General Data Protection Regulation

An Introduction to GDPR

D. Vanderbist 05/06/2017

Content

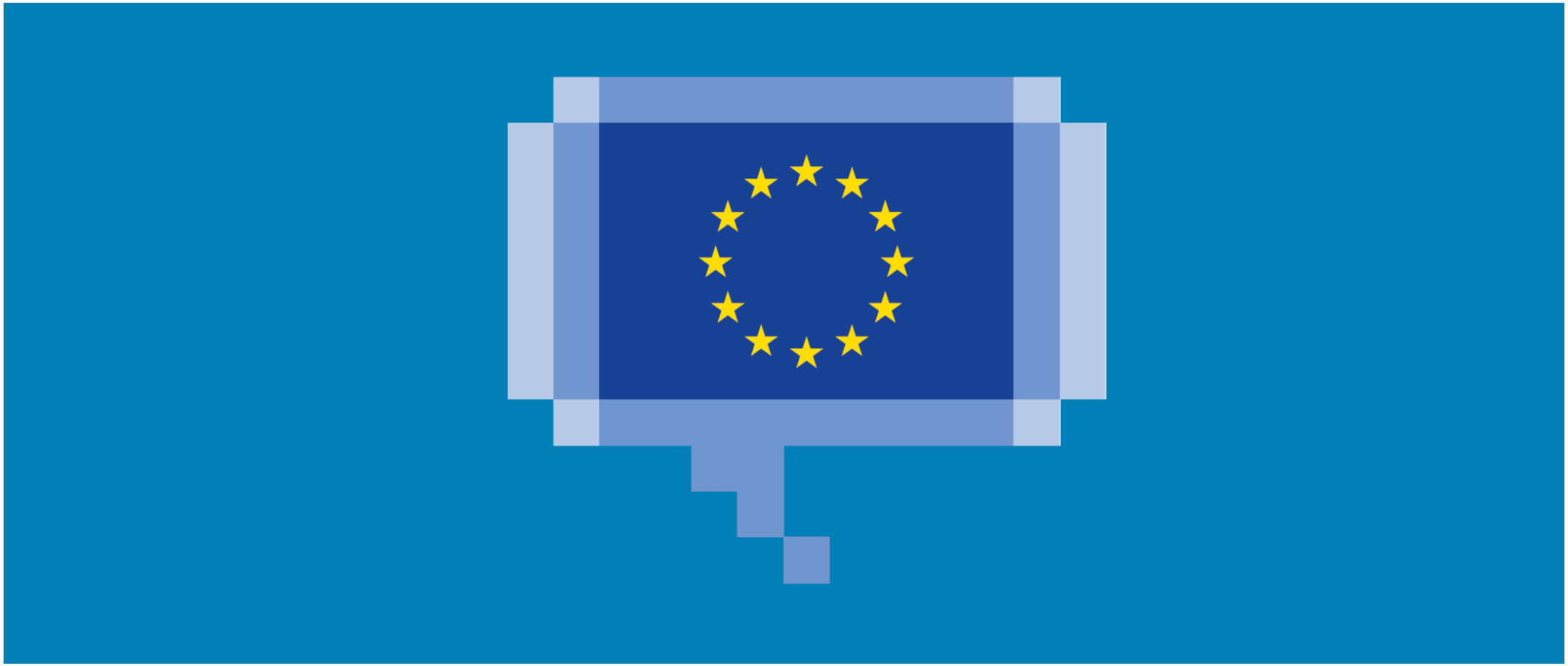
GDPR Europe's Vision:

- What is GDPR?
- Why GDPR?
- GDPR addresses what?
- What must a company do?
- Impact?
- GDPR in practice!
- Additional Resources

GDPR in Microsoft's Eco-System:

- Introduction
- MS' interpretation of GRP
- How to Address GDPR?
  - Discover
  - Manage
  - Protect
  - Report
- GDPR in MS Technologies
  - GDPR in MS Azure
  - GDPR in MS Dynamics 365
  - GDPR in MS Enterprise Mobility and Security
  - GDPR in MS Office and Office 365
  - GDPR in MS SQL Server/Azure SQL Database
  - GDPR in MS Windows 10 and Windows Server 2016
- Additional Resources

GDPR Europe's Vision



What is GDPR?

GDPR:

- GDPR stands for General Data Protection Regulation
- GDPR is a privacy regulation that allow citizen to gain control of one's personal data.

GDPR's goals:

- To make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the internet.
- To strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market

Timeframe:

- Updates legislation from 1995
- Comes into play in May 2018

Why GDPR?

Why change the rules?

It's about trust...

A lack of trust in old data protection rules held back the digital economy and quite possibly your business.

of people feel they have complete control over the information they provide online.

And helping business boom...

One set of rules for all companies processing data in the EU

Doing business just got easier and fairer

The new system keeps costs down and will help business grow

€130 million

cost of informing 28 different Data Protection Authorities for business in the EU under the old system.

€2.3 billion

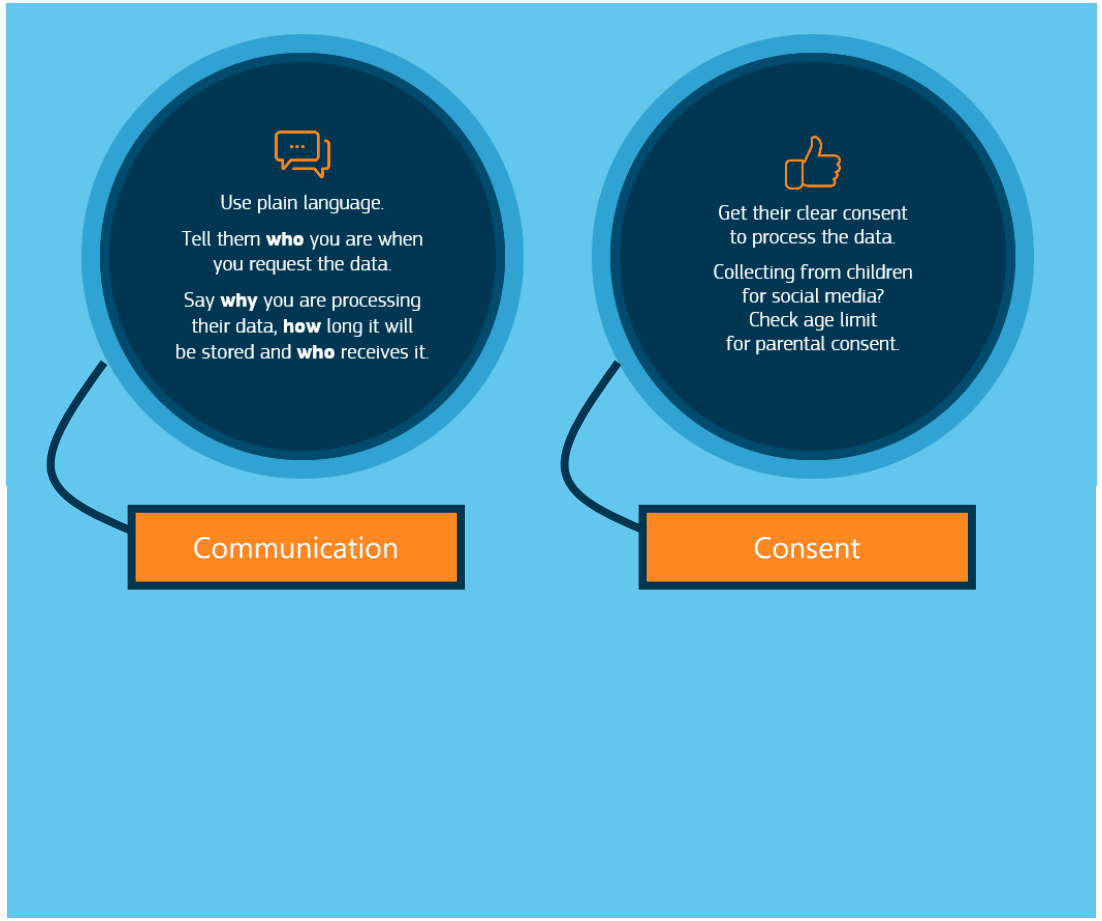
estimated economic benefits of having one law.

