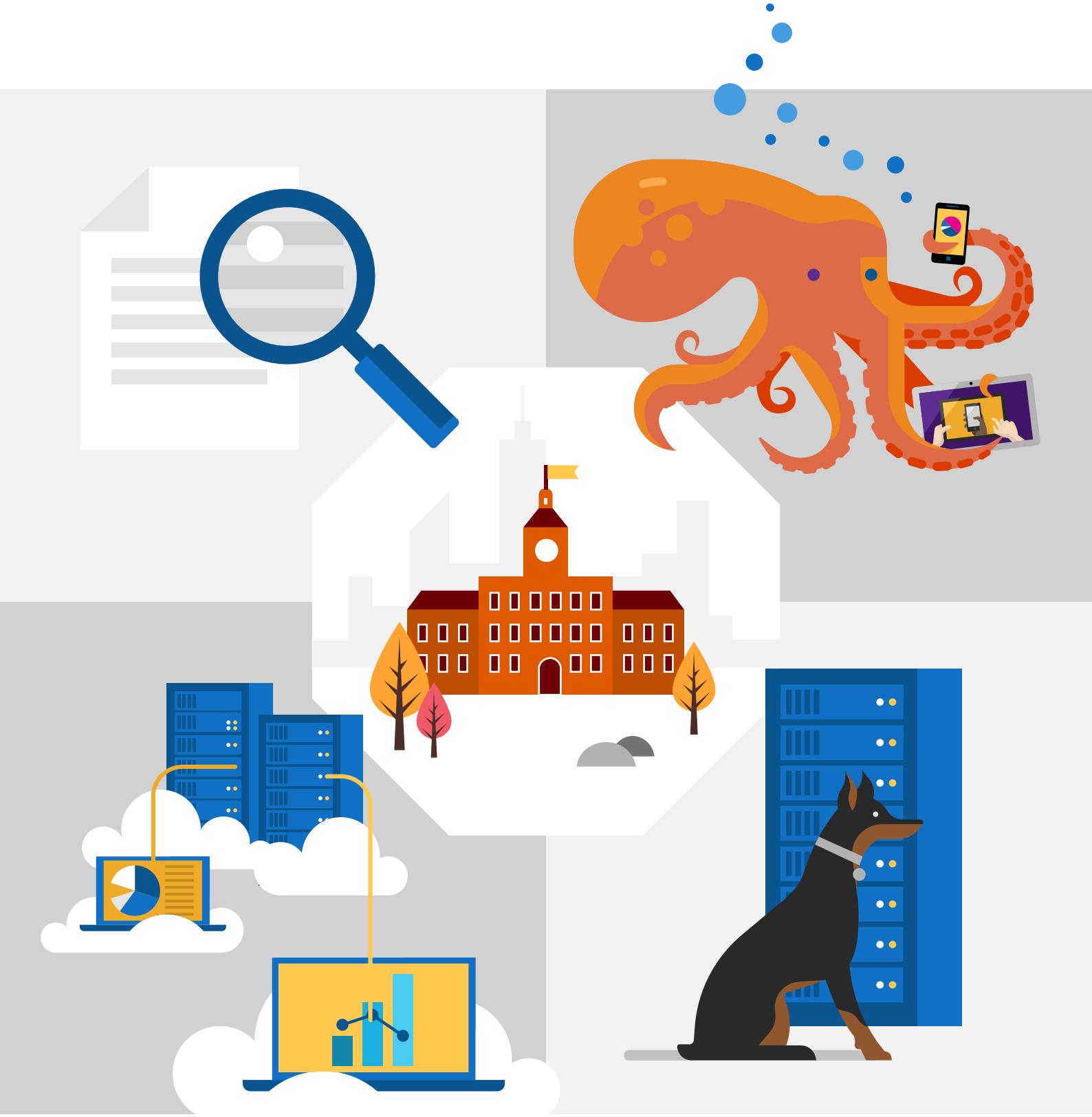


GDPR for education

A kick-start guide for educational institutions

Microsoft

About this guide

This guide is designed to help your journey to General Data Protection Regulation (GDPR) compliance, with concrete examples and to-do lists. It is not exhaustive, but it will give you a good idea of the processes and factors to consider from 25th May 2018, when GDPR comes into force.

