SMS - GUI003

GDPR Information

Release Certificate	
Status of this Document:	**Approved**
Document Version:	**1.0**
Release Date:	**27/03/2018**

Document Control

Title:	SMS - GUI003 - GDPR Information
Client:	Internal
Version:	1.0
Release Date:	27/03/2018
Author:	Sebastien Masterton-Smith
Total Pages:	Including Preliminaries & Appendices
Disclaimer:	This document is uncontrolled when printed.

Document Approval

Approved By:	Ben Hobbs	Approved by e-mail

1 TABLE OF CONTENTS

2 INTRODUCTION

This document provides information about the European General Data Protection Regulations (GDPR), how it impacts businesses of various size, and how Office 365 or Microsoft 365 can mitigate some of the risks and issues that the regulations pose.

This document applies to anyone that does business for or with businesses or individuals in the European Union (EU) and interacts with any residing member of the EU.

The information contained within this document is not exhaustive, it should not be taken as a full and comprehensive document on how to completely secure a business. Therefore, care should be taken to review the full GDPR documentation available via the link below and create appropriate policies in accordance. This document is intended as a guide to how Office 365 and cloud technologies can help with these policies.

https://www.eugdpr.org/

3 GDPR SUMMARY

3.1 Overview

The GDPR applies in the UK from 25th May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

It is a new legal framework which has some similarities to the UK Data Protection Act 1998 (DPA), with some key differences. It is for those that have day-to-day responsibility for data protection.

Having clear laws with safeguards in place is more important than ever given the growing digital economy.

3.2 Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors'. The definitions are broadly the same as under the DPA – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

  If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

  However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

3.3 What Information does the GDPR apply to?

Personal data

Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). These categories are broadly the same as those in the DPA, but there are some minor changes.

For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

3.4 Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

The principles are similar to those in the DPA, with added detail at certain points and a new **accountability** requirement. The GDPR does not have principles relating to individuals' rights or overseas transfers of personal data - these are specifically addressed in separate articles (see GDPR Chapter III and Chapter V respectively).

The most significant addition is the accountability principle. The GDPR requires you to show how you comply with the principles – for example by documenting the decisions you take about a processing activity.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

3.5 Key areas to consider

3.5.1 Lawful processing

For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing" under the DPA.

It is important that you determine your lawful basis for processing personal data and document this.

This becomes more of an issue under the GDPR because your lawful basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, for example to have their data deleted.

3.5.2 Consent

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent. Public authorities and employers will need to take particular care to ensure that consent is freely given.

Consent must be verifiable, and individuals generally have more rights where you rely on consent to process their data.

Remember that you can rely on other lawful bases apart from consent – for example, where processing is necessary for the purposes of your organisation's or a third party's legitimate interests.

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

3.5.3 Children's personal data

The GDPR contains new provisions intended to enhance the protection of children's personal data.

Privacy notices for children

Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.

Online services offered to children

If you offer an 'information society service' (i.e. online service) to children, you may need to obtain consent from a parent or guardian to process the child's data.

The GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 can't give that consent themselves and instead consent is required from a person holding 'parental responsibility' – but note that it does permit member states to provide for a lower age in law, as long as it is not below 13.

'Information society services' includes most internet services provided at the user's request, normally for remuneration. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

3.6 Individuals' rights

3.6.1 The right to be informed

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

3.6.2 The right of access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

These are similar to existing subject access rights under the DPA.

3.6.3 The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

3.6.4 The right to erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

3.6.5 The right to restrict processing

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

3.6.6 The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.

3.6.7 The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise
- of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

4 OFFICE 365

Microsoft designed Office and Office 365 with industry-leading security measures and privacy policies to safeguard your data in the cloud, including the categories of personal data identified by the GDPR. Office and Office 365 can help you on your journey to reducing risks and achieving compliance with the GDPR.

One essential step to meeting the GDPR obligations is discovering and controlling what personal data you hold and where it resides. There are many Office 365 solutions that can help you identify or manage access to personal data.

4.1 Data Loss Prevention (DLP)

Office and Office 365 can identify over 80 common sensitive data types including financial, medical, and personally identifiable information. In addition, DLP allows organizations to configure actions to be taken upon identification to protect sensitive information and prevent its accidental disclosure.

4.2 Advanced Data Governance

Advanced Data Governance uses intelligence and machine-assisted insights to help you find, classify, set policies on, and take action to manage the lifecycle of the data that is most important to your organization.

