Microsoft

Getting to know the GDPR

What it means for Australian and New Zealand businesses

Contents

This document is a commentary on the General Data Protection Regulation (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.

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 or your organisation. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organisation, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. This document 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 document for your internal, reference purposes only.

Published April 2018
Version 1.0

What does the GDPR mean for you?

On 25 May 2018, a new European Union (EU) privacy regulation will come into effect with wide-reaching implications for organisations in Australia and New Zealand that offer goods and services to people in the EU, or collect and analyse data tied to EU residents.

This regulation, called the General Data Protection Regulation (GDPR), sets a new global bar for privacy rights, security and compliance. It enhances individual privacy rights and imposes new requirements on the collection, storage and use of personal information. Among other things, it details how organisations must:

- identify and secure personal data in their systems
- be open and transparent about their data usage
- detect and report personal data breaches.

Microsoft and our customers are now on a journey to realise these important goals. For some, it will be a difficult path. But it's a path worth taking as we all strive to ensure that privacy is viewed and treated as a fundamental right.

We prepared this document as part of our commitment to partnering with you on your GDPR journey. The document provides an overview of the GDPR, includes compliance guidelines, clarifies some common misconceptions and outlines key differences between the GDPR and your obligations under Australian and New Zealand privacy laws. We have also shared some examples of steps you can take with Microsoft to start on the path to compliance.

We look forward to sharing updates about how we can help you comply with this important new law and, in the process, advance personal privacy protections. Please visit www.microsoft.com/gdpr to find additional resources and to learn more about how Microsoft can help with your compliance needs.

We trust you will find this paper useful, and look forward to helping you meet your policy, people, process and technology goals on your journey to GDPR compliance.

Tom Daemen
Director, Corporate, External and Legal Affairs
Microsoft Australia

Introducing the GDPR – the key points

Before describing the specific ways that Microsoft can help you prepare for the GDPR, we'd like to address some common questions from Australian and New Zealand organisations about the regulation and what it may mean for businesses.

What is the GDPR?

The GDPR is a new privacy regulation that applies across the EU. It gives individuals who are located in the EU (EU Data Subjects) more control over their personal data, improves transparency about the use of personal data and requires security and controls to protect personal data.

In doing so, the GDPR imposes many new obligations on organisations that collect, handle or analyse personal data. It requires that organisations respect and protect personal data – no matter where it is sent, processed or stored. Failure to comply with the GDPR could result in significant penalties.

Enhanced personal privacy rights

Increased duty for protecting data

Mandatory breach reporting

Significant penalties for non-compliance

When does the GDPR take effect?

The GDPR takes effect on 25 May 2018 and replaces the current EU's Data Protection Directive.

Does the GDPR apply to organisations in Australia and New Zealand?

The GDPR applies more broadly than may be apparent at first glance. The law imposes new rules on individuals, companies, public authorities, government agencies, non-profit organisations and other entities that offer goods and services to EU Data Subjects, or that collect and analyse data tied to the behaviour of EU Data Subjects – whether or not those organisations are located in the EU.

In other words, an Australian or New Zealand company will have to comply with the GDPR if it targets EU consumers or monitors any personal data of EU Data Subjects.

Who are the EU Data Subjects?

An EU Data Subject includes:

- EU citizens
- EU residents
- Temporary residents of the EU
- People who are on a vacation or business trip in the EU.

GDPR: Not just Europe

The GDPR applies more broadly than many people think. The law imposes new rules on individuals, companies, government agencies, non-profits, and other organisations that offer goods and services to EU Data Subjects or that collect and analyse data tied to EU Data Subjects – no matter where their personal data is processed.

What is 'personal data' under the GDPR?

The GDPR seeks to protect the 'personal data' of EU Data Subjects. This is data from which a living individual can be identified, whether directly or indirectly.

Australian and New Zealand organisations will be familiar with the term 'personal information'. It is important to note that the definition of 'personal data' under the GDPR is broader than the definition of 'personal information' under the *Australian Privacy Act 1988* (AU Privacy Act) and the *New Zealand Privacy Act 1993* (NZ Privacy Act).

The GDPR looks at whether the data could be "reasonably likely to be used" to identify an individual. If it can, then it is most likely personal data. This could be a name, an ID number, location data, an online identifier (e.g. an IP address if held by an Internet Service Provider (ISP)) or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The definition of 'personal information' under the AU and NZ Privacy Acts does not include a list of the types of information specifically included, such as location data and online identifiers.

