



GDPR Workshop

Tuesday 13th February 2018



Agenda

GDPR, the story

Michael Wignall, National Technology Officer - Microsoft

How to prepare and implement

Alun Rogers, Director and Co-owner – risual

Abby Williams, Data Analyst Consultant – risual

Supporting GDPR with Technology

Stefanie Jacobs, Technology Solutions Professional - Microsoft

Break for lunch

Roundtable – Open Discussion

Accelerate GDPR compliance with the Microsoft Cloud

Michael Wignall - @mdwigs
Chief Technology Officer – Microsoft UK

“Make no mistake, the GDPR sets a new and higher bar for privacy rights, for security, and for compliance.

And while your journey to GDPR may seem challenging, Microsoft is here to help all of our customers around the world.”

Brad Smith
President & Chief Legal Officer
Microsoft Corporation



Providing clarity and consistency for the protection of personal data

The **General Data Protection Regulation** (GDPR) imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Microsoft believes the GDPR is an important step forward for clarifying and enabling individual privacy rights

What are the key changes to address the GDPR?



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 personal data



Controls and notifications

Organizations will need to:

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



Transparent policies

Organizations are required to:

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



IT and training

Organizations will need to:

- Train privacy personnel & employee
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

What does this mean for my data?



Our commitment to you

To simplify your path to compliance, we are committing to GDPR compliance across our cloud services when enforcement begins on May 25, 2018.

We will share our experience in complying with complex regulations such as the GDPR.

Together with our partners, we are prepared to help you meet your policy, people, process, and technology goals on your journey to GDPR.



Supporting our customers with contractual commitments

We will stand behind you with contractual commitments for our cloud services that:

- Meet stringent security requirements
- Support customers in managing data subject requests
- Provide documentation that enables customers to demonstrate compliance for all the other requirements of the GDPR applicable to processors and more

Microsoft was the first major cloud services provider to make these commitments to its customers. Our goal is to simplify compliance for our customers with both the GDPR and other major regulations.

Preparing for the GDPR



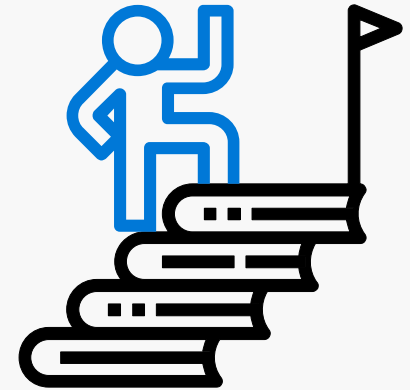
Simplify your privacy journey

Elevate your privacy practices with our cloud



Uncover risk & take action

Use our solutions to expose areas of risk and respond with agility and confidence

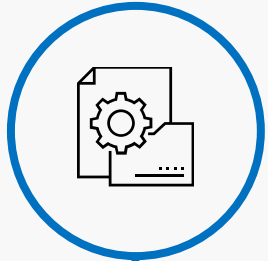


Leverage guidance from experts

Use our partner network to help you meet your privacy, security, and compliance goals

Simplify your privacy journey

Centralize, Protect, Comply with the Cloud



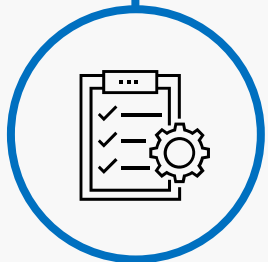
Process all in one place

Centralize processing in a single system, simplifying data management, governance, classification, and oversight.



Maximize your protections

Protect data with industry leading encryption and security technology that's always up-to-date and assessed by experts.



Streamline your compliance

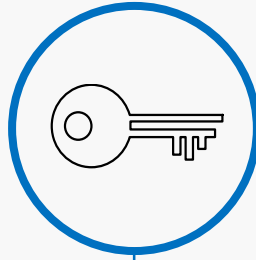
Utilize services that already comply with complex, internationally-recognized standards to more easily meet new requirements, such as facilitating the requests of data subjects.