4.3 Office 365 eDiscovery

eDiscovery search can be used to find text and metadata in content across your Office 365 assets—SharePoint Online, OneDrive for Business, Skype for Business Online, and Exchange Online. In addition, powered by machine learning technologies, Office 365 Advanced eDiscovery can help you identify documents that are relevant to a particular subject (for example, a compliance investigation) quickly and with better precision than traditional keyword searches or manual reviews of vast quantities of documents.

4.4 Customer Lockbox

Customer Lockbox for Office 365 can help you meet compliance obligations for explicit data access authorization during service operations. When a Microsoft service engineer needs access to your data, access control is extended to you so that you can grant final approval for access. Actions taken are logged and accessible to you so that they can be audited.

Another core requirement of the GDPR is protecting personal data against security threats. Current Office 365 features that safeguard data and identify when a data breach occurs include:

4.5 Advanced Threat Protection

Exchange Online Protection helps protect your email against new, sophisticated malware attacks in real time. It also allows you to create policies that help prevent your users from accessing malicious attachments or malicious websites linked through email.

4.6 Threat Intelligence

Threat Intelligence helps you proactively uncover and protect against advanced threats in Office 365. Deep insights into threats—provided by Microsoft's global presence, the Intelligent Security Graph, and

input from cyber threat hunters—help you quickly and effectively enable alerts, dynamic policies, and security solutions.

4.7 Advanced Security Management

Advanced Security Management enables you to identify high-risk and abnormal usage, alerting you to potential breaches. In addition, it allows you to set up activity policies to track and respond to high risk actions.

4.8 Office 365 audit logs

Office 365 audit logs allow you to monitor and track user and administrator activities across workloads in Office 365, which help with early detection and investigation of security and compliance issues.

5 ENTERPRISE MOBILITY + SECURITY

Securing and managing personal data is critical to you, your customers, and to complying with the coming requirements of the GDPR. Microsoft designed Enterprise Mobility + Security to safeguard customer data both in the cloud, and on-premises, with industry-leading security capabilities. This includes personal data no matter where it might travel across your users, devices, and apps. Enterprise Mobility + Security offers innovative technology and solutions today that can help you on your journey to reducing risks and achieving compliance with the GDPR. Microsoft designed Enterprise Mobility + Security with industry-leading security capabilities to safeguard your data in the cloud, including the categories of personal data identified by the GDPR. Enterprise Mobility + Security can help you on your journey to reducing risks and achieving compliance with the GDPR. The GDPR obligations include discovering what personal data you hold and where it resides, controlling how your users access and use personal data, and establishing security controls to prevent, detect, and respond to vulnerabilities and data breaches.

Enterprise Mobility + Security features identity-driven security technologies that help you discover, control, and safeguard personal data held by your organization, reveal potential blind spots, and detect when data breaches occur.

5.1 Azure Active Directory (Azure AD)

Azure AD helps you ensure that only authorized users can access your computing environments, data, and applications. It features tools such as Multi-Factor Authentication for highly secure sign-in. Additionally, Azure AD Privileged Identity Management helps you reduce risks associated with administrative access privileges through control, management and reporting of these critical administrative roles.

5.2 Microsoft Cloud App Security

Microsoft Cloud App Security helps you discover all the cloud apps in your environment, identify users and usage, and get a risk score for each app. You can then decide if you'd like your users to access these apps. Cloud App Security then provides visibility, control, and threat protection for the data stored in those cloud apps. You can shape your cloud security posture by setting policies and enforcing them on Microsoft and third-party cloud applications. Finally, whenever Cloud App Security discovers an anomaly, it sends you an alert. Microsoft Intune helps you protect data that may be stored on personal computers and mobile devices. You can control access, encrypt devices, selectively wipe data, and control which applications store and share personal data. Intune can help you inform users about your management choices by posting a custom privacy statement and terms of use. It also gives you the ability to rename or remove devices.

5.3 Microsoft Azure Information Protection

Azure Information Protection helps ensure that your data is identifiable and secure, a key requirement of the GDPR—regardless of where it's stored or how it's shared. You can classify, label, and protect new or existing data, share it securely with people within or outside of your organization, track usage, and even revoke access remotely. Azure Information Protection also includes rich logging and reporting to monitor the distribution of data, and options to manage and control your encryption keys.

