprocessors it engages meet these requirements

I have data retention requirements through compliance. Do these override the right to erasure?

Where there are legitimate grounds for continued processing and data retention, such as "for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject" (Article 17(3)(b)), the GDPR recognizes that organizations may be required to retain data. You should, however, make sure you engage your legal counsel to ensure that the grounds for retention are weighed against the rights and freedoms of the data subjects, their expectations at the time the data was collected, etc.

Does my business need to appoint a Data Protection Officer (DPO)?

It depends on several factors identified within the regulation. Article 37 of the GDPR states that controllers and processors shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

How does the GDPR change an organization's response to personal data breaches?

The GDPR will change data protection requirements and make stricter obligations for processors and controllers regarding notice of personal data breaches. Under the new regulation, the processor must notify the data controller of a personal data breach, after having become aware of it, without undue delay. Once aware of a personal data breach, the controller must notify the relevant data protection authority within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, controllers will also need to notify impacted individuals without undue delay. Additional guidance on this topic is being developed by the EU's Article 29 Working Party.

Microsoft products and services—such as Azure, Dynamics 365, Enterprise Mobility + Security, Office 365, and Windows 10—have solutions available today to help you detect and assess security threats and breaches and meet the GDPR's breach notification obligations.

Do we need to carry out data protection impact assessments and what do they involve?

You must carry out data protection impact assessments if your processing activities present high risks to the rights and freedoms of individuals. These assessments generally involve identifying and documenting privacy risks raised by proposed processing, and planning mitigation measures to help control and minimize those risks. See GDPR Article 35 for more.

In some cases, organizations must also consult data protection authorities before undertaking processing.

Is Microsoft making any commitments in its volume licensing agreements to comply with the GDPR?

Yes. Microsoft has proactively made contractual commitments to its Volume Licensing customers that provide specific assurances related to GDPR.

Our GDPR contract terms govern our processing and security of personal data, transfers of personal data to third countries, confidentiality requirements for individuals authorized to access personal data, and use of sub-processors. They also define our commitments to help you: respond to data subjects' requests to correct, amend, or delete their personal data; delete or return personal data when our provision of services ends; respond to personal data breaches; and demonstrate your compliance with the GDPR.

Our GDPR terms are incorporated into the Online Services Terms available at microsoft.com/licensing. Accordingly, they are available automatically to all our customers who enter into a volume licensing agreement without need for amendment.

Where can I learn more about the GDPR?

To learn more about the General Data Protection Regulation (GDPR) please visit www.microsoft.com/gdpr where you can also learn more about how specific Microsoft products can help you prepare to comply with the GDPR, please see the sections on Azure, Dynamics 365, Enterprise Mobility + Security, Office 365, and Windows 10.

FastTrack for Microsoft 365 GDPR Specific FAQs

How is FastTrack involved or going to help me with the Global Data Protection Requirements (GDPR)?

Microsoft FastTrack is a service benefit*, our customer success service to help businesses realize business value faster with the Microsoft Cloud. FastTrack helps to:

- Migrate email, content, and light up Microsoft 365 services
- Deploy and securely manage devices
- Enable your business and gain end-user adoption.

Microsoft FastTrack is an ongoing and repeatable service benefit, available to customers, and delivered by Microsoft engineers and specialists to help customers or partners to plan, onboard and drive adoption/usage and help to move to the cloud confidently and at customers' and partners' own pace.

As we help customers with specific deployments and migration to our Online Services, Microsoft FastTrack commits to being GDPR compliant by the time enforcement begins on May 25, 2018. As part of the FastTrack professional service benefit, we also work with our customer's existing partner(s) or refer Partners for deployment and adoption assistance.

Refer to https://FastTrack.Microsoft.com for further information.

*"Service benefit" is considered a "professional service" as defined by our OST and MBSA.

As part of the Microsoft FastTrack customer success service, will FastTrack advise on what online service features need to be turned on and configured to be "GDPR compliant"?

The FastTrack engineers and specialists are industry experts in the planning for the scenarios and business value customers or partners want to achieve, and are focused on the planning, deployment and driving adoption of the products and services to help customers or partners achieve these objectives. Learn more about how Microsoft's products and services support your compliance with GDPR via our Trust Center website. We encourage our customers and partners to work with a legally qualified professional to discuss GDPR, how it applies specifically to their organization, and how best to ensure compliance.

As part of our FastTrack professional service benefit, we also work with our customer's existing partner(s) or refer Partners for deployment and adoption assistance. You can learn more about Partners specialized in GDPR who are available to help Microsoft Partners toward compliance as described on the Trust Center's GDPR page here. You can reference our Trusted Cloud/GDPR Web page to assess your readiness for the GDPR and how you can accelerate GDPR compliance with the Microsoft Cloud, and use Microsoft FastTrack for deployment assistance.

Does Microsoft handle data as part of a FastTrack engagement in compliance with GDPR?

GDPR compliance is specific to a customer's data collected, use scenarios, and industry sectors or vectors. We advise that our customers should work with their own legal and compliance teams to determine GDPR requirements for encryption, data handling, and overall GDPR requirements. Key to

note, Microsoft products and services such as Azure, Dynamics 365, Enterprise Mobility + Security (EMS), Office 365, SQL Server / Azure SQL Database, and Windows 10 offer robust encryption for data in transit and data at rest.

As part of a FastTrack engagement, will FastTrack advise on GDPR compliance?

We advise that our customers should work with their own legal and compliance teams to determine GDPR requirements for encryption and overall GDPR requirements. GDPR compliance is specific to a customer's data collected, use scenarios, and industry sectors or vectors.

As part of a FastTrack engagement, will FastTrack help me conduct data audits during a deployment?

GDPR compliance is specific to a customer's data collected, use scenarios, and industry sectors or vectors. We advise that our customers should work with their own legal and compliance teams to determine GDPR requirements for conducting data audits and overall GDPR requirements.

Does FastTrack have the responsibility to help me architect assigned data processors due to changes in regulatory oversight that have direct obligations under GDPR?

The GDPR applies to both data controllers and processors, the data controller of our customer is responsible for the architecture and the data processor that will process the data for the controller according to GDPR requirements. Microsoft and our partners can help you meet your policy, people, process, and technology goals on your journey to GDPR compliance as a thought leader in the industry on the GDPR. Go here for additional resources to review.

Is Microsoft FastTrack GDPR certified or compliant?

For the pre- and post-migration tools or other Online services used by Microsoft FastTrack, Microsoft FastTrack commits to being GDPR compliant by the time enforcement begins on May 25, 2018, where our Online Services will be operated by our top security standards, and meeting GDPR compliance. As part of our FastTrack customer success service, we also work with our customers existing partner(s) or refer Partners for deployment and adoption assistance.

Does FastTrack help support me, and accelerate my deployment, to be GDPR compliant?

Microsoft FastTrack is a customer success service committed to delivering faster deployments, ROI and driving higher adoption for your employees or end users of Microsoft products and services. With that in mind, as customers or partners submit a request for assistance through Microsoft FastTrack, we will begin our process to appropriately deploy the Microsoft products and services for our customers or partners.

Are Microsoft products that you are deploying for me GDPR certified or compliant?

We are committed to GDPR compliance across our cloud services when enforcement begins May 25, 2018, and provide GDPR related assurances in our contractual commitments. While FastTrack is a

professional service versus a product, all of our Microsoft pre-migration, post-migration, products, migration tools, processes and services provided will be GDPR compliant -offered only by Microsoft or a qualified partner / vendor.

To learn more about how Microsoft products and services can help you prepare to comply with the GDPR, please see How our products help you meet GDPR requirements.