Uncover risk and take action



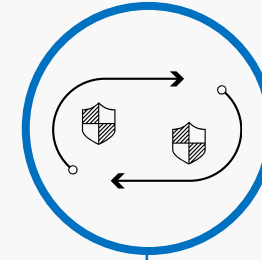
Discover data across systems

- Easily discover and catalog data sources
- Increase visibility with auditing capabilities
- Identify where personal info resides across devices, apps and platforms



Govern access and processing

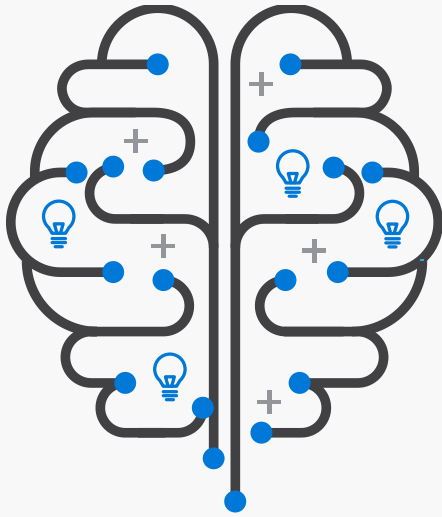
- Enforce use policies and access controls across your systems
- Classify data for simplified compliance
- Easily respond to data requests and transparency requirements



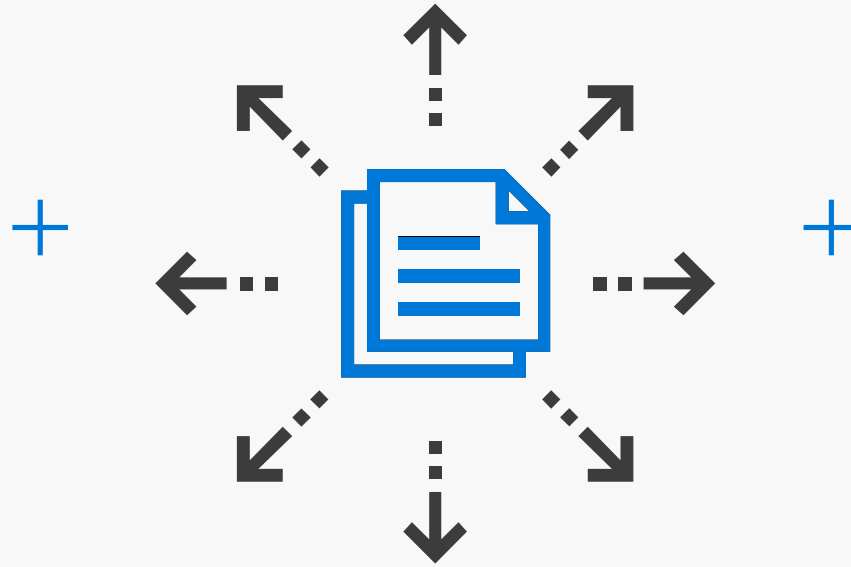
Protect through the entire lifecycle

- Protect user credentials with risk-based conditional access
- Safeguard data with built-in encryption technologies
- Rapidly respond to intrusions with built-in controls to detect and respond to data breaches