5.4 Microsoft Advanced Threat Analytics

Advanced Threat Analytics helps pinpoint breaches and identifies attackers using innovative behavioural analytics and anomaly detection technologies. Advanced Threat Analytics is deployed on-premises and works with your existing Active Directory deployment. It employs machine learning and the latest user and entity behavioural analytics to help find advanced persistent threats and detect

suspicious activities and malicious attacks used by cybercriminals, to help identify breaches before they cause damage to your business.

6 WINDOWS 10 AND SERVER 2016

Microsoft designed Windows 10 and Windows Server 2016 with industry-leading security measures and privacy policies to help safeguard your data in the cloud, including the categories of personal data identified by the GDPR.

The security capabilities available today in Windows 10 and Windows Server 2016 can help you on your journey to reducing risks and achieving compliance with the GDPR. A key requirement of the GDPR is protecting personal data. Microsoft believes effective security needs to be end-to-end, from the desktop to the servers where the data resides. Windows 10 and Windows Server 2016 include industry-leading encryption, anti-malware technologies, and identity and access solutions that enable you to move from passwords to more secure forms of authentication.

6.1 Windows Hello

Windows Hello is a convenient, enterprise-grade alternative to passwords that uses a natural (biometrics) or familiar (PIN) method to validate your identity, providing the security benefits of smartcards without the need for additional peripherals.

6.2 Windows Defender

Windows Defender is a robust anti-malware solution that works right out of the box to help you stay protected. Windows Defender is quick to detect and protect you against emerging malware, and it can immediately help protect your devices when a threat is first observed in any part of your environment.

6.3 Windows Defender Advanced Threat Protection

Windows Defender ATP provides security operations teams with advanced breach detection, investigation, and response capabilities across all your endpoints, with up to six months of historical data. Windows Defender ATP helps address a key requirement of the GDPR that companies have clear procedures for detecting, investigating, and reporting data breaches.

6.4 Device Guard

Device Guard allows you to lock down your devices and servers to protect against new and unknown malware variants and advanced persistent threats. Unlike detection-based solutions such as antivirus programs that need constant updating to detect the latest threats, Device Guard locks down devices so they can only run the authorized applications you choose, which is an effective way to combat malware.

6.5 Credential Guard

Credential Guard is a feature that isolates your secrets on a device, like your single sign-on tokens, from access even in the event of a full Windows operating system compromise. This solution fundamentally prevents the use of hard to defend attacks such as “pass the hash.”

6.6 BitLocker Drive Encryption

BitLocker in Windows 10 and Windows Server 2016 provides enterprise-grade encryption to help protect your data when a device is lost or stolen. BitLocker fully encrypts your computer’s disk and flash drives to prevent unauthorized users from accessing your data.

6.7 Windows Information Protection

Windows Information Protection picks up where BitLocker leaves off. While BitLocker protects the entire disk of a device, Windows Information Protection protects your data from unauthorized users and applications running on a machine. It also helps you prevent data from leaking from business to non-business documents or to locations on the web.

6.8 Shielded Virtual Machines

Shielded Virtual Machines allow you to use BitLocker to encrypt disks and virtual machines (VMs) running on Hyper-V to prevent compromised or malicious administrators from attacking the contents of protected VMs.

6.9 Just Enough Administration and Just in Time Administration

JEA and JITA allows administrators to perform their regular jobs and actions, while enabling you to limit the scope of capabilities and time that administrators can run. If a privileged credential is compromised, the scope of damage is severely limited. This technique provides administrators with only the level of access they require during the time they are working on the project.

7 SKYKICK DATA PROTECTION

Part of the GDPR is to ensure that data is protected. With SkyKick Cloud Backup data is protected indefinitely from Exchange, SharePoint and OneDrive.

People delete data. Mostly accidentally, sometimes intentionally. 75% of data loss is due to people deleting content, and 32% of companies will experience a data loss event1. That means that even in the cloud, IT partners can spend a lot of time helping customers get back on track. Without a cloud backup solution for Office 365, you are missing the foundational piece of data protection to complement native Office 365 features.

SkyKick Cloud Backup for Office 365 is a cloud-to-cloud service that offers unlimited backup, lightning-fast search and one-click restore of your customer's Office 365 Exchange email, calendar, contacts, public folders, and more. Together with native Office 365 features, Cloud Backup delivers a complete cloud data protection and recovery solution.

