Microsoft

Prepare for GDPR today with Microsoft 365

Table of Contents

01. Executive Summary

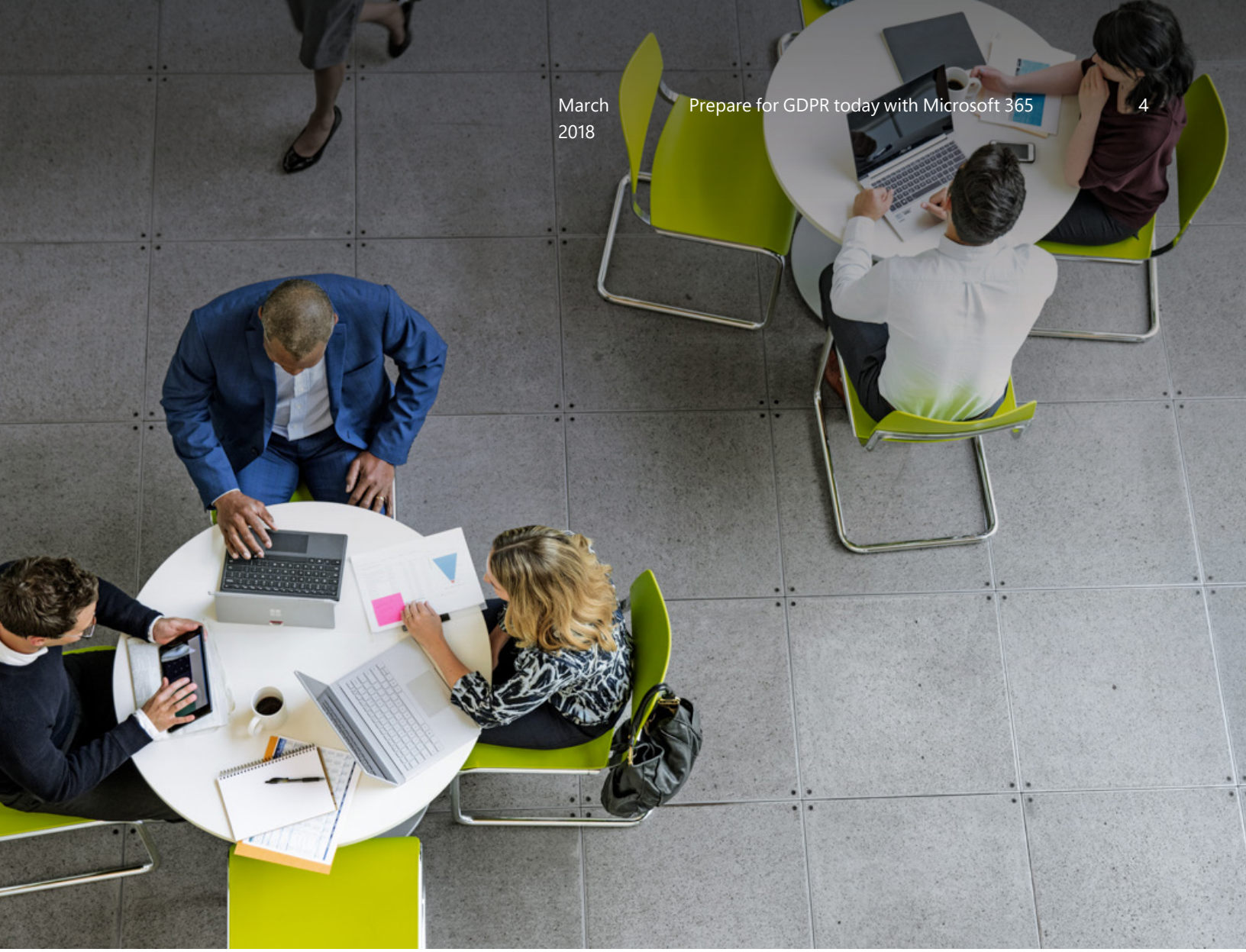
We live in a time where digital technology is profoundly impacting our lives, from the way we connect with each other to how we interpret our world. As the private sector continues to push the boundaries of innovation, policy makers work to ensure that the appropriate personal data oversight and safeguards are in place through compliance standards such as the European Union's General Data Protection Regulation (GDPR).