The GDPR applies to institutions that have a physical presence in the European Union (EU) and to organisations who provide goods and services to EU citizens or that collect and analyse data tied to EU residents. If your institution resides outside the EU, consider this guide for compliance with GDPR as a best practice approach.

Education is a story of data

At the start of every academic year, new students generate vast amounts of data at schools and universities. This adds to the mountains of data these organisations already deal with as data owners.

But this data is vital for schools and universities to operate. Therefore, clear and well-documented processes need to be in place for every single record processed.

Moreover, these processes need to extend beyond a student's time at your institution. When they leave, databases, files, and even email streams will require documented policies for protection, retention and processing.

Defining the data journey

The information created and processed at academic institutions serves multiple purposes. First, there's the curriculum, the knowledge educators share with students, enhanced by the ideas that students generate as they progress throughout their learning journey.

There's also a second body of data: the information that organisations collect about teachers and students, as well as the school's performance. Add to this the information gathered from administrative processes—from parents, school nurses, governors, councillors, and external agencies—and you have a seemingly endless supply of data flowing through the organisation, a large portion of which is personal data.

As any administrator knows, this second set of data is just as vital to an academic institution as its core educational mission. It becomes part of the GDPR journey that students, teachers, and parents experience as they access and share information through the learning tools and communications services schools and universities provide.

What do you do with all that data?

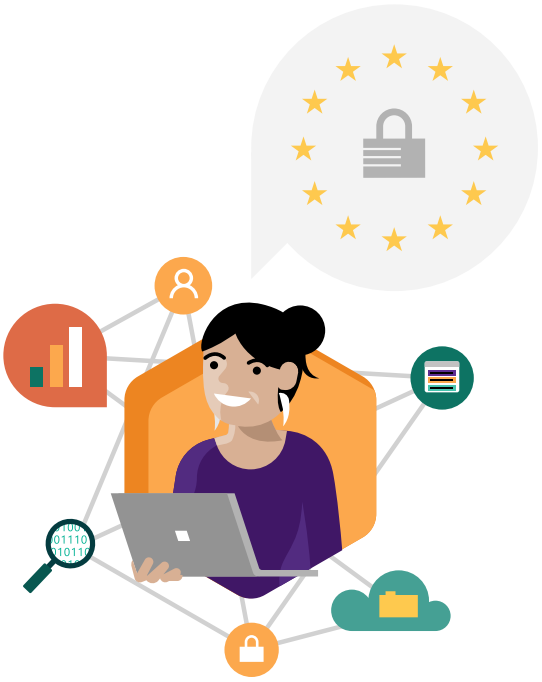
As the data owner, you are already subject to existing legislation that enforces careful handling and processing of the data you own and manage. Although there are additional considerations under GDPR on how, why and with whom you need to share parts of it with organisations — like regulatory and state bodies in addition to 3rd parties, i.e. insurance providers — process it, and analyse it, the chances are you already have multiple data protection and privacy policies in place.

But are they enough to protect the personal and sensitive information you handle?

Introducing GDPR

As of 25th May 2018, many organisations, even those outside the European Union (EU), will be accountable for all their data under a new EU regulation, the General Data Protection Regulation (GDPR).

The regulation is designed to protect all EU citizens' data privacy and to harmonise all data privacy laws across Europe. GDPR will affect what data you have, how you use it, where it is stored, and how long it can be stored for.



Why is GDPR important?

An educational institution's journey can mirror a student's learning journey, marked by milestones that are recorded and evaluated at every stage. Sometimes the data generated will stay the same for years, while at other times it will change rapidly as students and staff move through the institution.

GDPR creates a uniform European legal framework, giving subjects who reside in Europe rights over this data.

The key changes affecting education include:

Personal privacy

Individuals have the right to:

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

Controls and notifications

You will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Document how you process personal data
- Keep records detailing data processing and consent*

Transparent policies

You will be expected to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies
- Outline how customers can exercise their rights under GDPR

IT and training

Educational institutions will need to:

- Train privacy personnel and employees—for example, school administrators or IT staff
- Audit and update data policies relating to students, staff, and contractors
- Employ a Data Protection Officer (if required)
- Create and manage compliant vendor contracts, including all vendors and supply teachers

***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 EU Member states may individually set the age of consent anywhere between 13 and 16 years old.**

How does GDPR affect you?

How do you align these new rules with the fact that multiple people in an institution need access to data every day?