7.1 Key features

No data caps

SkyKick Cloud Backup has no data caps or costly overage charges, unlike other solutions available. For one simple price, they offer unlimited data storage for the data giving peace of mind.

Unlimited retention

There is no catch! SkyKick Cloud Backup offers unlimited retention for all files and emails. Data is retained for any legal or compliance requirements and organizational knowledge is not lost even when an employee leaves the organization. This does not impact the right to be forgotten, data that has been backed up is not required to be deleted.

Reliable and secure

SkyKick Cloud Backup uses industry leading 256-bit encryption at rest and 128-bit in transit. Your data never leaves the Azure environment, which ensures all the inherent security and compliance capabilities that Azure offers.

6-backups a day

SkyKick Cloud Backup takes snapshots at regular intervals throughout the day. This ensures that your end customers can go about accessing Office 365 without any fear of disruption due to data loss.

8 MICROSOFT AND GDPR COMPLIANCE

The journey to General Data Protection Regulation (GDPR) compliance begins with a set of defined steps. The information here is designed to help both compliance professionals and IT implementers understand how Microsoft Office 365 and Windows 10 can assist you in discovering, managing, and protecting your data in the cloud, and compile the necessary reports and documentation to help meet GDPR requirements.

Microsoft Enterprise Mobility + Security provides the latest mobility and cloud innovations plus helps to protect your business from threats across your data, identities, devices, and apps. Enterprise Mobility + Security enables the types of business and technical controls that you need as you work toward meeting the requirements of the GDPR.

Sensitive personal data can be contained in email messages, documents, spreadsheets, notes, and local databases, and saved in individual cloud storage accounts. Restricting access to that data is an essential element in protecting the privacy of individuals. Office 365 incorporates privacy by design, and Microsoft has robust policies, controls, and systems built into Office 365 to help keep personal data private.

Compliance is an on-going process and a shared responsibility. Microsoft is investing in additional features and functionality to help organizations achieve their GDPR compliance goals. Whether you're a compliance officer, a decision-maker considering Office 365 as a business productivity solution, a current Office 365 administrator seeking help with a specific GDPR-compliant implementation, or an interested party looking for general information on how the GDPR relates to Office 365 and related products, the information here can provide a starting point for your journey.

Your path to GDPR compliance begins with focusing on four key steps, and Microsoft Office 365 products and services provide powerful tools and solutions for tackling each step. Learn more about how Microsoft products and services can help you on the road to GDPR compliance.

8.1 STEP 1 – Discover

The first step towards GDPR compliance is to assess whether the GDPR applies to your organization, and, if so, what data under your control is subject to the GDPR. This analysis includes understanding what data you have and where it resides. Adopting a classification scheme that applies throughout your organization helps you respond to data subject requests because it enables you to more readily identify and process personal data requests.

Microsoft Office 365 and related tools help you discover and classify personal data.

- Use **Content Search** to query for and identify personal data using relevant keywords, file properties, or built-in templates.
- Use **Advanced eDiscovery**, which is built on machine learning technologies, to perform more efficient searches.
- Use **Office 365 Advanced Data Governance (ADG)**, in conjunction with Content Search, to identify, classify, and manage personal data, and set and implement retention policies for personal data across Office 365 environments.
- Use **Office 365 Data Loss Prevention (DLP)** policies to identify personal data as it travels through Exchange Online, SharePoint Online, and OneDrive for Business. Use DLP policies to classify personal data in SharePoint Online, OneDrive for Business, Outlook, Outlook Web Access, and Office 365 Groups.
- Help identify, classify, and label personal data at the time of creation or modification with **Azure Information Protection**.
- Configure policies to trigger some actions based on sensitivity labels such as automatic encryption of data or adding of visual markings such as a headers, footers, or watermarks with **Azure Information Protection**.
- Identify the use of cloud apps, filter the data, and generate specific views to identify cloud applications that may contain personal data with the **Cloud App Discovery** functionality.

- Use policies to control the use of personal information within third-party cloud applications.
- Use Cloud App Security to investigate files and set policies based on **Azure Information Protection** classification labels in cloud apps.
- Administrators can use PowerShell string-matching or regex queries to search for and identify personal data in some file types in local or connected storage.
- **Azure Information Protection (AIP)** enables classification, labelling, and protection of data in local storage and in Windows Server file servers that support File Classification Infrastructure (FCI).