To thrive in this privacy-focused era, you need a trusted partner who can help you not only overcome the challenges, but make the most of the opportunities that lie ahead. The Microsoft Cloud is uniquely positioned to help you meet your GDPR compliance obligations. Microsoft 365 brings together Office 365, Windows 10 and Enterprise Mobility + Security – offering a rich set of integrated solutions that leverage AI to help you assess and manage your compliance risk, protect your most important data and streamline your processes.

Because achieving organisational compliance can be very challenging, understanding your compliance risk should be your first priority. Compliance Manager is a cross–Microsoft Cloud services solution designed to help organisations meet complex compliance obligations like the GDPR.

Beyond understanding your compliance risk, protecting personal data and other sensitive content is key. With the information protection capabilities within Microsoft 365 we provide an integrated classification, labelling and protection experience, enabling persistent protection of your data wherever it is – across devices, apps, cloud services and on-premises.

No matter where you are in your GDPR efforts, the Microsoft Cloud and our intelligent compliance solutions in Microsoft 365 can help you on your journey to GDPR compliance.



02. Landscape

We live in a time where digital technology is profoundly impacting our lives, from the way we connect with each other to how we interpret our world. Central to this digital transformation is the ability to store and analyse massive amounts of data to generate deeper insights and more personal customer experiences.

The GDPR is a comprehensive and complex regulation designed to protect the personal data of EU residents.

As the private sector continues to push the boundaries of innovation, policy makers work to ensure that the appropriate personal data oversight and safeguards are in place through compliance standards such as the European Union's Global Data Protection Regulation (GDPR).

The GDPR is a comprehensive and complex regulation designed to protect the personal data of EU residents. The requirements address internal policies, processes, people and technology. They range from designating a data protection officer for larger organisations, to when notifications of personal data breaches must be provided to data protection authorities and affected individuals. Organisations across the world are focused on compliance, because while the GDPR applies to organisations established in the EU, it also applies to organisations – wherever they are located – who offer goods or service in the EU or monitor the behaviour of residents in the EU.

To thrive in this privacy-focused era, you need a trusted partner who can help you not only overcome the challenges, but make the most of the opportunities that lie ahead. At Microsoft, our mission is to empower every person and every organisation on the planet to achieve more. And trust is always at the core of everything we do. Microsoft works closely with local governments and policy makers to help shape the regulations that impact technology because we understand that compliance policies can actually help accelerate innovation and digital transformation. Adhering to a common set of compliance standards is one way to mitigate the kind of high profile data losses that erode customer confidence across the industry and ultimately helps us maintain

greater long-term trust with the customers and partners who choose the Microsoft cloud to help them achieve more in both their personal and professional lives.

Our research suggests that companies not only see the long-term value of building trust by protecting customer data, but in fact believe their investments in compliance will positively impact other areas of their business – like productivity and collaboration. When IT decision makers in Europe and the U.S. were asked to identify their top concern in achieving GDPR compliance, "protecting customer data" was the #1 response while avoiding fines ranked #8. More than half of respondents said the GDPR brings added benefits like collaboration, productivity and security. Cloud solutions like Microsoft 365 are a big reason that businesses see opportunity in compliance. Of those surveyed, 41% said they are likely to move more of their company's infrastructure to the cloud to become compliant. And among leading cloud vendors, Microsoft was identified as most trusted by a wide margin (28%), followed by IBM (16%), Google (11%) and Amazon (10%). All told, 92% of IT decision makers in companies that store data primarily in the cloud identified as being confident in their GDPR readiness, compared with just 65% of those who prefer to store data on-premises.

Your journey to GDPR compliance includes identifying what personal data you have and where it resides, governing how it is used and accessed, establishing adequate security controls and preparing to respond to requests from individuals whose personal data you have. This may sound like a lot of work, but Microsoft is here to help. We've taken a principled approach to building privacy, security, compliance and transparency into everything we do, which means that they are integrated into the products and services you use every day.