Leverage guidance from experts



Learn from our
experience

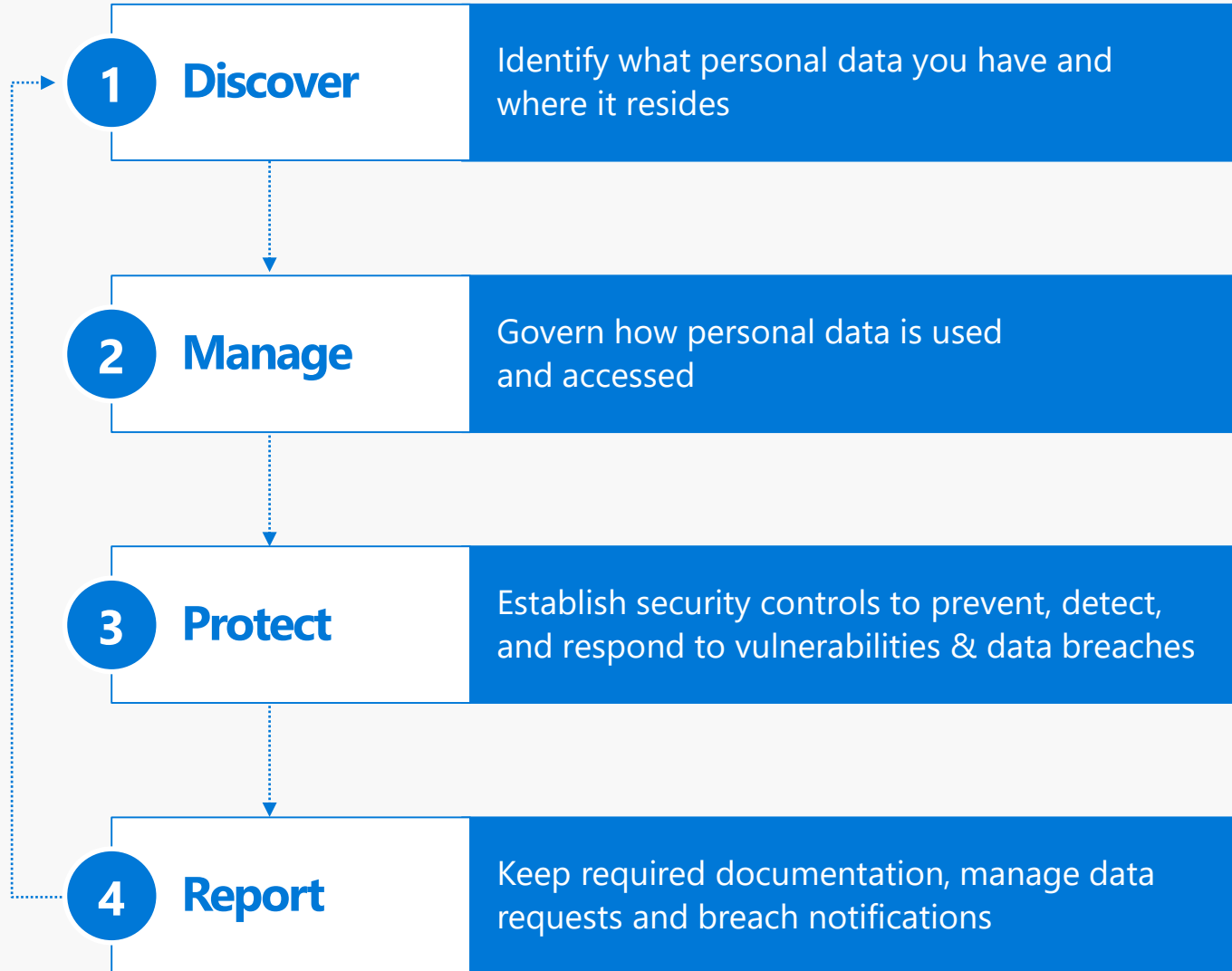


Leverage our GDPR
preparation resources



Engage our global
partner ecosystem

How do I get started?





1 Discover:

Identify what personal data you have and where it resides

In-scope:

Any data that helps you identify a person

- Name
- Email address
- Social media posts
- Physical, physiological, or genetic information
- Medical information
- Location
- Bank details
- IP address
- Cookies
- Cultural identity

Inventory:

Identifying where personal data is collected and stored

- Emails
- Documents
- Databases
- Removable media
- Metadata
- Log files
- Backups

Example solutions

Microsoft Azure

Microsoft Azure Data Catalog

Enterprise Mobility + Security (EMS)

Microsoft Cloud App Security

Dynamics 365

Audit Data & User Activity
Reporting & Analytics

Office & Office 365

Data Loss Prevention
Advanced Data Governance
Office 365 eDiscovery

SQL Server and Azure SQL Database

SQL Query Language

Windows & Windows Server

Windows Search

2 Manage:

Govern how personal data is used and accessed within your organization

Data governance:

Defining policies, roles and responsibilities for the management and use of personal data

- At rest
- In process
- In transit
- Storing
- Recovery
- Archiving
- Retaining
- Disposal

Data classification:

Organizing and labeling data to ensure proper handling

- Types
- Sensitivity
- Context / use
- Ownership
- Custodians
- Administrators
- Users

Example solutions

Microsoft Azure

Azure Active Directory
Azure Information Protection
Azure Role-Based Access Control (RBAC)

Enterprise Mobility + Security (EMS)

Azure Information Protection

Dynamics 365

Security Concepts

Office & Office 365

Advanced Data Governance
Journaling (Exchange Online)

Windows & Windows Server

Microsoft Data Classification Toolkit

3 Protect:

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

Preventing data attacks:

Protecting your data

- Physical datacenter protection
- Network security
- Storage security
- Compute security
- Identity management
- Access control
- Encryption
- Risk mitigation

Detecting & responding to breaches:

Monitoring for and detecting system intrusions

- System monitoring
- Breach identification
- Calculating impact
- Planned response
- Disaster recovery
- Notifying DPA & customers

Example solutions

Microsoft Azure

Azure Key Vault
Azure Security Center
Azure Storage Services Encryption

Enterprise Mobility + Security (EMS)