8.2 STEP 2 - Manage

The GDPR provides data subjects—individuals to whom data relates—with more control over how their personal data is captured and used. Microsoft Office 365 enables data governance practices and processes using multiple tools that enable you to manage personal data to help keep it secure and private.

- **Advanced Data Governance**. Use this tool to manage personal data with proactive policy recommendations and data classifications that help you act on system alerts to flag risks, and filter and migrate data to Office 365.
- **Labels**. Use Labels to classify personal data across the organization for governance and enforce retention rules based on that classification.
- Information Rights Management. Use this technology to prevent unauthorized persons from accessing personal data in Office 365.
- **eDiscovery and Advanced eDiscovery**. Use these tools to manage eDiscovery cases in your organization.
- **PowerShell**. Use this command line shell and scripting language to disable data subject access to target services to prevent additional processing of personal data.
- **SharePoint Online**. Use SharePoint Online to manually track and manage data subject rights requests.
- **Exchange Online mail flow rules**. Use mail flow rules to route mail to specific mailboxes to help with a customized client process for receiving, managing, and responding to data subject rights requests.
- **PowerShell for the Office 365 admin centre**. Use these to rectify inaccurate or incomplete personal data and to erase personal data upon request.
- **Advanced eDiscovery and PowerShell, and Exchange Online.** Use these to export personal data to be provided to data subjects in a common, structured format.
- **Office 365 Data Loss Prevention (DLP) policies**. Use these policies to set limits on the processing of the personal data of specific data subjects and use PowerShell to identify and place restrictions on files that match specific personal data types or match keyword queries.
- Use labels to apply classifications with persistent data protection to enable secure file sharing and apply governance policies to personal data with **Azure Information Protection**.
- Restrict certain processing activities for specific data subjects with **Azure Information Protection**.
- Leverage the classification labels set by Azure Information Protection to enforce automatic governance actions and take additional governance actions for specific files or users, or from a specific policy on connected apps with **Cloud App Security**.
- Create restrictive policies that ingest the relevant Azure Information Protection classification label with **Cloud App Security**.
- Present your own customized privacy notice and contact information to customers as well as present your own custom terms for a click-through acceptance with **Microsoft Intune**.
- Administrators can use Windows permissions to manage the authorization of users, groups, and computers to access network objects and object properties.
- Domain-based **Dynamic Access Control (DAC)** enables you to apply and enforce access-control permissions and restrictions based on well-defined rules that can include the sensitivity of the resources, the job or role of the user, and the configuration of the device that is used to access these resources.
- With Azure RMS in **Azure Information Protection (AIP)**, you can assign and enforce persistent restrictions on sharing files that contain personal data, as well as enforce encryption requirements.

- Organizations can host customized privacy notices within their individual public-facing applications on the Windows platform. Plus, Windows can run applications or house other technologies used to obtain consent for relevant processing activities.
- You can use Windows Search or PowerShell to locate and discontinue processing of files containing personal data, to rectify inaccurate or incomplete personal data or erase personal data when requested, and to restrict processing of personal data.
- You can use the native data export features of Windows 10 to manually transfer data in a variety of file formats.
- Windows provides a platform for accessing applications such as Dynamics 365 and Office 365 that can help you track and manage Data Subject Rights requests.

8.3 STEP 3 – Protect

The GDPR requires that organizations incorporate data privacy and protection principles into their products and services. To support customers' efforts to protect their sensitive personal data, Microsoft Office 365 solutions are developed using the Microsoft Secure Development Lifecycle, which defines the privacy principles and standard privacy features that inform product development and incorporates privacy-by-design and privacy-by-default methodologies.