Under the GDPR, there are additional protections and restrictions for special categories of personal data and sensitive personal data.

This is data relating to an individual's:

- racial or ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- health or sex life
- sexual orientation
- genetic data or biometric data.

It all comes down to personal data

GDPR analysis begins with understanding what data exists and where it resides. The GDPR regulates the collection, storage, use and sharing of broadly defined personal data.

For example, personal data can reside in:

- customer databases
- feedback forms filled out by customers
- email content
- photos
- CCTV footage
- loyalty program records
- HR databases.

Who are controllers and processors under the GDPR?

Privacy laws in Australia and New Zealand don't differentiate between the types of organisations that deal with personal data. The GDPR differentiates two important roles assumed by organisations that fall under its umbrella: controllers and processors.

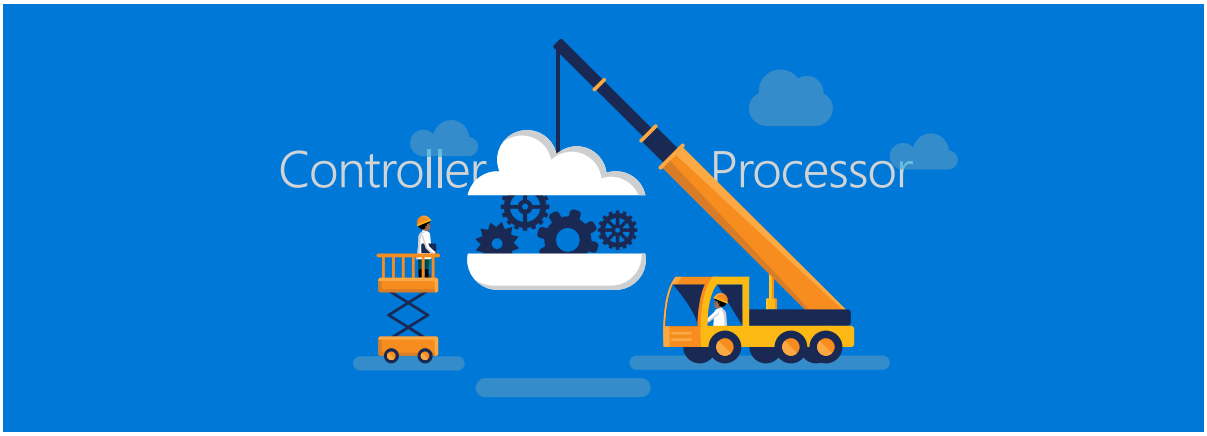
Most obligations under the GDPR fall on the data controller who determines the purposes and means of processing personal data. The controller can act alone or jointly with others.

The GDPR also imposes specific and separate duties and obligations on data processors. A processor is an entity that processes personal data on behalf of a data controller.

The controller controls the processing of personal data, whereas the processor performs the processing on the controller's behalf. The same organisation can act as both controller and processor, or the two roles can belong to two separate organisations. In most cloud services relationships, the customer (e.g. an organisation such as yours) is the controller and the cloud services provider (e.g. Microsoft) is the processor that carries out the processing on behalf of the customer.

Controllers and processors are specifically required to demonstrate compliance with the GDPR. They must demonstrate that they have undertaken appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

The GDPR prohibits organisations from using third-party data processors unless those processors agree by contract to implement the technical and organisational requirements of the GDPR. As a processor, Microsoft has extensive expertise in protecting data, championing privacy and complying with complex regulations, and is committed to GDPR compliance. Microsoft makes available the contractual obligations required of processors under the GDPR, including assisting our customers to respond to requests from Data Subjects to correct, amend or delete personal data. We also help our customers to detect and report personal data breaches and demonstrate their compliance with the GDPR.



What activities are caught by the GDPR?

There is a common misconception that organisations located outside the EU do not have to comply with the GDPR. In fact, the GDPR may capture your organisation even if the AU Privacy Act and NZ Privacy Act do not currently apply to your business.

As mentioned previously, the GDPR will apply to all organisations that control or process the personal data of EU Data Subjects and that are:

- located and conducting activities in the EU, regardless of where the data processing occurs
- not located in the EU but are offering goods or services to EU Data Subjects
- not located in the EU but are monitoring the behaviour of EU Data Subjects (to the extent that the relevant behaviour takes place in the EU).