Azure Active Directory Premium
Microsoft Intune

Office & Office 365

Advanced Threat Protection
Threat Intelligence

SQL Server and Azure SQL Database

Transparent data encryption
Always Encrypted

Windows & Windows Server

Windows Defender Advanced Threat Protection
Windows Hello
Device Guard

4 Report:

Keep required documentation, manage data requests and breach notifications

Record-keeping:

Enterprises will need to record the:

- Purposes of processing
- Classifications of personal data
- Third-parties with access to the data
- Organizational and technical security measures
- Data retention times

Reporting tools:

Implement reporting capabilities

- Cloud services (processor) documentation
- Audit logs
- Breach notifications
- Handling Data Subject Requests
- Governance reporting
- Compliance reviews

Example solutions

Microsoft Trust Center
Service Trust Portal

Microsoft Azure
Azure Auditing & Logging
Azure Data Lake
Azure Monitor

Enterprise Mobility + Security (EMS)
Azure Information Protection

Dynamics 365
Reporting & Analytics

Office & Office 365
Service Assurance
Office 365 Audit Logs
Customer Lockbox

Windows & Windows Server
Windows Defender Advanced Threat Protection

Resources

[Microsoft.com/GDPR](https://microsoft.com/GDPR)

- [GDPR Assessment Tool](#)
- [Guidance](#)
- [Whitepapers](#)
- [GDPR F.A.Q.](#)
- [Solutions](#)







risual

Alun Rogers

Co-founder and Director of risual Ltd



What we do



Consulting

plan | implement



Services

monitor | optimise



Skills

develop | adopt



Solutions

sector | software

Values: Honesty, Openness and Trust. These core values are embedded in everything we do from delivering new and exciting technology solutions to the work we undertake within the community on a monthly basis.

Visual Consulting Services

PRINCE2[®] PRACTITIONER

APMG International[™] AgilePM

ISO/IEC 27001 ISO 20000

CYBER ESSENTIALS PLUS

ITIL[®]

Standards and Accreditations

SC Cleared

INVESTORS IN PEOPLE

Microsoft CERTIFIED

DBS CHECKED (formerly CRB) Disclosure and Barring Service

IBA[®] International Institute of Business Analysis

TOGAF[™]

MSP[®]

