Novalytics Limited

Govern or Grind: Balancing Usability and Security in Microsoft's Compliance Ecosystem

Novalytics Gibraltar

Abstract—Organisations increasingly rely on cloud services like Microsoft Azure and Office 365 to enable seamless data sharing and collaboration. However, they must simultaneously enforce strict information governance and Data Loss Prevention (DLP) measures to protect sensitive information and comply with regulations such as the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018. This report examines the tension between usability and security in this context. We analyse how Microsoft's suite of tools—including Microsoft Purview (encompassing compliance and governance solutions), Microsoft 365 DLP policies, Information Protection labelling, and Azure Active Directory Conditional Access—facilitate data governance and regulatory compliance. We highlight the trade-offs these measures introduce, noting how they enhance security and compliance at the potential cost of user convenience. Using peer-reviewed research and official Microsoft documentation, we discuss strategies to balance user productivity with robust security, ensuring that data governance is effective without unduly hindering organisational workflows.

Keywords—*Data Loss Prevention (DLP); Information Governance; Microsoft Purview; Microsoft 365 Compliance; Azure Conditional Access; GDPR Compliance; UK Data Protection; Sensitivity Labelling; Data Classification; Cloud Security; Usability versus Security Trade-off; Enterprise Collaboration; Subject Access Request (SAR); Data Protection Impact Assessment (DPIA)*

1. Introduction

Modern enterprises thrive on the ability to share and use data between distributed teams and with external partners. Cloud-based productivity platforms such as Microsoft Office 365 (now part of Microsoft 365) and Azure cloud services have become fundamental to enabling collaboration and data accessibility. With this increased ease of data sharing, organisations face increasing risks to data security and privacy. Information governance frameworks and Data Loss Prevention (DLP) strategies are implemented to ensure that sensitive data is handled in compliance with laws and protected against leakage.

A fundamental challenge lies in balancing security controls with usability. Overly restrictive policies can frustrate users, impede workflows, or drive employees to seek ungoverned workarounds, whereas lax controls may lead to data breaches or regulatory violations. This tension between usability and security has been recognised in both industry and academic discourse. Users tend to prioritise accomplishing their tasks efficiently, often perceiving security mechanisms as obstacles when those mechanisms are intrusive or slow down their work. A recent survey of employees at multiple companies found that security controls such as strict access restrictions and DLP measures were viewed as "intrusive" and "blocking" to get work done [2]. On the other hand, regulators and data protection officers demand rigorous safeguards, guided by the principle that security should be 'privacy by design and default', as mandated by GDPR. The situation is further complicated by the fact that modern data environments are sprawling and heterogeneous, spanning on-premise systems and multiple cloud services. Governance solutions must therefore be comprehensive and user-friendly.

This report provides a technical examination of data sharing, information governance, and DLP within Microsoft Azure and Office 365 infrastructures. We focus on Microsoft's tool set (under the Microsoft Purview umbrella, among others) and how these tools enforce data governance policies or, in some cases, hinder user experience. We discuss key capabilities such as data classification, sensitivity labelling, encryption, DLP policy enforcement, and access control, highlighting how each contributes to security and compliance goals. We also address how these measures align with legal requirements in the EU and the UK, notably GDPR and the UK Data Protection Act 2018, which impose obligations such as protecting personal data, respecting data subjects' rights, and ensuring accountability. Throughout, we identify trade-offs and best practices to strike an optimal balance between keeping data secure and allowing the business to operate effectively.