GDPR provides the regulation to manage and protect this data while creating consistent policies and practices. It's up to you to build a GDPR framework that works for your institution.

Enhanced personal privacy rights

GDPR strengthens data protection for individuals, including students, within the EU by ensuring they have the right to:

- Access data and correct inaccuracies
- Erase data
- Object to processing of their information
- Move their data

Increased duty for documenting processes and protecting data

Educational institutions that process personal data will need to show clear evidence of compliance.

Mandatory data breach reporting

Educational institutions are required to report data breaches within 72 hours.

Significant penalties for non-compliance

Educational institutions risk potential fines if they fail to respond. To be compliant, it is important to consider several measures to protect personal data and to be cautious when handling it.

How to get started? A compliance map for GDPR

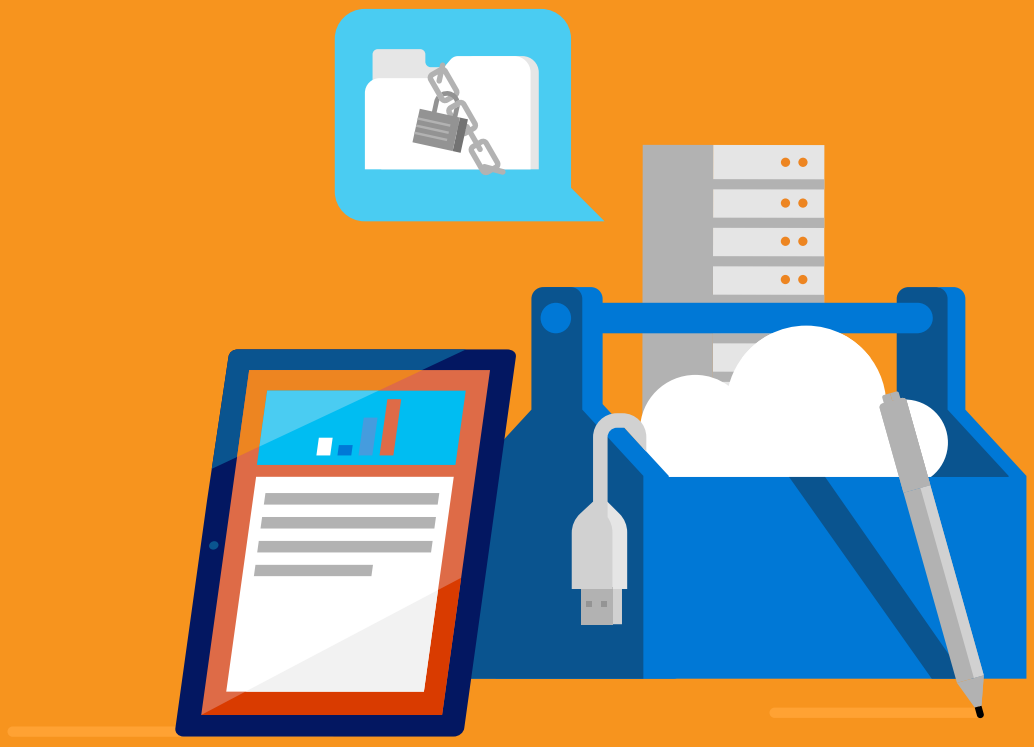
GDPR will have a significant impact on your institution. It requires you to update personal privacy policies, implement or strengthen data protection controls and breach notification procedures, deploy highly transparent policies, and further invest in IT and training.

With the **most comprehensive set of compliance offerings** of any cloud service provider, the Microsoft Cloud can ease your journey towards GDPR compliance. You'll find that the Microsoft Cloud gives you the most resources to meet your GDPR requirements.

We have developed a process for GDPR implementation, focusing on four key steps:

- **Discover**. Identify what personal data you have and where it resides
- **Manage**. Govern how personal data is used and accessed
- **Protect**. Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches
- **Report**. Keep required documentation, and manage data requests and breach notifications

Microsoft tools and resources can help you at each stage as you put GDPR compliance into place.



Discover

Manage

Report

Protect

Discover

Identify what personal data you have and where it resides.

Discover what you have

Personal data is often stored in multiple locations, including in emails, documents, databases, removable media, metadata, log files, and backups.

The first job is to identify where personal data is collected and stored.