Technical Expertise

Dedicated Specialist Technical Teams

Microsoft Specialists

Award Winning

MVP Connected

Certified Subject Matter Experts

ISO Accredited structured methodology

Business aligned Architects

Proven Strategic Approach

Flexible and scalable Delivery

Advisory and Management services

Enterprise Portfolio Management

Enterprise Architecture

Business Transformation Services

Enterprise Change Management

Industry Insight

Agile and Waterfall Delivery

Business Analytics

Digital Strategy And Management Consultancy

Digital Transformation

Inspire and Retain Staff

Reduce Digital Skills Gap

Create New Revenue Streams

Reimagine Business Processes

Offer New Services

Integrated IT and Business Strategy

Optimised Service Vision

Hybrid, Public or Private Cloud

Out-of-hours Migrations

Proven Security Strategy

Azure IaaS Expertise

Azure Adoption Roadmap

Identity and Access Consultancy

Azure Application Analysis

GDPR Consultancy

DevOps aligned Cloud migration

End User Computing

Work From Anywhere

Office 365 Consultancy

Windows 10 Expertise

BYOD/CYOD

End User Training

Product Sales Specialists

Automation and Workflows

Dedicated Skype Consultants

Intranet Deployments

Connected Business

Machine Learning

Custom App Development

Hadoop and R expertise

Systems Integration

Dynamics 365 Consultancy

Power BI Specialists

Data & Analytics Services

IOT Expertise

Create Value From Legacy Data

User Adoption

End User Training

Floorwalking & On Site Support

Managed Delivery

Continuous Feedback

On Demand Courses

Adoption Reporting

Training Videos

Learning-as-a-Service

Microsoft Technology

Office 365

Azure

Dynamics 365

Business Expertise

ITSM Consultancy

GDPR Consultancy

ISO/IEC Standards Gap Analysis

End User Training

'One Visual' Approach

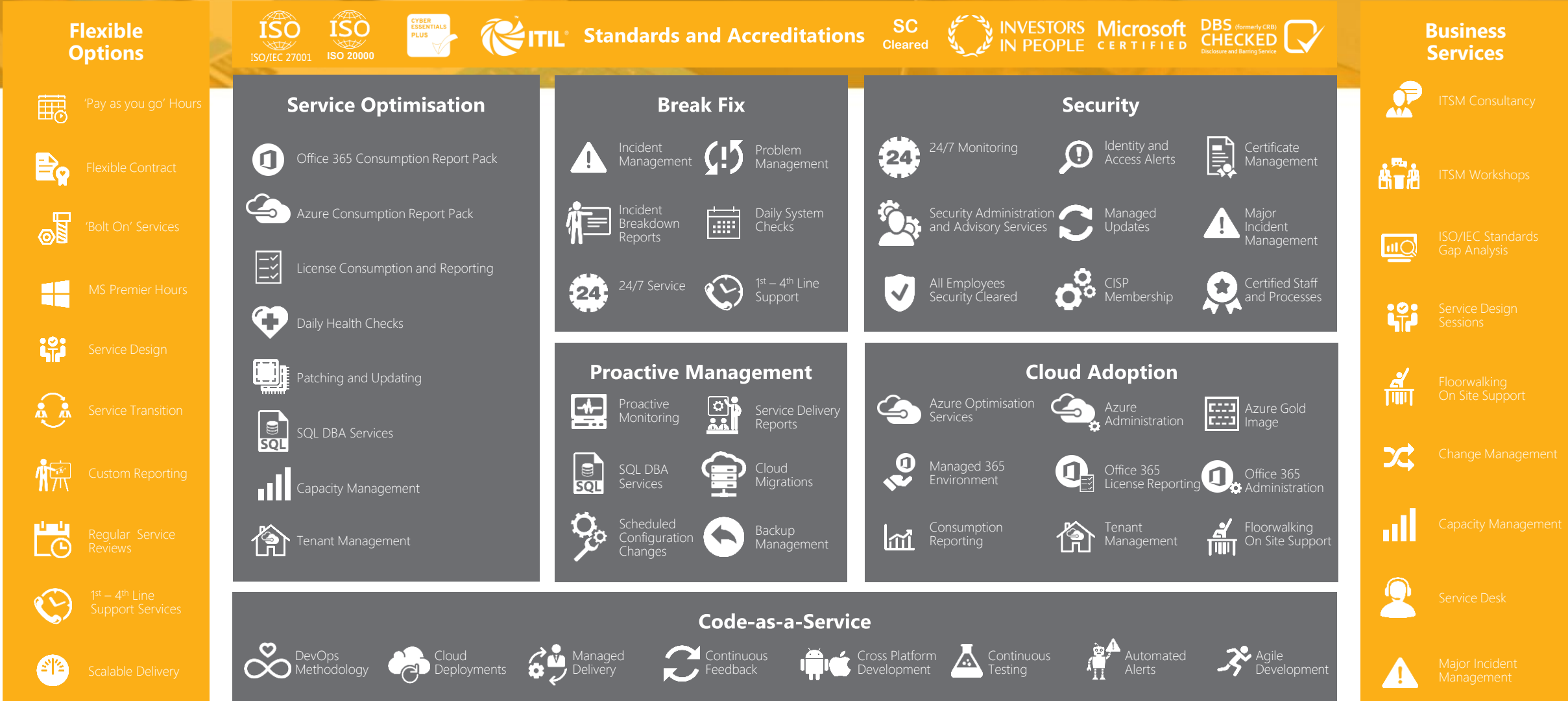
Cloud First Agenda Aligned

Adoption Management

Application Development

Integrated Managed Services

Visual Managed Services (rMS)