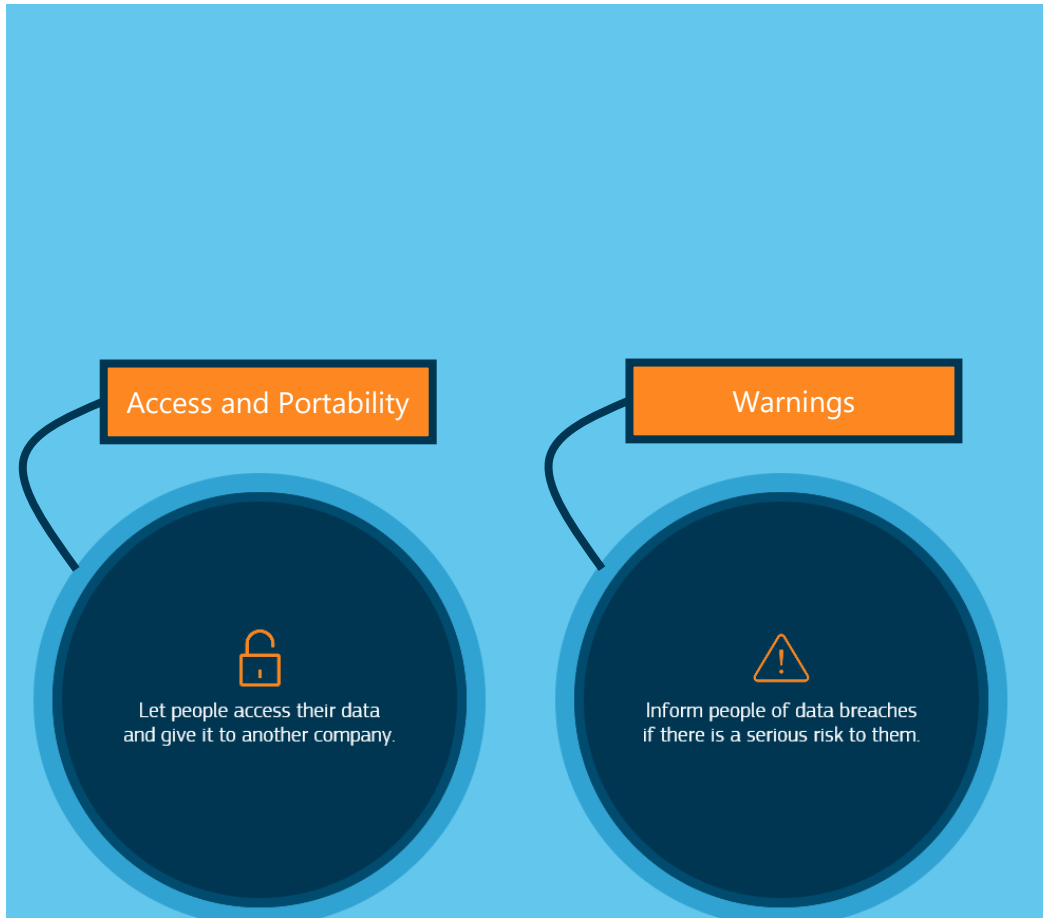
New rules should **boost consumer confidence** and in turn **business**.