The GDPR may also capture activities that the AU Privacy Act does not currently regulate. For example, the AU Privacy Act does not apply to businesses with an annual turnover of less than A$3 million but there is no such threshold in the GDPR.

The table on page 8 offers useful guidelines on factors that may be relevant in determining whether an organisation offers goods or services to, or monitors, EU Data Subjects.

Capturing additional activities

The AU Privacy Act does not apply to businesses with an annual turnover of less than A$3 million but there is no such threshold in the GDPR.

New and additional obligations

A common misconception is that if an organisation already complies with Australian or New Zealand privacy laws, that is enough. In fact, while there are areas of overlap between the AU Privacy Act and the NZ Privacy Act and the GDPR, the GDPR places new and prescriptive obligations on organisations that fall within its scope. To understand these additional obligations in more detail, see pages 11–13.

Offering goods or services

- Use of an EU language on a website
- Offering EU customers the ability to pay in a local EU currency when purchasing goods or services
- Paying a subscription fee to a search engine to enable access to a particular EU country
- Arranging with a third party to target advertisements to EU Data Subjects with EU contact details (such as addresses or phone numbers)
- Using testimonials from individuals located in the EU
- Using a localised EU domain name (e.g. '.fr' or '.de') and/or telephone number
- Offering goods or services of a certain nature (e.g. for the purpose of international tourism)
- Conducting any type of tracking on the internet, such as email surveillance

Monitoring

- Profiling (analysing or predicting behaviour)
- Using location tracking (geo-location)
- Tracking wellness, fitness and health via wearable devices
- Using cookies (persistent rather than static), particularly where a number of different cookies combined can be used to track an EU Data Subject)

Each situation will be different and the factors above should be considered collectively. Depending on the circumstances, other factors may also be relevant. See page 15 for examples.

I'm already complying with the AU Privacy Act or NZ Privacy Act – what's new?

The GDPR will create new and additional obligations on Australian and New Zealand organisations that it regulates.

Let's take a closer look. The following table sets out the GDPR obligations that are additional to your existing Australian and New Zealand privacy law obligations.

The right to restrict and object to processing	Under the GDPR, in certain circumstances individuals have a right to ask that their personal data no longer be processed. The grounds for objection are contested accuracy, unlawful processing, the data is no longer required, or the legitimate interests of the controller do not override those of the EU Data Subject.
Consent	Organisations that are regulated by the GDPR must ensure that any consent for processing personal data is freely given, clear, specific, informed and unambiguous, either through a statement or affirmative action (such as ticking a box or choosing particular technical settings). Consent cannot be bundled with other consents or terms, and any consent that is bundled will not be binding. In contrast, under the AU Privacy Act, consent can be express or implied, and the appropriate form depends on the circumstances. There are also specific consent conditions that apply to children and sensitive personal data.
The right to be forgotten (or the right to erasure)	In some circumstances, EU Data Subjects have the right to request their data be deleted by an organisation. An example of such a circumstance is when the Data Subject believes that the data is no longer necessary for the purpose it was collected. Organisations must comply with these requests without undue delay and within one month, unless they are required by law to retain that data.

Data breach notification

Data controllers must notify the appropriate authorities within 72 hours of becoming aware of a data breach. Additionally, if the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations will also need to notify affected individuals without undue delay.

There is no equivalent requirement under the NZ Privacy Act, although the new NZ Privacy Bill introduced in March this year may signal a change.

While the GDPR's data breach notification rule is similar to notification requirements imposed recently under Australia's Notifiable Data Breach (NDB) scheme, there is no obligation to assess whether or not a data breach is eligible to be notified (as is the case in Australia). A breach must simply be notified regardless of the potential impact it could have on an EU Data Subject.

The relevant supervisory authority will be the appointed public authority in the EU member state in which the EU Data Subject is located.

For Australian organisations subject to the GDPR, these are separate notification obligations in addition to notifying the Office of the Australian Information Commissioner and affected individuals in Australia in accordance with Australia's NDB scheme.

Notifications under the GDPR rule also require a substantially shorter timeframe than Australia's NDB scheme, which requires notification "as soon as practicable" after becoming aware of an "eligible" data breach. (Organisations in Australia have up to 30 days after becoming aware of a data breach to assess whether or not it is an eligible data breach.)