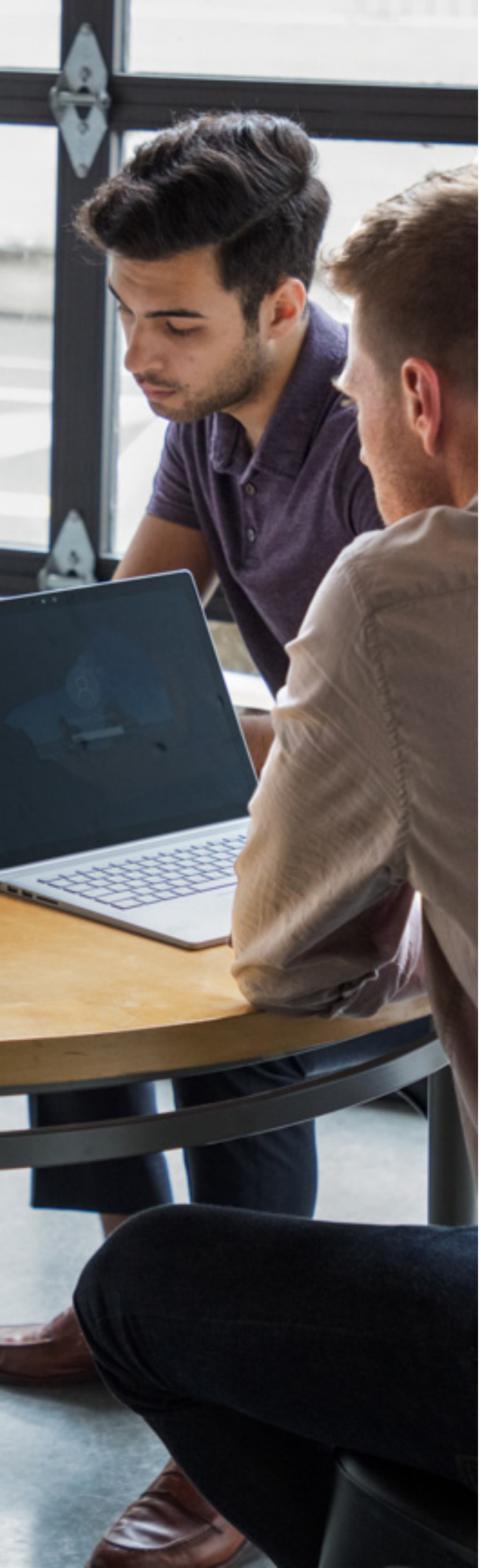
The Microsoft Cloud is uniquely positioned to help you meet your GDPR compliance obligations, with the largest certified compliance portfolio, services architected to be secure by design and the most extensive global datacentre footprint in the industry. Our cloud solution is built for power, scale and flexibility. Microsoft 365 brings together Office 365, Windows 10 and Enterprise Mobility + Security – offering a rich set of integrated solutions that leverage AI to help you assess and manage your compliance risk, protect your most important data and streamline your processes.

With the GDPR being enforceable beginning 25th May, 2018, there are a number of steps you can take today with Microsoft 365 to help you prepare.

03.

Assess and manage your compliance risk

Because achieving organisational compliance can be very challenging, understanding your compliance risk should be your first priority. Compliance Manager is a cross–Microsoft Cloud services solution designed to help organisations meet complex compliance obligations like the GDPR.



It helps the person who oversees the data protection strategy for your organisation (sometimes called a data protection officer) to manage the compliance and risk assessment process.

Compliance Manager helps you perform an on-going risk assessment that reflects your compliance posture against data protection regulations when using Microsoft Cloud services, such as Office 365, Azure and Dynamics 365. As achieving GDPR compliance is a shared responsibility between data processors and data controllers, you can see from the Compliance Manager dashboard that 60% of the controls are managed by Microsoft, and the tool provides you detailed information about how Microsoft implemented and tested those controls. For the remaining 40% of the controls managed by you, Compliance Manager enables you to conduct self-assessment so that you can monitor your compliance stature continuously. In each assessment tile, a Compliance Score reflects your overall compliance performance based on a risk weight assigned to each control. The score helps you to estimate where your organisation stands in terms of achieving compliance and enables you to make better decisions about prioritising tasks. However, the score does not express an absolute measure of how compliant you are, so it should not be interpreted as a guarantee.

