An Overview of the General Data Protection Regulation (GDPR)

Table of Contents

Disclaimer

This white paper 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 white paper 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 white paper, 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 May 2017

Version 1.0

Introduction

The General Data Protection Regulation, or GDPR, will set a new bar globally for privacy rights, security, and compliance. At Microsoft, we believe privacy is a fundamental right and that the GDPR is an important step forward in protecting and enabling the privacy rights of individuals.

This white paper serves as an introduction to GDPR and its key concepts. For more details on beginning your GDPR journey, and how Microsoft can help you, please visit www.microsoft.com/gdpr.

What is the GDPR?

The GDPR is the European Union's new data protection law. It replaces the Data Protection Directive (Directive"), which has been in effect since 1995.

While the GDPR preserves many of the principles established in the Directive, it is a much more ambitious law. Among its most notable changes, the GDPR gives individuals greater control over their personal data and imposes many new obligations on organizations that collect, handle, or analyze personal data. The GDPR also gives national regulators new powers to impose significant fines on organizations that breach the law.

When does the GDPR take effect?

The GDPR takes effect on May 25, 2018. The GDPR actually became law in April 2016, but given the significant changes some organizations will need to make to align with the regulation, a two-year transition period was included.

Organizations should not expect any grace period from regulators beyond May 25, 2018. Some EU member state regulators have already gone on record to say there will be no enforcement holiday for organizations that fail to comply.

What are the main requirements of the GDPR?

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, fairnesss, 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.

Does the GDPR apply to my organization?

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.

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" includes any data that relates to an identified or identifiable individual. This can include data such as 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. Indeed, the term is so broad that 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.

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 Directive, which applies primarily to controllers.

What risks does my organization face if it does not comply?

For the last several decades, European privacy laws have generally not included significant fines for breaches. That will change dramatically under the GDPR. The maximum fine for serious infringements will be the greater of €20 million or four percent of an organization's annual global revenue. In addition, the GDPR empowers consumers (and organizations acting on their behalf) to bring civil litigation against organizations that breach the GDPR.

You say that organizations must be "transparent." What does that mean?

The GDPR includes detailed rules about what you must tell individuals about your processing of personal data. This includes, among other things, information about why the personal data is being processed, how long the data will be stored (or, if that is not possible, the criteria used to determine that period), with whom the personal data will be shared, and whether the personal data will be transferred outside the European Economic Area. This information must be presented in a way that is clear and easily accessible. You should review your disclosures against the GDPR's requirements carefully.

What does it mean that organizations must have a "legal basis" for processing personal data?

Under the GDPR, you can't process personal data simply because you want to. Instead, you must be able to point to a "legal basis" for processing. The GDPR provides several grounds for processing, including where the processing is necessary to perform a contract, where an an individual has consented to the processing of their data, or where the processing is in the organization's "legitimate interest" (assuming that interest is not outweighed by the individual's rights).

What are the key terms to be aware of in the GDPR?

Article 4 of the GDPR includes a list of defined terms used in the regulation. Several are particularly important:

"Controller" means the 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.

"Processor" means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

What about security under the GDPR?

The GDPR requires you to take measures to keep personal data secure. This includes "organizational measures," such as limiting the number of people inside your organization who can access personal data, and "technical measures," such as encryption.

The GDPR doesn't mandate the exact security measures organizations must take, however. Instead, it requires organizations to determine security measures themselves, depending on factors like the nature of the personal data, its sensitivity, and the risks involved in the processing.

There are many types of security risks to consider, from physical intrusion to rogue employees, to accidental loss, and to online hackers. Building risk management plans and taking risk mitigation steps, such as password protection, audit logs, and encryption, can help ensure compliance.

Are the six principles described above the only requirements set out by the GDPR?

No. There are many more requirements in the GDPR. For example, the GDPR gives individuals a number of rights over their personal data, such as the right to access or correct their personal data or to have it deleted. You will need to have plans in place to respond to individuals who want to exercise these rights.

You may also need to comply with other requirements, such as observing special rules about profiling individuals; keeping careful records of processing; following principles of "privacy by design" and "privacy by default"; appointing a data protection officer; reporting data breaches; carrying out data protection impact assessments; and limiting transfers of data to certain destinations outside the European Economic Area, among other obligations.

You mention individuals' rights. Can you say more?

Individuals have many rights under the GDPR that organizations must respect. This includes rights to access the personal data you hold about them; to have their personal data corrected or deleted (the "right to be forgotten"); to ask you to stop processing their personal data; to object to direct marketing; and to revoke consent for certain uses of their personal data. Additionally, the right to data portability means you must provide individuals their personal data in a way that makes it easy for them to move their personal data elsewhere.

How does the GDPR require "privacy by design" and "by default"?

Under the GDPR, you are expected to incorporate privacy features and functionality into your products and services from the time they are first designed. The GDPR doesn't dictate the features. Instead, you should develop features based on factors like the nature of the processing and the privacy risks it poses; the need for security; and the cost of implementation. You must also implement measures to ensure that, by default, no more data is processed than is necessary.

What kind of record-keeping does the GDPR require?

Large organizations must maintain detailed internal records of processing activities. This includes records about the purposes of processing, the categories of personal data processed, transfers of personal data outside the European Economic Area, and the security measures employed to protect data.

Auditing tools can help you ensure that any processing of personal data – whether it be collection, use, sharing, or otherwise – is tracked and recorded.

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.

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

What does the GDPR require if a data breach occurs?

The GDPR defines a "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." In the event of a personal data breach, the GDPR requires notice to regulators within 72 hours of detecting the breach. You may also need to notify affected individuals if there is a significant risk of harm due to the breach.

What if my organization transfers data to countries outside of the EU?

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.

If my business uses a vendor to process personal data, what do I need to know?

The GDPR requires controllers to only use processors that 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. In the context of enterprise online services such as Office 365, Microsoft is a processor and our customers are the controller.

Microsoft recently offered its volume licensing customers a contractual commitment, known as the "GDPR Terms", to meet the GDPR's contractual requirements with regard to Microsoft's enterprise online services. Among other things, the GDPR Terms commit that Microsoft will only process data in accordance with a controller's instructions; will provide controllers with advance notice and an opportunity to object to new sub-processers; will support controllers in managing data subject requests; will abide by the GDPR breach notification requirements; will assist controllers with data protection impact assessments and related consultations; and will ensure the security of processing in accordance with the GDPR.

Can Microsoft Help Us Meet the Requirements of the GDPR?

Yes. Microsoft stands ready to help organizations meet the GDPR compliance deadline of May 25, 2018. The Microsoft Cloud can help you achieve compliance. For more information about how we can help, please visit www.microsoft.com/gdpr.