GDPR Addresses …

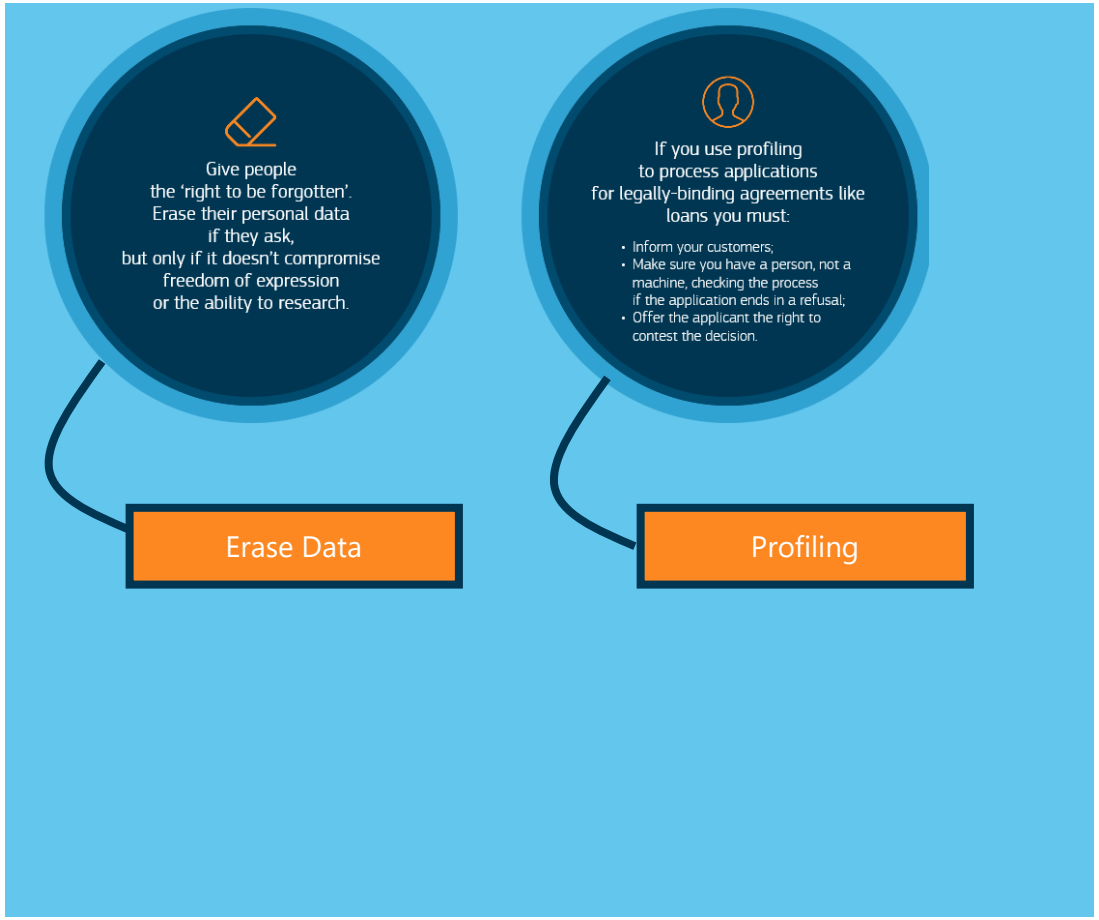
- A "right to be forgotten": When an individual no longer wants her/his data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted. This is about protecting the privacy of individuals, not about erasing past events or restricting freedom of the press.
- Easier access to one's data: Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. A right to data portability will make it easier for individuals to transmit personal data between service providers.
- The right to know when one's data has been hacked: Companies and organizations must notify the national supervisory authority of data breaches which put individuals at risk and communicate to the data subject all high risk breaches as soon as possible so that users can take appropriate measures.
- Data protection by design and by default: 'Data protection by design' and 'Data protection by default' are now essential elements in EU data protection rules. Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm – for example on social networks or mobile apps.
- Stronger enforcement of the rules: data protection authorities will be able to fine companies who do not comply with EU rules up to 4% of their global annual turnover.

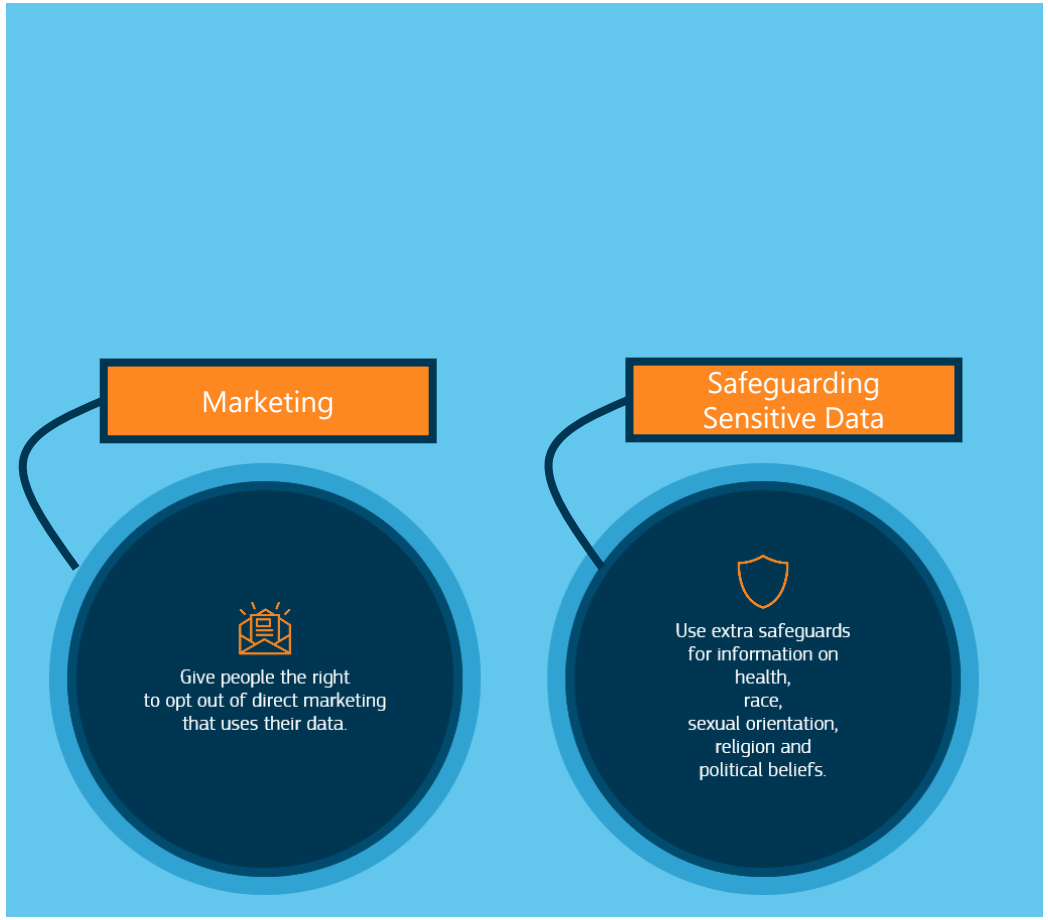
What must a Company do?





What must a Company do?





What must a Service Provider do?

Processing data for another company?
Make sure you have a watertight contract listing the responsibilities of each party.

Check if you need a data protection officer

This is not always obligatory. It depends on the type and amount of data you collect, whether processing is your main business and if you do it on a large scale.

You process personal data to target advertising through search engines based on people's behaviour online.	Yes
You send your clients an advert once a year to promote your local food business.	No
You are a GP and collect data on your patients' health.	No
You process personal data on genetics and health for a hospital.	Yes

Anticipate with impact assessments

Impact assessments may be required for **HIGH-RISK** processing.

- New technologies
- Automatic, systematic processing and evaluation of personal information
- Large-scale monitoring of a publicly accessible area (e.g. CCTV)
- Large-scale processing of sensitive data like biometrics

Keep records

SMEs only have to keep records if data processing is

Records should contain:

- ✓ **Name and contact details of business**
- ✓ **Reasons for data processing**
- ✓ **Description of categories of data subjects and personal data**
- ✓ **Categories of organisations receiving the data**
- ✓ **Transfer of data to another country or organisation**
- ✓ **Time limit for removal of data, if possible**
- ✓ **Description of security measures used when processing, if possible**

VDB

Impact?

The cost of non-compliance

Your local Data Protection Authority monitors compliance; their work is coordinated at EU-level.
The cost of falling foul of the rules can be high.