Standards and Accreditations



INVESTORS
IN PEOPLE

Microsoft
CERTIFIED

DBS (formerly CRB)
CHECKED
Disclosure and Barring Service



Bespoke Packages



On Demand Technical Training



Apprenticeships



Delivery Partners



Project Integration



End User Adoption and Training



Flexible Learning

Multiple Learning Options



Microsoft Aligned



Visual Solutions



Standards and Accreditations



Sector Specific



Tailored Offerings



Long Term Partnerships



Microsoft Influence



Software and Consultancy



Driving Transformation

Software Development



DevOps Methodology



Cloud Deployments



Managed Delivery



Cross Platform Development



Continuous Testing



Agile Development

Industry Development



Dedicated Industry Business Manager



Customised Offerings to Meet Industry Challenges



Award Winning Work in Government



Reference Customers



Multiple Awards in Emergency Services



Working Collaboratively With Sectors



SOCITIM Alignment



Building Long Term Relationships

Industry Solutions



Led By Industry Experts



Award Winning Development Team



Out-the-Box Digital Disruption



Managed Delivery



Continuous Patching and Updating



Bespoke Development Available



Born in Cloud Solutions



Tenant Management

Minerva 365



Business Process Applications



Office 365 Add Ons



Room Booking



Facilities Management



Geo-Location Tagging



Mobile Case Management



Customisable To You



Cross Platform

Akin



Easy To Deploy



Monitor Sales Activity



Automate Marketing



Auditable Messaging With Customer



Profiling and Preferences



Reskin For Your Brand



Cross Platform



Analytics Built In

Nimos



Safeguarding Services



Mobile First Solutions



Dynamics Case Management



NHS Guardian Management



Cross-Platform



UK In-House Support



Training Provided



Growing Portfolio of Services

Key Sectors



Local and Central Government



Emergency Services



Professional Services



Retail & Hospitality



Health

Flexible Options



Scalable Delivery



Regular Service Reviews



1st - 4th Line Support Services



Custom Reporting



'Bolt On' Services



risual's approach to GDPR

Abby Williams
Business Analyst

GDPR Compliance

- You will always be working towards compliance
- Looking for companies to be working towards compliancy
- Continuous action plan
- Data Protection Officer and Working Group
- Replacing Data Protection Act to keep up with the digitalised world
- Review continuously

Differences from the Data Protection Act

Difference	DPA	GDPR
Maximum penalty	£500,000	4% of annual global revenue or €20 million (whichever is greater)
Responsibility	Data Controllers only	Data Controllers and Processors
Breach notifications	Not mandatory for most org.	Mandatory within 72 hours
Parental consent	No	Required
Accountability – owner of process or data	Limited	Explicit
Subject access requests	£10 fee chargeable, respond within 40 days	Free of charge, respond within 30 days
Data consent	Freely given, specific and informed	Clear, affirmative action with the ability to be withdrawn at a later date.

Common pain points

- Telemarketing Process – record, tell customer the call is being recorded, consent to stay in touch
- Consent in general – Opt in instead of Opt Out
- Cleansing and retaining data
- Discovery of data for subject requests
- Regularity of contact – 6 months new customers, 18 months current customers
- Training – DPO and across board in the company
- Managing it continuously and improving