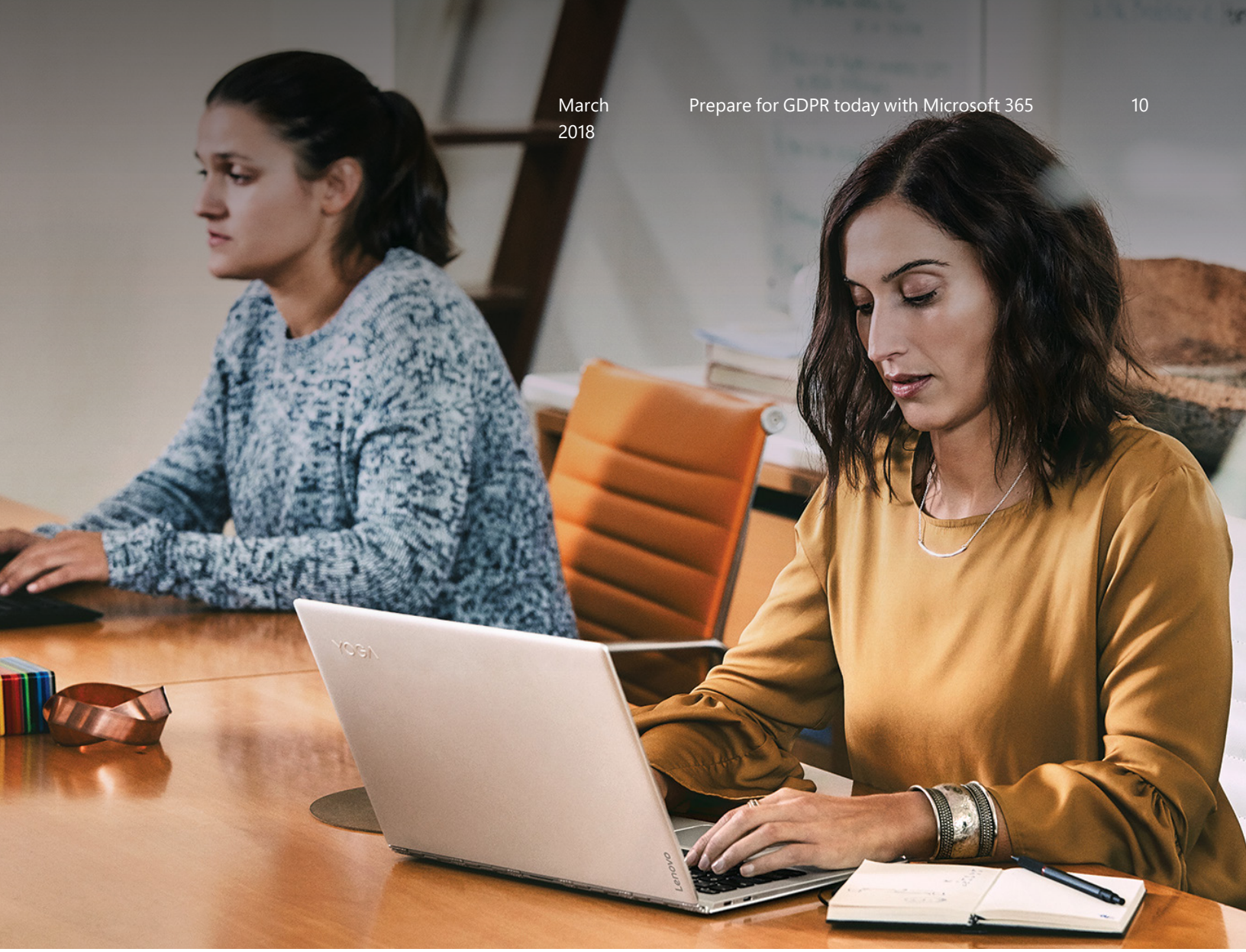
We know that the compliance process can be very disjointed. Compliance personnel are the experts of industrial regulations and standards, while IT professionals are the experts of technology solutions.