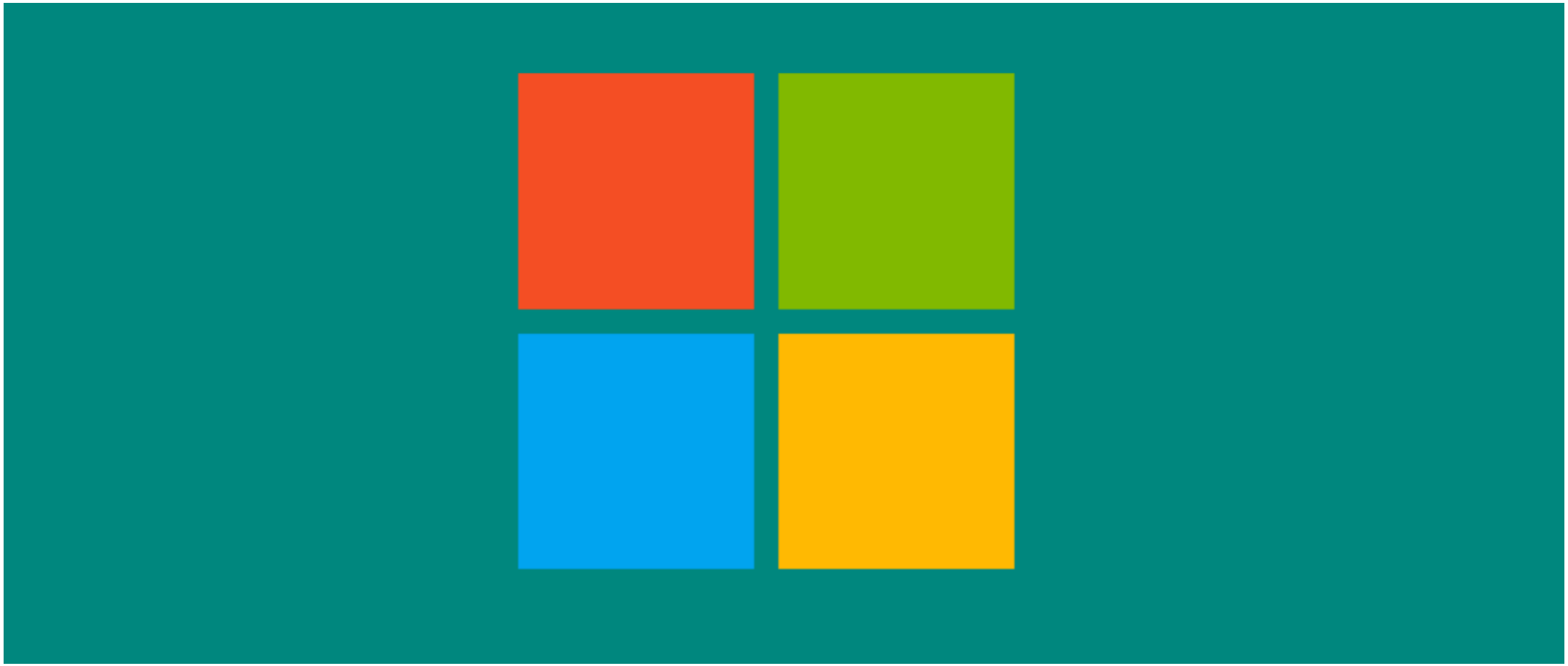
GDPR in Practice! EU simplified the Rules

- One continent, one law: a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Companies will deal with one law, not 28. The benefits are estimated at €2.3 billion per year.
- One-stop-shop: a 'one-stop-shop' for businesses: companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU.
- The same rules for all companies – regardless of where they are established: Today European companies have to adhere to stricter standards than companies established outside the EU but also doing business in our Single Market. With the reform companies based outside of Europe will have to apply the same rules when they offer goods or services on the EU market. This creates a level playing field.
- Technological neutrality: the Regulation enables innovation to continue to thrive under the new rules

Additional resources:

http://ec.europa.eu/justice/data-protection/reform/index_en.htm

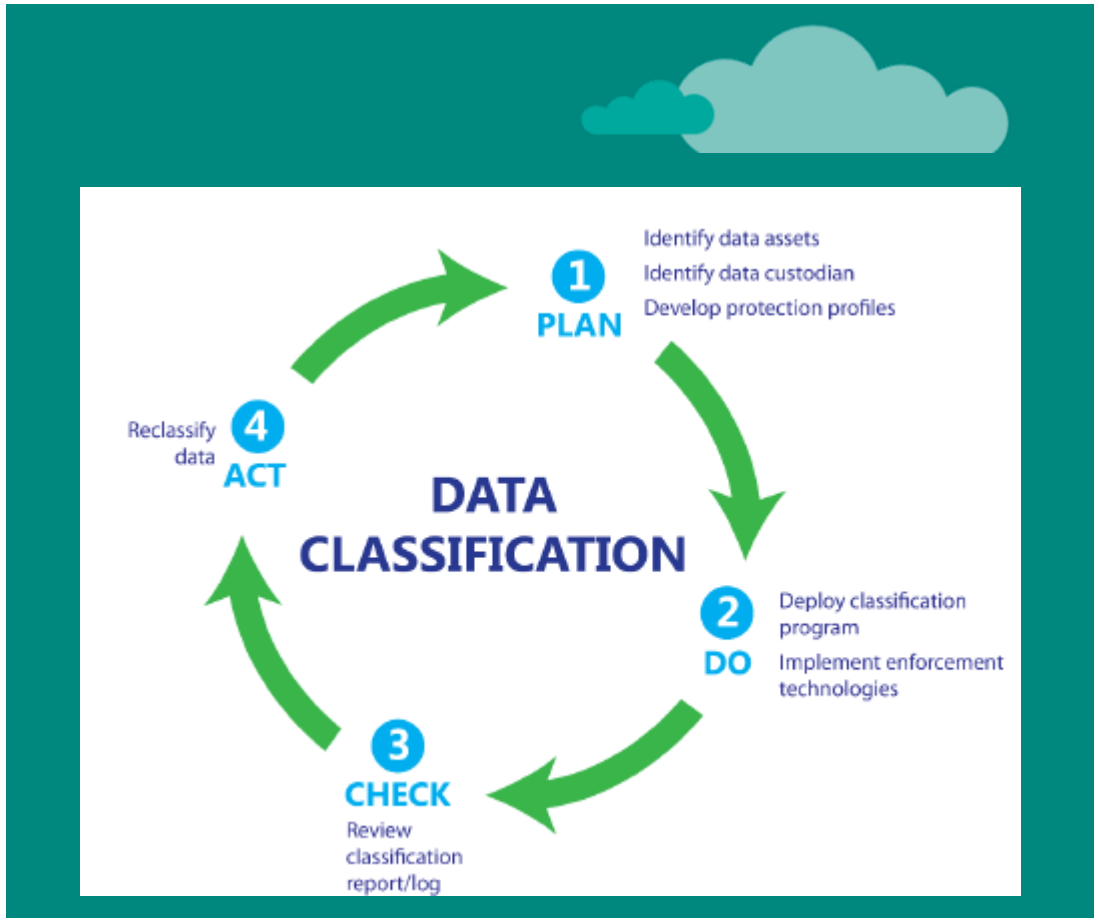
GDPR in Microsoft's Eco-System



Introduction

MS' Interpretation of GDPR

- Enhanced personal privacy rights - strengthened data protection for residents of EU by ensuring they have the right to access to their personal data, to correct inaccuracies in that data, to erase that data, to object to processing of their personal data, and to move it;
- Increased duty for protecting data - reinforced accountability of companies and public organizations that process personal data, providing increased clarity of responsibility in ensuring compliance;
- Mandatory data breach reporting - companies are required to report personal data breaches to their supervisory authorities without undue delay, generally no later than 72 hours; and
- Significant penalties for non-compliance - steep sanctions, including substantial fines that are applicable whether an organization has intentionally or inadvertently failed to comply.



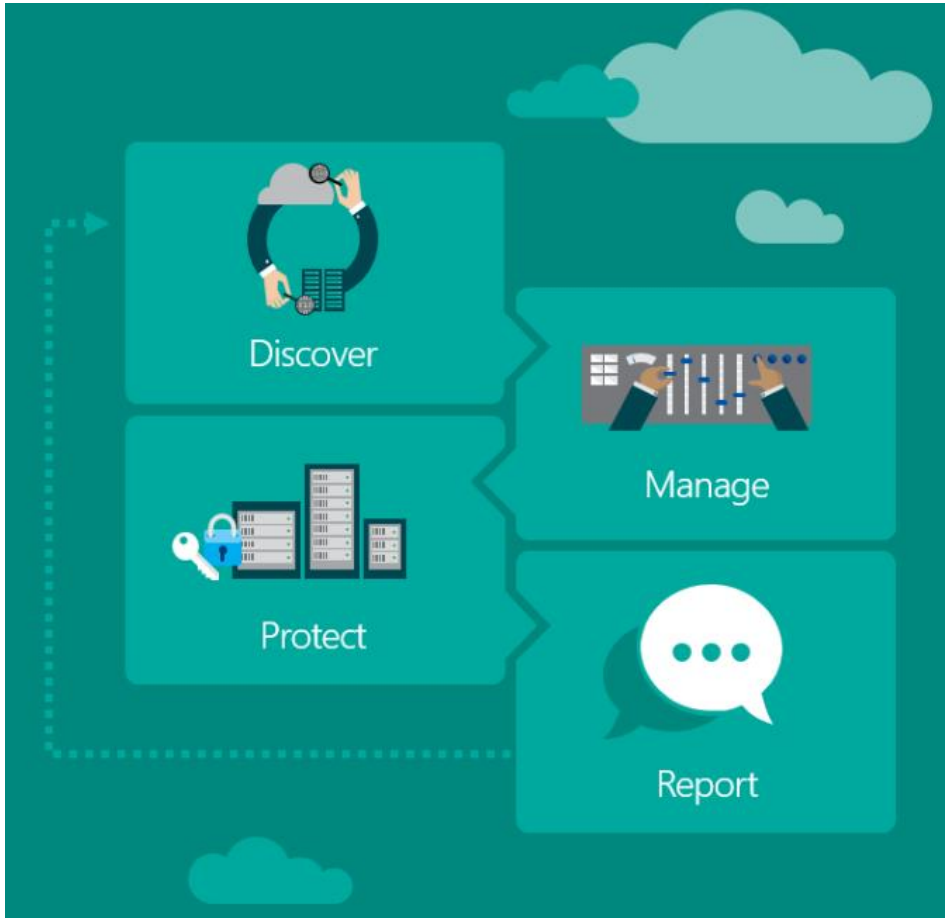
MS' Interpretation of GDPR

- *Transparency, fairness, and lawfulness in the handling and use of personal data. You will need to be clear with individuals about how you are using personal data and will also need a "lawful basis" to process that data.*
- *Limiting the processing of personal data to specified, explicit, and legitimate purposes. You will not be able to re-use or disclose personal data for purposes that are not "compatible" with the purpose for which the data was originally collected.*
- *Minimizing the collection and storage of personal data to that which is adequate and relevant for the intended purpose.*

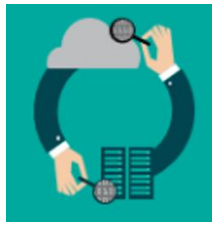
- *Ensuring the accuracy of personal data and enabling it to be erased or rectified. You will need to take steps to ensure that the personal data you hold is accurate and can be corrected if errors occur.*
- *Limiting the storage of personal data. You will need to ensure that you retain personal data only for as long as necessary to achieve the purposes for which the data was collected.*
- *Ensuring security, integrity, and confidentiality of personal data. Your organization must take steps to keep personal data secure through technical and organizational security measures.*

How to Address GDPR?

- Discover the data that's subject to the GDPR
- Manage how personal data is used and accessed
- Protect the data by establishing controls
- Report on data use, including plans for managing data requests and providing public notifications about breaches



How to Address GDPR? Discover



Identify what personal data you have and where it resides

Building your inventory

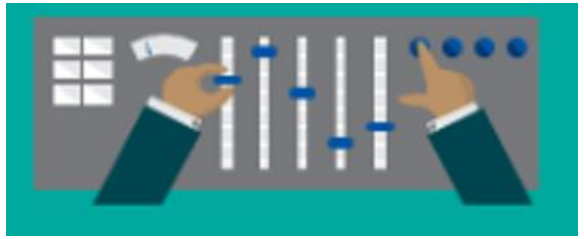
To understand whether the GDPR *does* apply to your organization and, if it does, what obligations it imposes, **it is important to inventory your organization's data**. This will help you to understand:

- What data is personal?
- Which are the systems where that data is collected and stored?
- Why it was collected?
- How it is processed and shared?
- How long it is retained?

Supporting Technologies:

- Azure: Microsoft Azure Data Catalog
- Dynamic 365: Reporting & Analytics dashboards of Dynamics 365
- Mobility: Microsoft Azure Information Protection, Enterprise Mobility and Security (EMS).
- Office 365: Data Loss Prevention (DLP), Content Search and eDiscovery
- SharePoint: SharePoint Search Services
- SQL Server and Azure DB: DB queries
- Windows and Windows Server: Window Search

How to Address GDPR? Manage



Govern how personal data is used and accessed

Data Governance

Once that inventory is complete, it is also important to develop and implement a data governance plan. A data governance plan can help you:

- **Define policies, roles, and responsibilities** for the access, management, and use of personal data,
- Ensure your data **handling practices comply** with the **GDPR.**

Data Classification:

Adopting a classification scheme that applies throughout your organization can be particularly helpful for **responding to data subject requests**, because it enables you to identify more readily and process personal data requests.