- Adjust privacy settings in Word, Excel, and PowerPoint to limit Office applications' connection to the internet, make hidden mark-up visible, and inspect and remove personal data from documents with Document Inspector.
- Limit access to shared files or folders in OneDrive for Business and manage who can view or edit the files.
- Use the option to encrypt Word, Excel, and PowerPoint documents with password protection.
- Use **Azure Information Protection** for encryption and rights management.
- Use the encryption option during the PST Import Service.
- Encrypt messages when transferring personal data to external parties via email with **Office 365 Message Encryption (OME)**.
- Use **Threat Intelligence** to help proactively uncover and protect against advanced threats in Office 365.
- Protect email against unknown, sophisticated malware attacks in real time by using **Advanced Threat Protection for Exchange Online (which requires an Office 365 E5 subscription)**.
- Identify high-risk and abnormal usage by getting alerts to potential breaches, enabling you to track and respond to high risk actions with **Advanced Security Management**.
- Monitor and capture all activity that occurs within your tenant using the **Management Activity API**.
- Create policies to automatically encrypt files containing sensitive personal data, and label sensitive files or emails using **Azure Information Protection**.
- Create, deploy, and monitor configuration policies that enforce device-level encryption for Android and iOS phones managed by **Microsoft Intune**.
- Protect against advanced persistent threats and malicious attacks with **Microsoft Advanced Threat Analytics**.
- Obtain deep visibility and control of data inside cloud applications and threat protection with **Microsoft Cloud App Security**.
- Manage employee identities and employee access privileges with **Azure Active Directory** to provide conditional access, user and sign-in risk calculation, multi-factor authentication and privileged identity management to help secure and restrict access to data.
- Protect your employees' privacy when you're discovering **Software as a Service (SaaS)** apps in your organization using the **Cloud App Security** log anonymization feature.
- Enforce compliance of policies restricting jailbroken devices and requiring encryption, and wipe or lock devices remotely with **Microsoft Intune**.
- Help defend against breaches by identifying abnormal behaviour of entities, advanced attacks and security risks using **Microsoft Advanced Threat Analytics** on-premises.

- Identify anomalies in cloud usage that may be indicative of a data breach and defend against unauthorized access or sharing of personal data by applying **File Policies** with **Microsoft Cloud App Security**.
- Provide administrators with reports of employee user accounts flagged for risk and risky sign-ins using **Azure Active Directory** security reports.
- Securely share data within or outside of an organization, and monitor activities on shared data.
- The **Just Enough Administration (JEA)** technology is used to restrict IT administrative rights. This technology provides a practical, role-based approach to set up and automate restrictions that reduce the risks associated with providing users with full administrative rights.
- **Shielded Virtual Machines** (VMs) and guarded fabric protect VMs from malicious administrators in the fabric by encrypting the disk and state of VMs so that only VM or tenant administrators can access them.
- Administrators can use **BitLocker Drive Encryption** to provide volume-level encryption that can help protect personal data housed on lost, stolen, or inappropriately decommissioned machines or removable media.
- **Windows Information Protection (WIP)** provides a tool to protect data against accidental or intentional disclosure and gives administrators the ability to create persistent data protection policies to enforce encryption of personal data.
- **Azure Information Protection (AIP)** enables users to classify, label, and protect data in local storage and in Windows Server file servers that support **File Classification Infrastructure (FCI).**
- **Windows Hello** provides biometric and multi-factor authentication for stronger security.
- **Windows Defender Credential Guard** helps mitigate the risk of certain credential-theft attacks.
- **AppLocker** helps administrators create and deploy application control policies, restricting access by unauthorized users to applications that could put personal data at risk.
- Personal information stored on or accessed by devices is safeguarded by device security technologies. These include **Windows Trusted Boot** and **Device Guard** for client/end-user devices and **Shielded Virtual Machines**— built on top of Microsoft Hyper-V—as well as **Windows Backup and Restore** for servers. These technologies protect sensitive Windows processes by isolating them from user mode processes and the Windows kernel.
- **Windows Defender Advanced Threat Protection (ATP)** for Windows 10 enables administrators to detect and respond to advanced threats on their networks.
- Enhanced Logging enables Windows Server administrators to identify suspicious behaviour by auditing access to kernel and other sensitive processes.
- Administrators can use **Advanced Threat Analytics**, the **Test-AppLocker PowerShell** cmdlet, and **Device Guard (in audit mode)** to facilitate regular testing of security measures.

8.4 STEP 4 – Report

The GDPR sets new standards in transparency, accountability, and record-keeping. Organizations processing personal data will need to keep detailed records to be compliant.

- Use the **Unified Audit** log to track and record processing activities across the Office 365 environment and record the resolution of data subject rights requests and log events associated with amending, erasing, or transferring personal data, and to provide insight into data that has transferred to third parties through email or shared using **SharePoint Online** and **OneDrive for Business**.
- Use **Exchange Message** tracking to determine the recipient of an email and if it was received, rejected, deferred, or delivered.
- Use the **Office 365 Management Activity API** to identify user sharing activities in **Exchange Online** and **SharePoint Online**.
- Analyse how sensitive data is distributed, including document tracking and revocation for users and admins, using **Azure Information Protection** logging and reporting functionality.
- Help identify privileged actions that occurred in the **Azure Active Directory** with the **Azure Active Directory Audit Reports**.