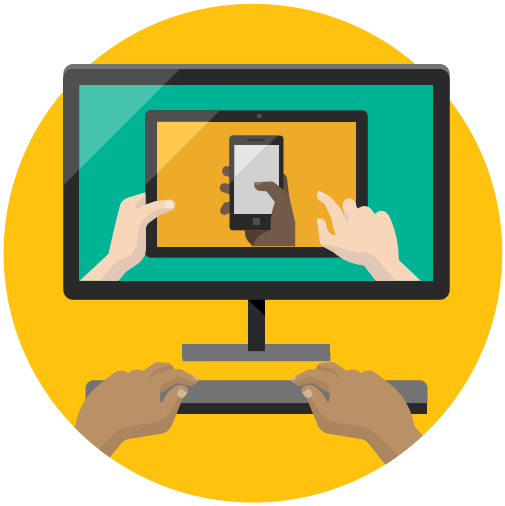
Existing data

Challenge

In addition to storing and securing existing data in a GDPR-compliant way, you should also document how you process personal data e.g. 1. consent, 2. contract, 3. legal, 4. health, 5. common, 6. legitimate cause.

To dos

- Identify what existing personal data is collected and stored.
- Discover locations where that data is stored. Be sure to include cloud vendors and third-party hosts, such as websites and shared service centres. Don't forget analogue data, such as files stored in filing cabinets.
- Organise and label existing data based on sensitivity, use, ownership, administrators, and users.
- Document GDPR grounds for processing.
- Check consent process and renew if applicable.



Existing devices and locations

Challenge

Personal data is often stored and accessed on a wide range of devices. These devices can include servers, desktops, laptops, tablets, smartphones, home computers, and managed and non-managed cloud environments. Personal and mobile devices pose a special challenge to the discovery of data.

To dos

- Take an inventory of and list all the devices that could be carrying personal data.
- Audit personal and mobile devices that do not belong to your institution.

GDPRs requirements

GDPR requires that organisations identify existing data and where it is held.

Once you create an inventory of all data, including locations, devices, and users, systems can be set up to collect new data as it comes in.

Existing users

Challenge

GDPR imposes strict rules on who can process what pieces of personal data and how and when they can do it. Before sharing personal data, you will need to ensure that those who have access to it are entitled to see it, both inside and outside the school.

To dos

- Identify and list all users, including students, staff and all contractors who may access data.

Existing subcontractors

Challenge

Personal data should be shared with or accessed by only people who are authorised. This applies to parties both inside and outside the organisation. Think about all the contractors—including catering services, cleaning services, and external assistants—that work with your institution.

It is your responsibility to make sure the people authorised to access the data—called the processors under GDPR—are compliant with the legislation. This means they will store personal data in a secure way, use it only for the purpose you requested, and delete it when it is no longer needed.

To dos

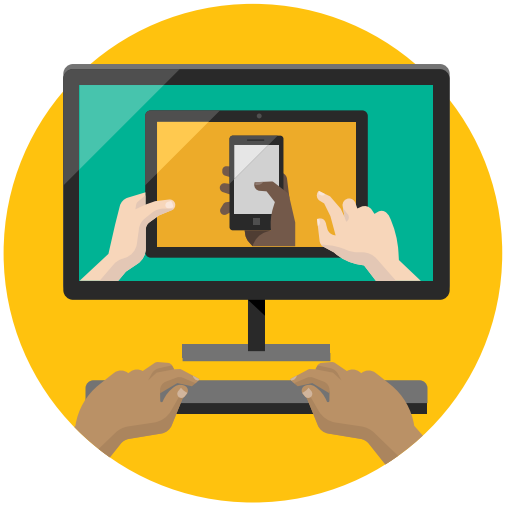
- Identify and list all subcontractors in the user directory.
- Check for GDPR compliance.
- Sign a GDPR compliance contract.
- Check to see if data can be centrally accessed while still onsite.

Manage

Govern how personal data is used and accessed.

Manage personal data

The first step in managing personal data is to define why you need to collect it in the first place. Ask yourself how it helps the delivery of education. Consider how it should be gathered, where it will be stored, what entities will support that process, who should access it, and how you will enable changes and deletions.



Managing new data

Challenge

GDPR allows for use of the data needed to fulfil your mission. If your mission is clearly defined your need to process the personal data it relates to will increase.