Supporting Technologies:

- Azure: Data Classification
- Dynamic 365: Security and Compliance Planning Guide
- Mobility: Azure Information Protection
- Office 365: Data Loss Prevention (DLP), Advanced Data Protection
- Windows and Windows Server: Advanced Data Classification Toolkit

How to Address GDPR? Protect

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

Protecting Data

There are many types of risk to identify and consider—ranging from physical intrusion or rogue employees to accidental loss or hackers.

- Risk management plans
- Risk mitigation steps: password protection, audit logs, and encryption

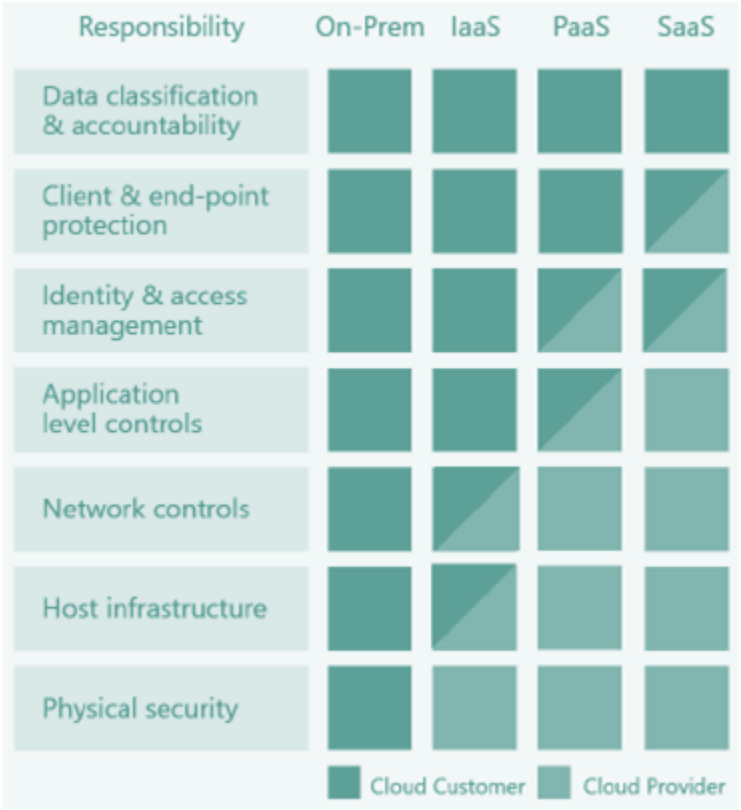
Supporting Technologies:

- Azure: Azure Security Center, Data Encryption, Azure Key Vault, MS Antimalware
- Dynamic 365: Role, Record and Field based Security
- Mobility: Azure AD, Azure Information Protection, Cloud App Security, MS Intune
- SQL Server and Azure DB: Azure SQL DB Firewall, SQL Authentication and Authorization, Dynamic Data Masking (DDM), Record Based Security (RBS), Transparent Encryption, Always Encrypted, SQL Server Audit, SQL DB Treat Detection
- Windows and Windows Server: Window Hello, Antivirus, Device and Credential Guard, BitLocker
- Office 365: Data Loss Prevention (DLP), Advanced Data Protection

Who Carries GDPR's Responsibility?

avanade

Microsoft



VDB

How to Address GDPR? Protect

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

Detecting and Responding to Data Breaches

In certain cases, the GDPR requires that if a data breach occurs, organizations **need to rapidly notify regulators**. In some cases, organizations will also **need to notify the affected data subjects.** In order to meet this requirement, organizations will benefit from being able to monitor for and detect system intrusions.

Incident response program process:

- **Assess** the **impact and severity** of the event.
- Conduct a t**echnical or forensic investigation**, and identify containment, mitigation, and workaround strategies.
- Create a **recovery plan** to mitigate the issue.
- Create a **post-mortem** that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the event.

Supporting Discover Technologies:

- Azure: Azure Security Center, Azure Log Analytics
- Mobility: MS Advance Threat Analytics, Cloud App Security, Azure AD Premium
- Office 365: Threat Intelligence, Advanced Security Management, Advanced Treat Protection
- Windows and Windows Server: Windows Defender Advance Treat Protection (ATP)

How to Address GDPR? Report

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

Record Keeping

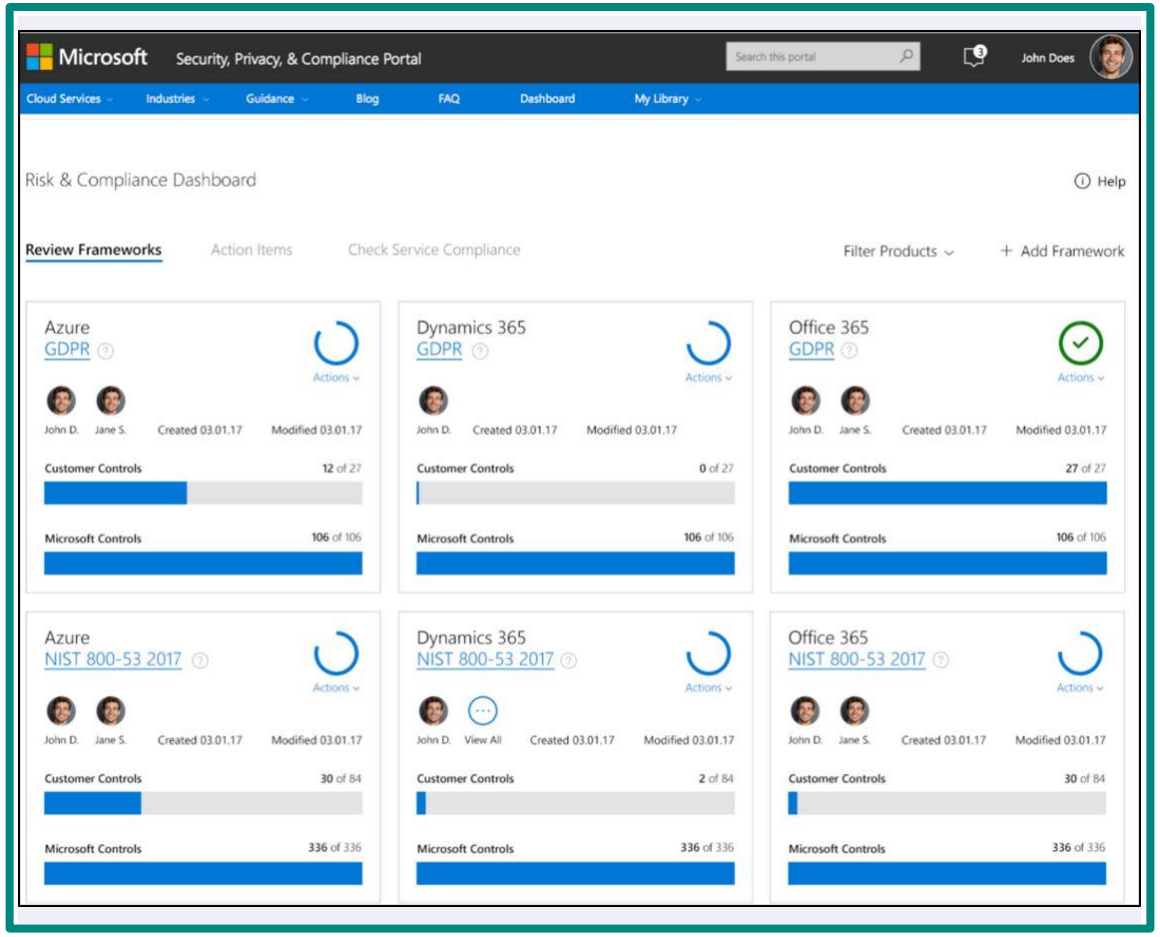
Organizations processing personal data will need to keep records about:

- The purposes of processing
- The categories of personal data processed
- The identity of third parties with whom data is shared
- Whether (and which) third countries receive personal data, and the legal basis of such transfers
- Organizational and technical security measures
- Data retention times applicable to various datasets.

Supporting Discover Technologies:

- Azure, Office 365, Dynamic 365: Service Trust Portal
- Azure: Logging, Azure Monitor
- Office 365: Service Assurance, Audit Logs, Customer Lockbox
- Mobility: Azure Information Protection
- Windows and Windows Server: Windows Defender Advance Treat Protection (ATP)

How to Address GDPR?
Compliance Portal



GDPR in MS Azure

Microsoft designed Azure 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. Azure can help you on your journey to reducing risks and achieving compliance with the GDPR.

Identifying what data you have and controlling who has access to it is a critical requirement of the GDPR. Azure enables you to manage user identities and credentials and control access to your data in several ways:

Azure Active Directory (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 privileges through access control, management, and reporting.

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 your organization, track usage, and even revoke access remotely. Azure Information Protection also includes rich logging and reporting capabilities to monitor the distribution of data, and options to manage and control your encryption keys.

Protecting personal data in your systems, and reporting on and reviewing for compliance are key requirements of the GDPR. The following Azure services and tools will help you meet these GDPR obligations:

Azure Security Center provides you with visibility and control over the security of your Azure resources. It continuously monitors your resources, provides helpful security recommendations, and helps you prevent, detect, and respond to threats. Azure Security Center's embedded advanced analytics help you identify attacks that might otherwise go undetected.

Data Encryption in Azure Storage secures your data at rest and in transit. You can, for example, automatically encrypt your data when it is written to Azure Storage using Storage Service Encryption. Additionally, you can use Azure Disk Encryption to encrypt operating systems and data disks used by virtual machines. Data is protected in transit between an application and Azure so that it remains secure at all times.

Azure Key Vault enables you to safeguard your cryptographic keys, certificates, and passwords that help protect your data. Key Vault uses hardware security modules (HSMs) and is designed so that you maintain control of your keys and therefore your data, including ensuring that Microsoft cannot see or extract your keys. You can monitor and audit use of your stored keys with Azure logging, and import your logs into Azure HDInsight or your SIEM for additional analysis and threat detection.

Log Analytics: Azure provides configurable security auditing and logging options that can help you identify and repair gaps in your security policies to prevent breaches. Additionally, Log Analytics helps you collect and analyze data generated by resources in either your cloud or on-premises environments. It provides real-time insights using integrated search and custom dashboards to readily analyze millions of records across all workloads and servers regardless of their physical location.

GDPR in MS Dynamics 365

Microsoft designed Dynamics 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. Dynamics 365 can help you on your journey to reducing risks and achieving compliance with the GDPR.

Controlling who has access to personal data is a key to securing that data, and data security is a critical requirement of the GDPR. Dynamics 365 enables you to manage and control access to your data in several ways:

Role-based security in Microsoft Dynamics 365 allows you to group together a set of privileges that limit the tasks that can be performed by a given user. This is an important capability, especially when people change roles within an organization.

Record-based security in Dynamics 365 allows you to restrict access to specific records.

Field-level security in Dynamics 365 allows you to restrict access to specific high-impact fields, such as personally identifiable information.

Azure Active Directory (Azure AD) helps you protect Dynamics 365 from unauthorized access by simplifying the management of users and groups and allowing you to assign and revoke privileges easily. Azure AD includes tools such as Multi-Factor Authentication for highly-secure sign-in. Additionally, Azure AD Privileged Identity Management helps you reduce risks associated with administrative privileges through access control, management, and reporting.

Another core requirement of the GDPR is to protect the personal data that you control or process. Dynamics 365 is designed to optimize the security of your data:

Security Development Lifecycle is a mandatory Microsoft process that embeds security requirements into every phase of the development process. Dynamics 365 is built using the Security Development Lifecycle.

Encryption in transit between your users' devices and our data centers, as well as while at rest in a Microsoft database, helps protect your Dynamics 365 data at all times.

GDPR in MS Enterprise Mobility and 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:

Azure Active Directory (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.