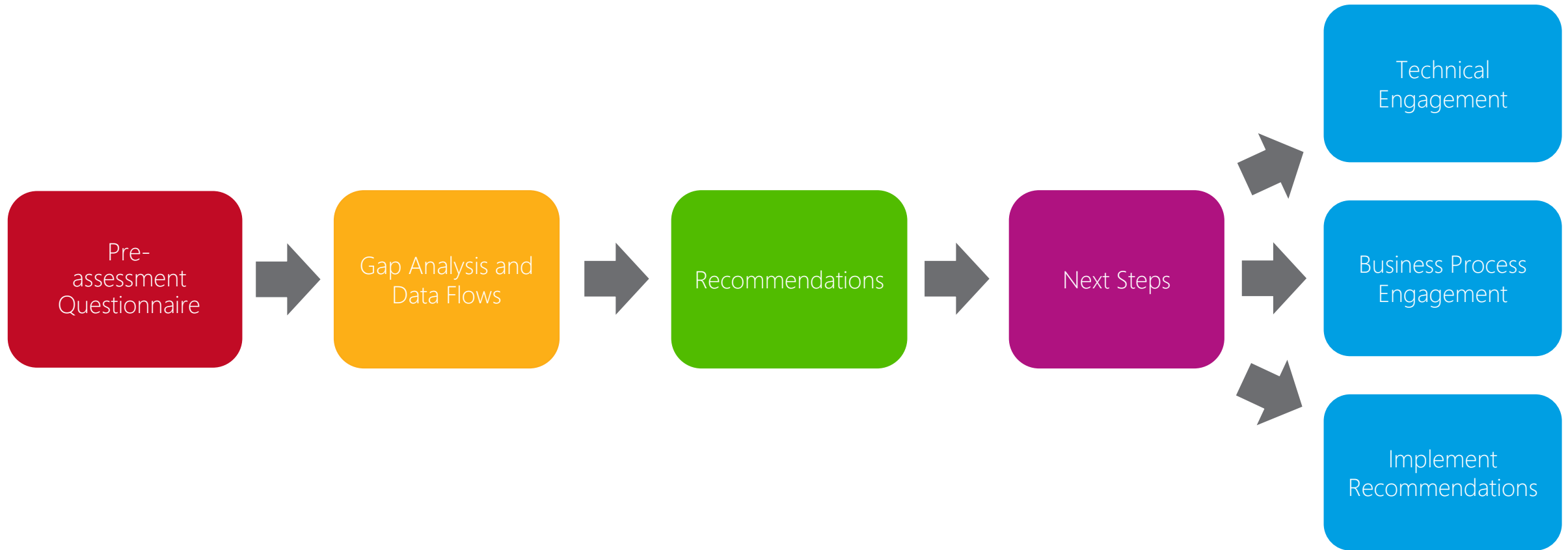
Privacy

- Part of taking a privacy by design approach:
 - promote privacy and data protection compliance from the start
 - Minimises risks and builds trust
 - Increases awareness of privacy and data protection across board
 - Less likely to breach the DPA
- Identify and reduce the privacy risks of projects
- Reduce the risk of harm to individuals through misuse of personal information
- Not a legal requirement but demonstrates to the ICO that you are complying to the DPA when data processing
- Privacy by Design
- Privacy Impact Assessments

Breaches and requests of information

- Breaches must be reported to ICO within 72 hours of finding them
- 1 month to reply to information requests (rather than 40 days)
 - Refuse or charge for requests if excessive
 - subject must be told and they have the right to complain to the supervisory authority
 - At the latest within 1 month of the request
- This could use the right to be forgotten
 - Processing technology must be in place to delete data in response to a request

Visual General Data Protection Regulation Process



GDPR Analysis

- Microsoft based questionnaire to gauge maturity
- Department Interviews
- Information flows – Visio
- Gap analysis
- Recommendations (Technology and Business)
- Action plan (risks and prioritisation)

GDPR and Technology

Stefanie Jacobs

Stefanie.Jacobs@Microsoft.com



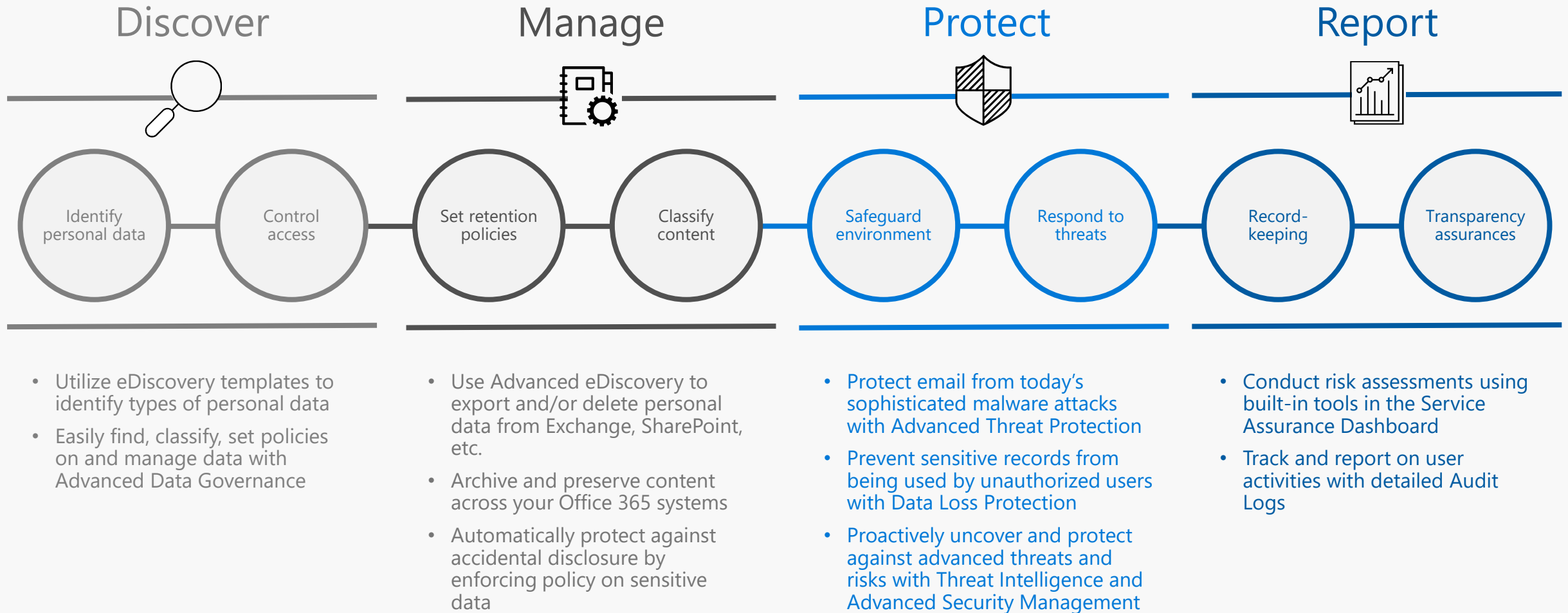
With the GDPR, it is critical to recognize that compliance is a shared responsibility