2. Microsoft Purview and Unified Data Governance

Microsoft Purview is a comprehensive suite of data governance, protection, and compliance solutions aimed at helping organisations manage their data estate centrally. Reflects Microsoft's unified approach to information governance in both Azure and Microsoft 365. At its core, Microsoft Purview provides a "single central pane of glass" for data governance throughout the entire data landscape of an organisation, which increasingly spans on-premise databases, cloud services, file shares, and Office 365 content [3]. According to an industry paper by the Purview engineering team, the service consists of three primary components: (1) a data map (metadata catalogue) populated by automated scanning of data sources, (2) a system to store and manage data sensitivity classifications, and (3) a policy management system that allows administrators to define and enforce data policies uniformly across the organisation [3]. In essence, Purview is designed to break down the silos of disparate data systems, so that a governance policy (for example, "mark all customer data as confidential and restrict its access") can be authored once and applied everywhere in a consistent manner.

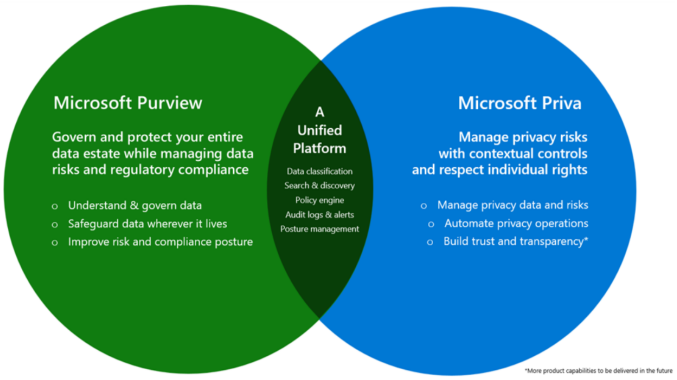

Figure 1. Purview and Priva Ecosystem

A key part of Purview's offering is *data discovery and classification*. Through automated scanning and built-in pattern recognition (such as identifying credit card numbers, national identification numbers, or other personally identifiable information), Purview's data map builds an inventory of where sensitive information resides. Administrators can define or use predefined *sensitive information types* (regular expressions, keywords, or even trainable classifiers) to have the system intelligently tag data [7]. This automated discovery is crucial for compliance: organisations cannot protect or regulate data if they do not know that it exists. By "discovering" and cataloguing data, Purview enables compliance officers to identify stores of personal data subject to GDPR or customer records subject to industry regulations.

The Purview classification engine integrates with *Microsoft Purview Information Protection* (formerly Microsoft Information Protection, MIP). This integration means that once sensitive content is found, it can be labelled and protected. Sensitivity labels (e.g. Public, Confidential, Highly Confidential) are a form of metadata that travels with documents and emails, indicating their classification and optionally

enforcing encryption or access restrictions. Microsoft's documentation emphasises that Purview's information protection provides the capabilities to "discover, classify and protect sensitive information wherever it lives or travels" [7]. When a file or email is labelled confidential, protection can be applied, such as encryption and rights management (preventing unauthorised viewing, printing, or forwarding). These labels can be applied manually by users (prompting them to consider data sensitivity at creation) or automatically based on content detection rules. Automating label application can significantly reduce the usability burden on employees while maintaining governance: for example, if a document contains what looks like customer personal data, a rule might automatically label it as sensitive and encrypt it, without the user having to take any action.

The ability to centrally write and implement *data governance policies* is another powerful feature of the unified approach of Purview. In a traditional environment, each system (database, SharePoint site, mailbox, etc.) might have its own access rules and governance settings, leading to inconsistency and administrative overhead. The Microsoft Purview policy system allows administrators to craft organisation-wide policies that are then translated and enforced across multiple services. For example, a policy could stipulate that "data classified as Highly Confidential must not be shared outside the company." Purview will ensure that this policy is evaluated whether those data are in an SQL database in Azure or a Word document in SharePoint Online. This cross-platform policy engine is a major step forward in balancing security and usability: it attempts to make security seamless and ubiquitous in the background, so users have a consistent experience (e.g., they simply find that certain actions like external sharing are blocked for certain data, regardless of where the data resides). According to the Purview system description, this unified governance; covering structured and unstructured data, cloud and on-premises, is a distinguishing feature, made possible by deep integration with Office 365 and other services [3].