Appointment of a Data Protection Officer

It is mandatory for certain organisations that are subject to the GDPR (e.g. organisations that conduct large-scale monitoring of EU Data Subjects or large-scale processing of sensitive information) to appoint a Data Protection Officer (DPO). The DPO will have the primary objective of monitoring and ensuring the organisation's compliance with the GDPR.

Data portability

EU Data Subjects have the right to request and receive the personal data provided by them to a controller in a structured, commonly used and machine-readable format. They also have the right to provide that data to another controller.

In addition to the general rights to access data under Australian and New Zealand privacy laws, the GDPR also gives an individual the right to require a data controller to transmit their data to another controller where this is technically possible. This right only applies where the processing of that data has been carried out by automated means. It will not apply if the transmission will adversely affect the public interest, the controller's official authority, or the rights or freedoms of others.

Appointment of a representative in the EU	If the GDPR applies to an organisation located outside the EU, that organisation must appoint a representative located in one of the EU member states where the relevant EU Data Subjects are located. Organisations are exempt from this requirement if the organisation's data processing is occasional, unlikely to be a risk to individuals, and does not involve large-scale processing of sensitive personal data.
Compulsory Data Protection Impact Assessment	Organisations that are subject to the GDPR must run a Data Protection Impact Assessment on any processing activities considered to present a high risk to the rights and freedoms of individuals (the risk may be considered to be greater when they involve vulnerable Data Subjects, e.g. children or employees). In Australia, only Commonwealth Government agencies are required to conduct privacy impact assessments of this kind.
Data transfer restrictions	The GDPR restricts the transfer of personal data for processing outside the EU unless the EU Commission's Data Protection Board determines that the destination country has an adequate level of protection for data transfers. To date, Australia is not on the list of permitted countries, although New Zealand is. This means that transfers of personal data from the EU to Australia (or from Australia to another unpermitted country) for processing will only be allowed where the controller or processor can show it has appropriate safeguards and legal remedies open to the EU Data Subject to enforce such obligations (e.g. contractual rights).
Automated processing	An EU Data Subject can object to automated decision-making (including profiling) that has legal or similarly significant effects on them (e.g. an online decision to award a loan or a recruitment aptitude test). This right will not apply in certain circumstances, such as where it is necessary for the performance of a contract with the EU Data Subject, with consent, or where the processing is required by law provided that the controller safeguards the EU Data Subject's right to obtain human intervention and contest the automated decision.
Privacy by design	The GDPR now requires controllers to implement data protection measures from the onset of designing and implementing their business systems and processes. This is similar to regulations in Australia.
Records of processing activities	Controllers and processors are required to maintain a record of processing activities under the GDPR (except for entities with fewer than 250 employees in limited circumstances).

Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to the processing of their personal data
- Export personal data

Controls and notifications

Organisations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies

Organisations are required to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT and training

Organisations will need to:

- Train privacy personnel and employees
- Audit and update data policies
- Employ a Data Protection Officer (in certain circumstances)
- Create and manage compliant vendor contracts

What are the consequences of breaching the GDPR?

EU regulators will be able to pursue an organisation located outside the EU, if the GDPR applies to that organisation and that organisation fails to comply with the GDPR.

An organisation may be required to pay compensation to a person who has suffered damage as a result of it failing to comply with the GDPR. The organisation may also have to pay fines imposed by a relevant EU supervisory authority.

For a serious breach of the GDPR, the maximum fine is up to 4 per cent of the global annual turnover of the company or €20 million, whichever is greater. Other contraventions may be subject to the greater of up to €10 million, or 2 per cent of the global annual turnover, whichever is greater. These levels of fines are substantially more than those that may be imposed under the AU Privacy Act or the NZ Privacy Act.

Some organisations could also face other practical consequences of breaching the GDPR. These may include temporary or permanent bans on processing personal data of EU Data Subjects in the EU country in which the GDPR was breached, which can interfere with business activities.

Significant penalties

For a serious breach of the GDPR, the maximum fine is up to 4 per cent of the global annual turnover of the company or €20 million, whichever is greater.

Other contraventions may be subject to up to €10 million or 2 per cent of the global annual turnover, whichever is greater. These fines are substantially greater than those that may be imposed under the AU Privacy Act or the NZ Privacy Act.