It's challenging to find talent with expertise in both areas to help define, implement and assess controls. Therefore, we provide recommended customer actions in each customer-managed control to help you connect the technology solutions with the GDPR regulatory requirements. You can follow the step-by-step guidance to improve your data protection capabilities and design your own business process for internal self-assessments.

To simplify your compliance process, Compliance Manager provides a control management tool to help you assign, track and record your compliance-related activities, and audit-ready reporting to help you be more prepared for internal or external audits. Authorised users in your organisation can upload documents, such as screenshots of configuration, business process documents, internal training materials and more, as evidence for your compliance activities. You can view the links to evidence that your organisation collected in the audit-ready reports.

Compliance Manager is available for all Office 365 Business and Enterprise subscribers in public cloud. GCC customers can access Compliance Manager, however users should evaluate whether to use the document upload feature of compliance manager, as the storage for document upload is compliant with Office 365 Tier C only.

Read the Compliance Manager white paper to learn more about the product.



04.

Protect your most sensitive data

Beyond understanding your compliance risk, protecting personal data and other sensitive content is key. At its core, GDPR is about protecting the personal data of individuals – making sure there is proper security, governance and management of such data. To help ensure that you're effectively protecting not only

personal data, but also other sensitive content that's relevant to your compliance goals, you should implement solutions and processes that enable you to identify, classify, protect and monitor the data that is most important to you – no matter where it lives or travels.

Identification and classification

With the information protection capabilities within Microsoft 365 we provide an integrated classification, labelling and protection experience, enabling persistent protection of your data wherever it is – across devices, apps, cloud services and on-premises.

Azure Information Protection scanner, which is now generally available, addresses hybrid and on-premises scenarios by allowing you to configure policies to automatically discover, classify, label and protect documents in your on-premises repositories such as the File Servers and on-premises SharePoint servers. The scanner can be configured to periodically scan on-premises repositories based on company policies. Read "Azure Information Protection scanner in public preview" to learn more about the scanner. You can deploy the scanner in your own environment by following instructions in this technical guide.

The next step is to protect data anywhere and prevent data loss. Today, data travels through many locations – across devices, apps, cloud services and on-premises. It is important to build protection into the file, so this protection persistently stays with the data itself.

As Microsoft's information protection solutions expand and develop, we take great strides in ensuring Cloud App Security integrates these advancements into our existing services.

Data labelling and encryption

Azure Information Protection (AIP) provides persistent data protection by classifying, labelling and protecting sensitive files and emails. Labels are used to define the sensitivity of a document or email, such as "General" or "Confidential". Additionally, AIP allows for encryption and authorisation, ensuring users must successfully authenticate to access the material.

Microsoft Cloud App Security (MCAS) can read files labelled by AIP and set policies based on the file labels. Furthermore, the service will scan and classify sensitive files in cloud apps and automatically apply AIP labels for protection – including encryption. Read the "Automatically apply labels to sensitive files in cloud apps" blog and technical documentation to learn more about this feature.

Our goal is to provide you with comprehensive protection of your sensitive data across a wide variety of platforms and applications. We also ensure users get the same seamless experience in protecting their data without compromising their productivity. In that regard, we now support native labelling and protection of sensitive data on your Mac devices. This will enable Mac users to easily classify, label and protect Word, PowerPoint and Excel documents. Considering that a significant amount of sensitive information is in PDF format, we've also integrated with Adobe to help you natively read labelled and protected PDF documents in Adobe Reader on Windows. As we deepen the integration of AIP with Adobe, we'll soon also enable native labelling and protection of PDFs using Adobe Acrobat Pro on Windows.

Windows 10 Enterprise protection features

Ensuring your devices are protected is another key aspect of information protection. Windows 10 Enterprise provides Identity and Information Protection capabilities that will help you comply with GDPR requirements by implementing security measures to protect personal data.

Identity protection capabilities delivered by Windows Hello for Business and Windows Hello companion devices further enhances

your ability to leverage biometrics and multifactor authentication to protect personal and sensitive data. Windows Defender Credential Guard significantly improves security against credential theft by implementing an architectural change in Windows designed to help eliminate hardware-based isolation attacks rather than simply trying to defend against them. Information protection capabilities in Windows 10 Enterprise including device protection using BitLocker, data separation between personal and business data and data loss prevention using Windows Information Protection, which is tightly coupled with Microsoft 365 cloud services such as Office 365 and Azure Information Protection.