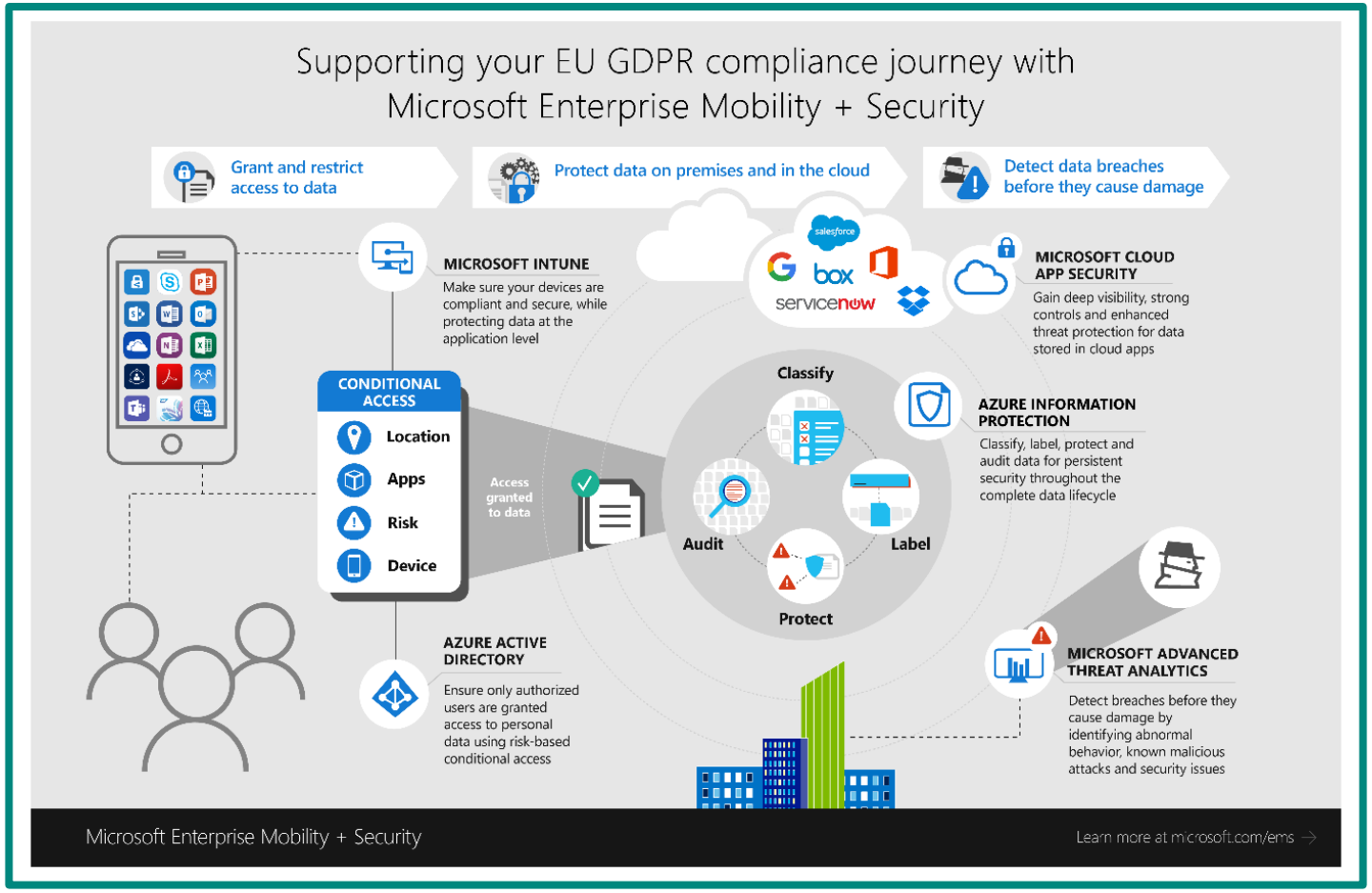
Microsoft Cloud App Security helps you discover all the cloud apps in your environment, identify users and usage, and get a risk score for each app. You can then decide if you'd like your users to access these apps. Cloud App Security then provides visibility, control, and threat protection for the data 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.

Microsoft 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.

Microsoft Advanced Threat Analytics helps pinpoint breaches and identifies attackers using innovative behavioral 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 behavioral 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.

GDPR in MS Enterprise Mobility and Security



GDPR in MS Office and Office 365

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:

Advanced Threat Protection in 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.

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.

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.

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.

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:

Advanced Threat Protection in 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.

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.

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.

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.

GDPR in MS SQL Server/Azure SQL Database

Microsoft designed SQL Server and Azure SQL Database with industry-leading security measures and privacy policies to safeguard your data in the database, including the categories of personal data identified by the GDPR. Built-in SQL security capabilities can help you on your journey to reducing risks and achieving compliance with the GDPR.

Controlling who has access to your database and managing how data is used and accessed is a critical requirement of the GDPR. SQL Server and Azure SQL Database provide controls for managing database access and authorization at several levels:

Azure SQL Database firewall limits access to individual databases within your Azure SQL Database server by restricting access exclusively to authorized connections. You can create firewall rules at the server and database levels, specifying IP ranges that are approved to connect.

SQL Server authentication helps you ensure that only authorized users with valid credentials can access your database server. SQL Server supports both Windows authentication and SQL Server logins. Windows authentication offers integrated security, and is recommended as the more secure option, where the authentication process is entirely encrypted. Azure SQL Database supports Azure Active Directory authentication, which offers a single sign-on capability and is supported for managed and integrated domains.

SQL Server authorization enables you to manage permissions according to the principle of least privilege. SQL Server and SQL Database use role-based security, which supports granular control of data permissions via the management of role memberships and object-level permissions.

Dynamic data masking (DDM) is a built-in capability that can be used to limit sensitive data exposure by masking the data when accessed by non-privileged users or applications. Designated data fields are masked in query results on the fly, while the data in the database remains unchanged. DDM is simple to configure and requires no changes to the application. For users of Azure SQL Database, dynamic data masking can automatically discover potentially sensitive data and suggest the appropriate masks to be applied.

Row-level security (RLS) is an additional built-in capability that enables SQL Server and SQL Database customers to implement restrictions on data row access. RLS can be used to enable fine-grained access over rows in a database table, for greater control over which users can access which data. Since the access restriction logic is located in the database tier, this capability greatly simplifies the design and implementation of application security.

Another core requirement of the GDPR is protecting personal data against security threats. SQL Server and SQL Database provide a powerful set of built-in capabilities that safeguard data and identify when a data breach occurs:

Transparent data encryption protects data at rest by encrypting the database, associated backups, and transaction log files at the physical storage layer. This encryption is transparent to the application, and uses hardware acceleration to improve performance.

Transport Layer Security (TLS) provides protection of data in transit on SQL Database connections.

Always Encrypted is an industry-first feature that is designed to protect highly sensitive data in SQL. Always Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the database engine. The mechanism is transparent to applications, as encryption and decryption of data is done transparently in an Always Encrypted–enabled client driver.

Auditing for SQL Database and SQL Server audit track database events and write them to an audit log. Auditing enables you to understand ongoing database activities, as well as analyze and investigate historical activity to identify potential threats or suspected abuse and security violations.

SQL Database Threat Detection detects anomalous database activities indicating potential security threats to the database. Threat Detection uses an advanced set of algorithms to continuously learn and profile application behavior, and notifies immediately upon detection of an unusual or suspicious activity. Threat Detection can help you meet the data breach notification requirement of the GDPR.

GDPR in MS Windows 10 and Windows 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:

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.

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.

Windows Defender Advanced Threat Protection (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.

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.

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."

BitLocker Drive Encryption 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.

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.

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.

Just Enough Administration and Just in Time Administration 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.

Additional resources:

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