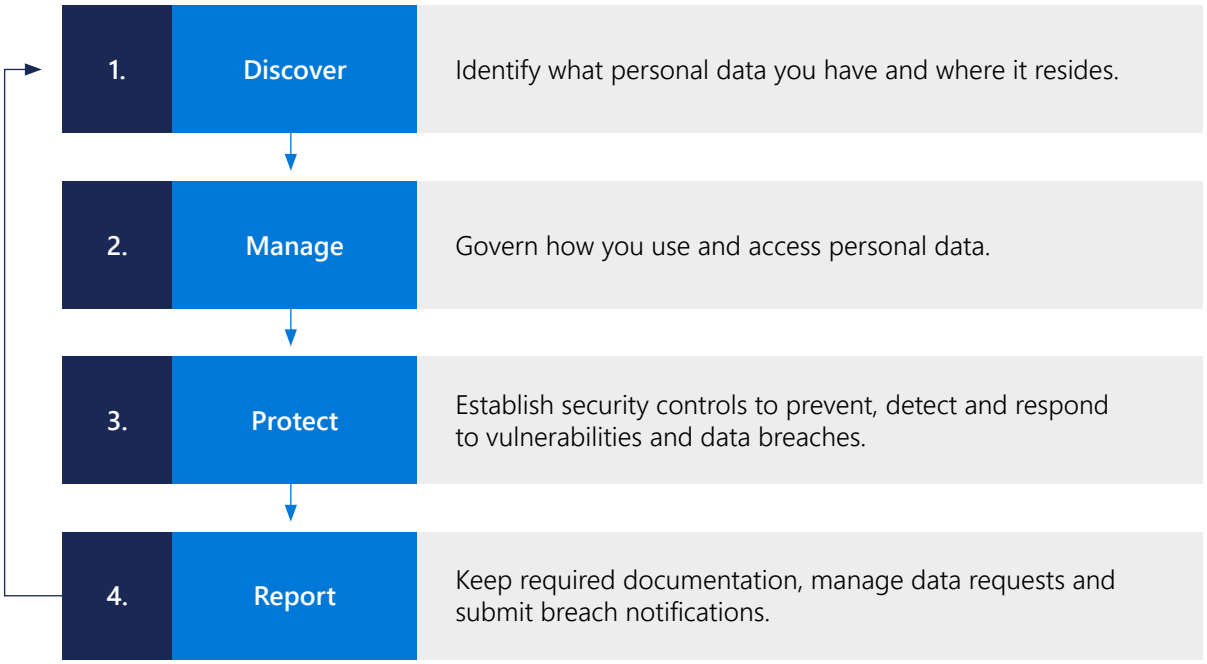
The applicability of the GDPR – case studies

Will the GDPR apply to ...

A New Zealand retailer that operates a branch in Copenhagen and collects the information of Danish customers, but then processes the orders in New Zealand?	Yes. The GDPR will apply to all organisations that are located in the EU and dealing with customers located in the EU, even if the data processing occurs outside the EU.
A large Australian company that recruits engineers through European recruitment pages but locates the workers in Australia or outside Europe?	Yes. The company's recruitment pages could be viewed as specifically monitoring or offering goods or services to EU individuals, particularly if the company uses persistent cookies to monitor visits to its recruitment pages. The GDPR will apply to organisations that are not located in the EU, but which monitor, or offer goods or services to, EU Data Subjects. Given that the collection and processing of the data will occur before the individuals leave the EU, the company's activities will be within the scope of the GDPR.
An Australian company that does not have a physical branch in Europe but operates a localised website (e.g., using an '.fr' domain, in the French language, and offering goods that can be purchased in euros)?	Yes. By customising its website to appeal to and facilitate ease of access within France, the Australian company is intentionally seeking French customers to purchase its products. The GDPR will apply to organisations that are not located in the EU, but which monitor, or offer goods or services to, EU Data Subjects.
A New Zealand service provider that operates solely in New Zealand but holds accounts for some individuals who moved and now live in Europe?	Yes, as the service provider now processes the account holder information while the individual is located in the EU or monitors that individual's behaviour while they are in the EU (regardless of whether the service provider originally intended to do so when the individual first became a customer).

Next steps

To confirm that you are complying with your privacy obligations, including any obligations under the GDPR, we recommend the following steps to progress your journey.