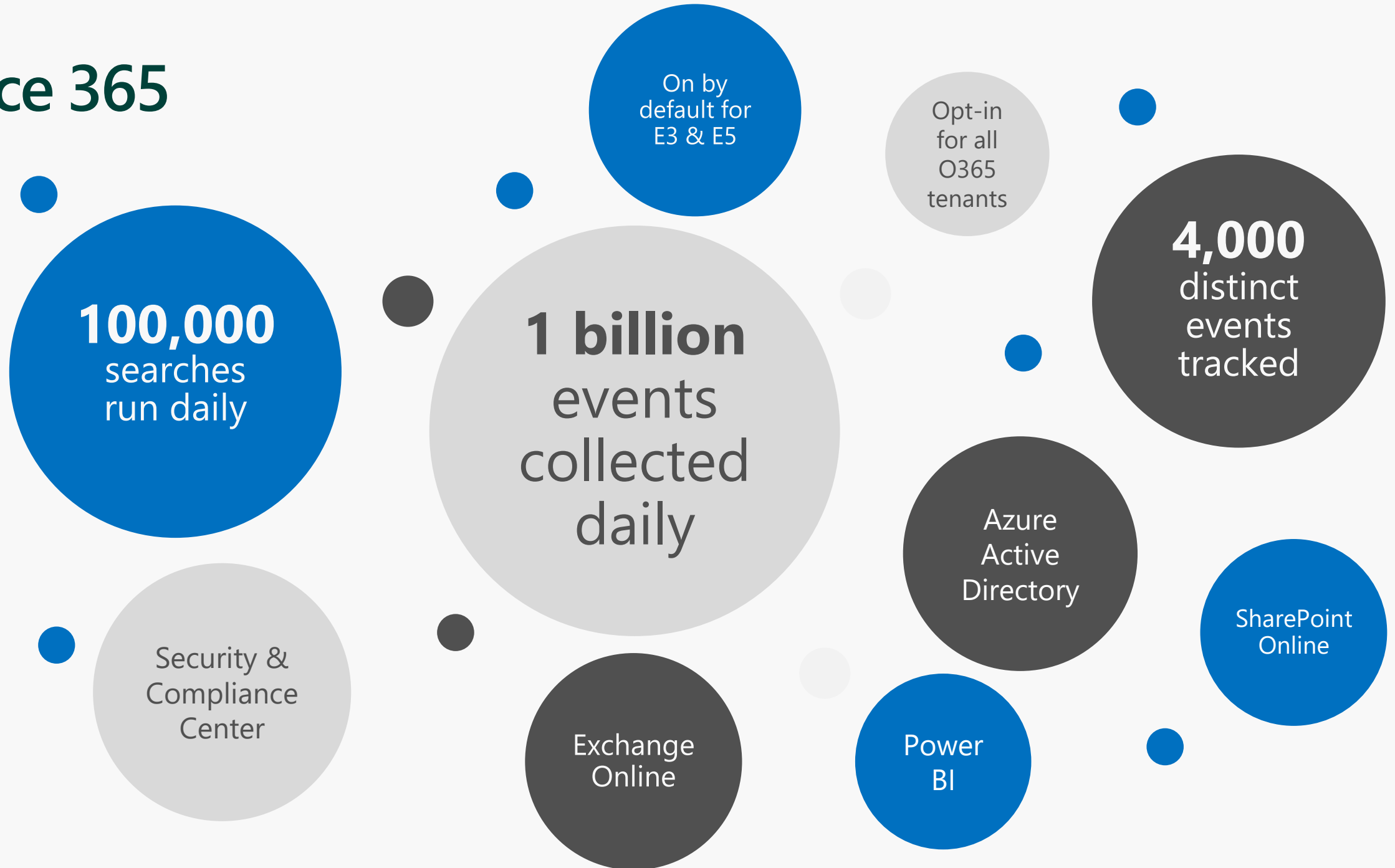
Top GDPR considerations



How does Office 365 help today?



Office 365



// Our mission is to empower every person and every organization on the planet to achieve more.



Satya Nadella





Break for Lunch