When students register, you will want to be transparent in what personal data you collect. Specifically, you need to know why you need this data, how long you're keeping it for, where you're storing it, and how you and others will be accessing it. Where applicable, consent for processing needs to be requested, obtained, and stored as proof. Students under the age of consent will require parental consent. When you hire staff, you will need to provide clear information about how personal data is processed.

To dos

- Clearly define your mission.
- List your data subjects.
- Establish what personal data is required.
- Automate data collection and be accountable.
- Clarify GDPR clauses to contracts with your HR partner and check consent and renew processes, if relevant.

Managing devices

Challenge

In an educational setting, devices are varied and spread across a vast range of users. You see teachers' home computers, students' smartphones and tablets, classroom computers, personal devices, private apps, non-monitored cloud apps and locations, subcontractor devices, USB keys and paper files stored in cabinets.

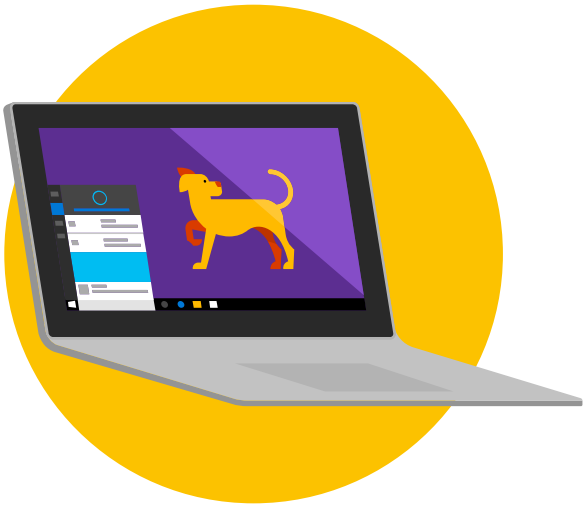
To meet the strict GDPR rules on securing personal data, you will need to manage devices—as well as education staff, students, and contractors—in a consistent way.

To dos

- Develop policies on the use of devices.
- Educate staff and students and make them aware of GDPR.
- Audit and log events.

GDPRs requirements

GDPR governs how personal data is used and accessed.



Managing users

Challenge

While the discovery process gives insights into your user database, the manage process helps you organise users into intelligent lists, allowing you to set permissions, secure sign-in policies, and track access.

When users leave your institution, their access to all school resources needs to end rapidly to avoid potential leaks.

To dos

- Organise users into security groups.
- Define permissions and policies.
- Roll out policies.
- Educate students, staff and contractors on correct use of data.

Managing your website

Challenge

Online activities are a vital part of promotion to attract staff and students. It is your duty to assure security on the online platforms you use.

To dos

- Audit the data your website collects automatically.
- List first- and third-party cookies.
- Check online forms for end-to-end security.
- Check consent processes for GDPR compliance.
- Create a privacy declaration documenting:
  - What information is being collected
  - Who is collecting it
  - How it is being collected
  - Why is it being collected
  - How it will be used
  - Who it will be shared with
  - What the effect will be on the individuals concerned
  - If the intended use is likely to cause individuals to object or complain

Protect

Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.

Protect users, data and devices

Security is one of the key attention points in our computerised world.

GDPR requirements include physical protection, network security, storage security, computer security, identity management, access control, encryption, and risk mitigation. Look at the way you monitor systems, identify breaches, calculate the impact of any breaches, and respond and recover from them.

Data

Challenge

GDPR is not a destination: it is an ongoing journey. It requires you to be accountable at all times, respond quickly when necessary, and protect personal data as it makes its way through your institution.

To dos

- Encrypt data and mail.
- Protect data on devices (MAM).
- Store securely.
- Add rights to individual files and mails.
- Monitor intrusions, infections, theft, and abnormal behaviour.

Devices, locations and apps

Challenge

Devices and apps touch nearly every aspect of your data. They can be part of your local area network (LAN), mobile devices, devices in other locations such as at home or on campus, and devices and apps in the cloud. Each device and app requires specific attention.

To dos

- Protect the LAN with antivirus, firewall, and physical protection.
- Encrypt devices, disks, and USB keys.
- Educate students and staff on best practice for home computers.

GDPRs requirements

GDPR sets the guidelines to establish security controls to prevent, detect and respond to vulnerabilities and data breaches.