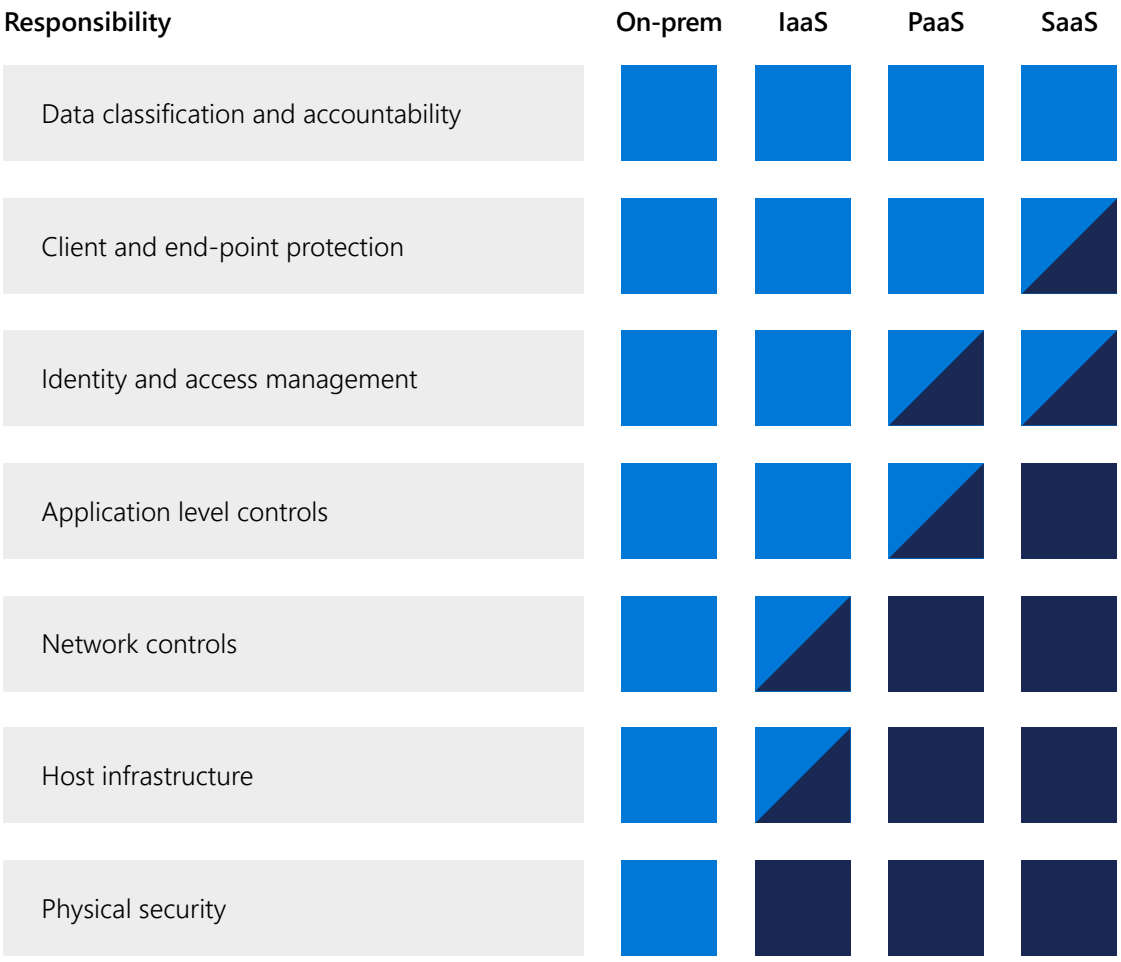
How Microsoft can help

We believe the GDPR is an important step forward for clarifying and enabling individual privacy rights. As your trusted partner for GDPR compliance, we want to help you focus on your core business while efficiently preparing for the GDPR.

Microsoft has extensive expertise in protecting data, championing privacy and complying with complex regulations. We are committed to GDPR compliance across our cloud services and we provide GDPR-related assurances in our contractual commitments.

Learn more about how our products help you comply with the GDPR and let us help you get started by visiting www.microsoft.com/GDPR. Here you will find resources such as webinars, videos, white papers and FAQs about the GDPR.

We have the tools to help, so reach out to your Microsoft account team as you begin your journey to GDPR compliance.




Microsoft