- Provide insight into auditable events within the directory using **Azure Active Directory** access and usage reports.
- Understand use cases, identify top users, and determine the risk associated with each cloud app with the **Cloud Discovery Dashboard** continuous reporting feature.
- Detect anomalies, suspicious activities, malicious attacks and security issues in your environment using the **Microsoft Advanced Threat Analytics** attack timeline.
- Geographically track documents classified with **Azure Information Protection** using the **Document Tracking and Revocation** functionality.
- Trace documents classified using Azure Information Protection and shared with third parties by using the **Azure Information Protection Document Tracking and Revocation** functionality.
- Identify SaaS applications in their environment and evaluate your security measures to help you perform a **Data Protection Impact Assessment (DPIA)** on your use of cloud applications with the **Cloud App Catalog** within **Microsoft Cloud App Security**.
- **Azure Information Protection**. Document Tracking and Revocation functionality can help map locations of users to restrict transfers of personal data outside the European Union.
- **Advanced Audit Policy Recommendations**. These can be used to help organizations track compliance with important business-related and security-related rules.
- **Active Directory Rights Management Services (AD RMS)**. Administrators can use AD RMS to track the use of protected documents and record flows of personal data to third-party service providers.

9 OFFICE 365 FEATURE COMPARISON

The following table displays which of the features are available from within each product set to ensure compliance with GDPR.

Feature	Office 365	Enterprise Mobility + Security	Windows 10
Data Loss Prevention (DLP)	✔	✔*	
Advanced Data Governance	✔	✔*	
Office 365 eDiscovery	✔	✔*	
Office 365 Advanced eDiscovery	✔	✔*	
Customer Lockbox	✔	✔*	
Advanced Threat Protection	✔	✔*	
Threat Intelligence	✔	✔*	
Advanced Security Management	✔	✔*	
Office 365 audit logs	✔	✔*	
Azure Active Directory (Azure AD)		✔	
Multi-Factor Authentication		✔	
Cloud App Security		✔	
Azure Information Protection		✔	
Advanced Threat Analytics		✔	
Windows Hello			✔
Windows Defender			✔
Windows Defender Advanced Threat Protection			✔
Device Guard			✔
Credential Guard			✔

Feature	Office 365	Enterprise Mobility + Security	Windows 10
BitLocker Drive Encryption			✔
Windows Information Protection			✔

*When combined with Office 365 or under the title Microsoft 365.

10 APPENDIX A – USEFUL LINKS

These links are helpful in planning for GDPR policies and securing the environment:

10.1 Data Loss Prevention Policies

These allow businesses to identify, monitor and protect sensitive information across Office 365.

https://support.office.com/en-US/article/Overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e

10.2 Advanced Data Governance

Manages the lifecycle of the data in the organisation.

https://support.office.com/en-us/article/Manage-data-governance-in-Office-365-48064107-fed2-4db0-9e5c-aa5ddd5ccb09

10.3 eDiscovery

Requires an Office 365 E5 Subscription. eDiscovery helps analyse unstructured data to allow for the reduction of data.

https://support.office.com/en-us/article/Office-365-Advanced-eDiscovery-fd53438a-a760-45f6-9df4-861b50161ae4

10.4 Customer Lockbox

Gives control to the end user when Microsoft might need to gain access to data.

https://blogs.office.com/en-us/2015/04/21/announcing-customer-lockbox-for-office-365/

10.5 Advanced Threat Protection

Protects against sophisticated attacks in real time.

https://products.office.com/en-us/exchange/online-email-threat-protection

10.6 Threat Intelligence

Helps proactively uncover and protect against advanced threats.

https://blogs.office.com/en-GB/2016/09/26/applying-intelligence-to-security-and-compliance-in-office-365/

10.7 Advanced Security Management

Detects potentially suspicious activity in the organisation.

https://blogs.technet.microsoft.com/solutions_advisory_board/2017/01/24/office-365-advanced-security-management-overview-and-demonstration/

10.8 Office 365 audit log

Search the audit log to identify risks.

https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c#auditlogevents

10.9 Microsoft Trust Center

The main source of information for security and trust in Office 365.

https://www.microsoft.com/en-us/trustcenter

10.10 Office 365 Protection Center

The main area for managing protection of the Office 365 tenancy.

https://protection.office.com/#/homepage