To review more about how Windows 10 Enterprise can assist with meeting GDPR requirements, please visit this article.

Office 365 and AIP labelling schemas

In the spirit of working towards providing a more consistent classification, labelling and protection model that will be used across our information protection technologies, we are previewing a shared labelling schema that will be used across Office 365 and Azure Information Protection. This means that the same default labels will be used across both Office 365 and Azure Information Protection, and labels you create in either of these services will automatically be synchronised in the other service – eliminating the need to create labels in two different places. The consistent labelling model also helps ensure that sensitivity labels – regardless of where they were created – are recognised and understood across Azure Information Protection, Office 365 Advanced Data Governance, Office 365 DLP and Microsoft Cloud App Security. For example, if you create a label in the Office 365 Security & Compliance Centre for "Confidential – Personal Data", this label will also appear in the Azure Information Protection admin portal. This is a big step forward in helping provide a consistent and predictable approach to data labelling.

The shared labelling schema will also make it easier for end-users to apply the appropriate sensitivity label and protection while working on documents or sending emails. We are building labelling capabilities natively into the core Office apps – including Word, PowerPoint, Excel and Outlook – no need to download or install any additional plug-ins. For example, if an end-user is working on a document that contains personal data, such as an employee ID number, the worker can easily select the

appropriate label, such as "Confidential", right within the app. To start, we are previewing the native labelling experience for Office apps on Mac and Outlook Web App. We plan to extend native labelling capabilities to Office apps running on iOS, Android and Windows in the future.

Common and custom data types

The ability to automatically classify personal data is a critical part of helping you achieve your GDPR goals. Today we have over 85 out-of-the-box sensitive information types that can be used to detect and classify your data. This includes several of the most common personal information data types, such as credit card numbers, national ID numbers and passport numbers. We will continue to add to these built-in sensitive information types and will soon provide a GDPR template to help detect and classify personal data relevant to GDPR. While many of the existing sensitive information types are relevant to the GDPR, the upcoming GDPR template will help consolidate these into a single template, as well as add several new personal data types to detect (such as addresses, telephone numbers, medical information). The new sensitive information template will make it

We plan to extend native labelling capabilities to Office apps running on iOS, Android and Windows in the future.

easier to configure the detection, classification and protection of GDPR related personal data. To learn more about the current sensitive information types, review this article. You can also create and customise your own sensitive information types – because we know that you may have your own unique data types, such as employee ID numbers. Learn more about how to create and customise your own sensitive information types in this article.

Closing

The European Union's General Data Protection Regulation (GDPR) calls for enforcement to commence on 25th May, 2018 and you should not delay evaluating your obligations under the regulation. Trust is central to Microsoft's mission to empower every person and every organisation on the planet to achieve more. So that you can trust the Microsoft products and services you use, such as Microsoft 365, we take a principled approach with strong commitments to privacy, security, compliance and transparency. This approach includes helping you on your journey to meet the requirements of the GDPR. If your organisation collects, hosts or analyses personal data of EU residents, GDPR provisions require that you only use third-party data processors who commit contractually to implement the technical and organisational requirements of the GDPR. Microsoft 365 provides a highly secure, complete and intelligence solution for digital work. By bringing together the best of Office 365, Windows 10 and Enterprise Mobility + Security, we can help accelerate your journey to compliance with the GDPR by:

- Assessing compliance risk
- Protecting personal and sensitive data
- Streamlining processes

In addition to understanding the capabilities provided to you in Microsoft 365, we recently released a new GDPR benchmark assessment to further round out our GDPR resources already available on the Microsoft Trust Centre.

This white paper is a commentary on the European Union's General Data Protection Regulation (GDPR), as Microsoft interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled.

As a result, this white paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organisation. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organisation, and how best to ensure compliance.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is." Information and views expressed in this white paper, including URL and other Internet website references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this white paper for your internal, reference purposes only.