Users

Challenge

Once users have been defined and organised into security groups with defined permissions and policies, you can add additional protective measures—access control and identity management—to achieve GDPR compliance.

To dos

- Review password policies and sign-in options.
- Educate and create awareness.

Testing

Challenge

Once you've put the technical and organisational measures in place to protect personal data, you'll need to regularly test, assess, and evaluate their effectiveness to ensure they're adequate and appropriate.

To dos

- Facilitate regular testing.
- Evaluate effectiveness of security measures.

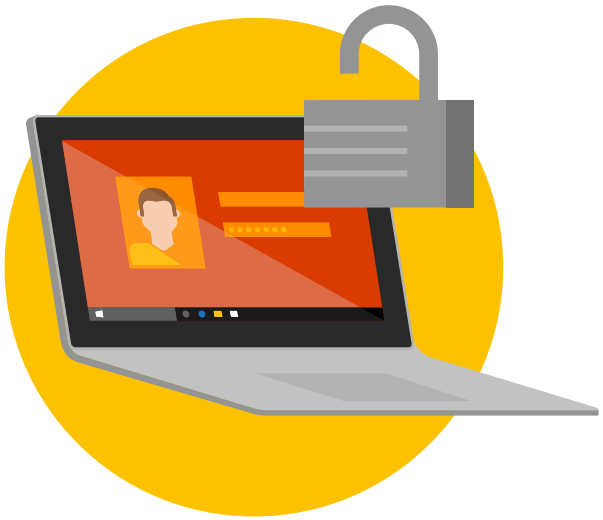
Report

Execute on data requests, report data breaches, and keep required documentation.

Reporting on audits and data breaches

A key principle of GDPR is to be accountable. You will need to create clear audit trails on processing, classifications, and third parties with access to personal data, including organisational and technical security measures, and data retention times. You may need to conduct Data Protection Impact Assessments (DPIAs).

A DPIA requires organisations to identify and analyse the impact of a proposed processing activity on the protection of personal data.



Audit trails

Challenge

GDPR requires you to be responsible for the safeguarding and appropriate processing of personal data. Your records should contain the nature of every request that a data subject makes—for example, to view or rectify personal data—and the resolution that followed.

To dos

- Retain records of data subjects' requests to demonstrate compliance with GDPR requirements.
- Track and record when personal data flows into and out of the EU.
- Track and record data sent to third-party service providers, such as IT contractors or educational services.
- Maintain audit trails to show GDPR compliance.
- Track and record flows of personal data to third-party service providers.
- Facilitate DPIAs.

Data breaches

Challenge

Organisations will need to notify the applicable authorities within 72 hours of identification of a breach.

To dos

- Activate logs and reports.
- Respond within the required timeframe.
- Keep a separate log of changes to personal data in case of disaster and backup restore.

GDPRs requirements

Organisations will need to notify the applicable authorities within 72 hours of identification of a breach.

Conclusion

Trust is central to Microsoft's mission to empower every person and organisation on the planet to achieve more. Nowhere is this more important than in the institutions that prepare the next generation of students to find and fulfil their purpose in society.

Microsoft is committed its principles of cloud trust – across **security, privacy, transparency** and **compliance**. As the GDPR enforcement begins on 25th May 2018, Microsoft's broad portfolio of cloud services address the rigorous security and privacy demands of our education customers and ensure we meet your obligations as a data processor.

Microsoft's cloud productivity offering Office 365 A1 is free for education customers. It provides essential GDPR compliance and information protection tools, enabling eDiscovery, rights management, data loss prevention, encryption, advanced email archiving, and legal hold capabilities. Customers requiring enhanced risk analysis, threat mitigation, data encryption, and control can consider **Office 365 A3 or A5** paid plans to support their specific GDPR requirements.

Customers seeking solutions that manage data archiving, governance, and discovery for their broader IT estate can leverage **Microsoft 365 Education**. This provide a simple and safe experience to manage users, data, and devices from a single dashboard that protects identity, apps, data, and devices with intelligent security enhanced by machine learning.

Get started today by using the GDPR **Assessment tool** to review your overall level of readiness. And if you are already a Microsoft Cloud customer, use **Compliance Manager** to get a holistic view of your data protection and compliance posture for Office 365, Dynamics 365, and Azure.

Tools and related links

We have compiled the following list of tools to help you on your GDPR journey.

Discover

- **Office 365 Advanced eDiscovery** or **Content Search** will support you in searching for existing information.
- **Office 365 data labelling** allows classifying data across your organisation for governance.
- **SharePoint Lists** are a flexible tool to help you organise and label data.
- **User Account Management in Office 365** supports you in organising users.
- **Microsoft Intune for Education** supports you in listing and managing a variety of devices.
- **System Center** is an ideal solution to list and manage servers with various OSs and cloud-hosted solutions.
- **Azure Search** will support you in adding advanced search functionality in your current environment.
- **Azure Data Catalog** registers, discovers, understands, and consumes data sources.
- **Cloud Discovery** analyses your traffic logs against Cloud App Security's cloud app catalogue of over 15,000 cloud apps that are ranked and scored based on more than 60 risk factors, to provide you with ongoing visibility into cloud use, shadow IT, and the risk shadow IT poses into your organisation.
- **Advanced Data Governance (ADG)** helps you automatically identify, classify, and manage personal data and sensitive data, as well as apply retention and deletion policies.

Manage

- **Use Security Groups** in Office 365 to set a single set of permissions across Office 365 apps.
- **Outlook smart attachments** prevent information from leaving the institution.
- Use **Office 365 mail tips** to avoid common mistakes.
- **Office 365 Data Loss Prevention** prevents information from leaving the premises.
- Creating automated **Flows** between applications will optimise and secure data flows.
- **Intune for Education** helps you manage policies, apps, and settings for your classroom devices
- **Azure AD** (Azure Active Directory) is the Microsoft cloud-based directory and identity management service.
- Use **PowerApps** to create mobile apps in no time to feed databases directly.
- Apply **labels** to personal data and manage **data governance** in Office 365.
- **Azure Information Protection:** Control and help secure email, documents, and sensitive data that you share outside your company.
- Embedding **Microsoft Forms** (Office 365) can secure data entry via online forms and allow GDPR-compliant requests for consent.
- **Office 365 Teams** enables institutions to centralise and coordinate all communication required for GDPR policies.

Report

- The **Microsoft Trust Center** is the ideal source to check for information on GDPR and compliance.
- Microsoft **Compliance Manager** helps you perform risk assessments and simplifies your compliance process by providing recommended actions, evidence gathering, and audit preparedness.
- **Azure auditing and logging** provides you with an electronic record of suspicious activities and helps you detect patterns that may indicate attempted or successful external penetration of the network, as well as internal attacks.
- **Securescore.office.com** is a security analytics tool that will help you understand what you have done to reduce the risk to your data in Office 365 and show you what you can do to further reduce that risk. It is the ideal source of knowledge on auditing, logging, and many other security features of Office 365.
- **Unified audit log** provides insight into data that has been transferred to third parties.

Protect

- **Office 365 (A3) Data Loss Prevention** allows the creation of rules preventing the desired types of information from leaving the premises.
- **Azure Information Protection:** Control and help secure email, documents, and sensitive data that you share outside your company. From easy classification to embedded labels and permissions, enhance data protection always with Azure Information Protection—no matter where it's stored or who it's shared with.
- **Customer Lockbox** can enable controllers to demonstrate that there are explicit procedures in place for access to customer content during service operations.
- **AppLocker** helps administrators create and deploy application control policies, restricting access by unauthorised users to applications that could put personal data at risk.
- **Microsoft Advanced Threat Analytics** (ATA) is an on-premises platform that helps protect your school from multiple types of advanced targeted cyber-attacks and insider threats.
- **Office 365 Threat Intelligence.**
- **Intune for Education** is a simple but powerful solution for rolling out security policies, apps, and settings for your classroom devices.
- **Windows Defender Advanced Threat Protection** available in Windows 10 Education, is a security service that enables enterprise customers to detect, investigate, and respond to advanced threats on their networks.
- **Azure Backup** and **Azure Disaster Recovery** increase availability.
- **BitLocker Drive Encryption** is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.
- Use **Multi Factor Authentication** in Office 365 and Windows 10 with Windows Hello.

Note: This is not a complete list of Microsoft tools and services available to support the four key steps. For a comprehensive overview of how all Microsoft Cloud Service and Products can help customers meet their GDPR obligations please download the **Accelerate your GDPR compliance with the Microsoft Cloud** e-Book

Published March 2018 Version 1.0