2.1. Usability Considerations in Unified Governance

While Microsoft Purview greatly assists administrators in achieving compliance and security objectives, it can introduce complexity that affects end users. For example, automatic classification might occasionally mislabel a document, leading to unnecessary restrictions on a file that a user is trying to share. If a false positive marks a benign document as sensitive and encrypts it, the intended recipients might be unable to access it, causing delays and frustration. Administrators must therefore fine-tune sensitive information types and trainable classifiers to balance catching most sensitive data without overclassifying normal business documents. Microsoft provides a "policy simulation" and a tuning period for DLP and auto-labelling rules to mitigate this risk, which is a recommended best practice to maintain usability.

Another challenge is that even when classification is accurate, the enforcement of policies such as 'no external sharing of confidential data' can impede legitimate business needs. An organisation might classify a project document as confidential (perhaps automatically due to certain keywords), but later find a need to share it with an outside consultant. The governance system could block sharing, requiring a security override or reclassification that takes time. Users might perceive governance tools as inflexible in such scenarios. Effective governance, therefore, requires not just technology but also well-considered processes: e.g. clear procedures for users to request exceptions or reclassification when business needs evolve. In terms of tooling, Microsoft's approach to soften this friction includes providing user feedback prompts. For example, if a user attempts an action that violates a policy, Office 365 can display a policy tip explaining the restriction (such as 'This document is labelled confidential and cannot be shared outside of the organisation') rather than simply failing silently. This at least informs the user about the reason and educates them on data handling policies.

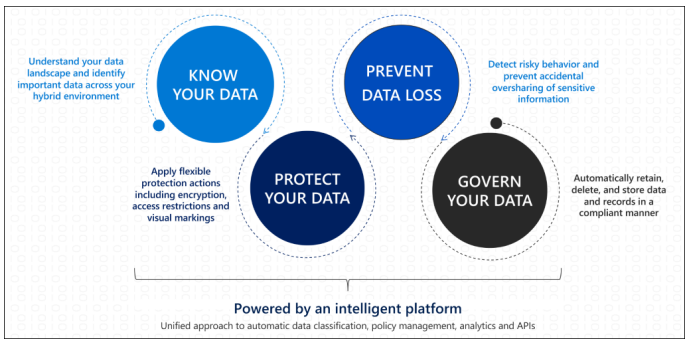

Figure 2. Microsoft Purview Information Protection (formerly Microsoft Information Protection) in the functions of discovering, classifying, and protecting information assets

The centralised Microsoft Purviewew model also means that any outages or misconfigurations can have a wide impact. If the Purview scanning service malfunctions, it could delay the appearance of newly created sensitive data in the catalogue, potentially leaving it unprotected for a window of time. Or, a mistaken policy configuration could inadvertently lock down information broadly. Thus, there is a dependency on the reliability of Purview and the diligence of administrators in testing policies. In summary, Purview significantly improves an organisation's ability to govern data (thereby supporting security and compliance) by unifying policy enforcement across the data estate and automating classification. However, to avoid hindering productivity, its use must be coupled with careful policy design, user engagement and training, and ongoing adjustments to ensure that security measures remain proportionate and context-sensitive.

3. Data Loss Prevention in Microsoft 365

Data Loss Prevention (DLP) in the Microsoft 365 context refers to a set of technologies and policies aimed at preventing sensitive information from leaving the organisation inappropriately. Microsoft 365 DLP is now integrated under the Purview branding as well, which emphasises its role in the broader information protection strategy. DLP policies target the problem of *oversharing*: they are designed to detect when a user is attempting to share or transmit sensitive data (such as personal information, financial records or confidential business data) to unauthorised recipients, and then block the action or alert the user/administrator. Microsoft's documentation defines DLP as a practice to 'prevent users from inappropriately sharing sensitive data with people who shouldn't have it' [8]. In practical terms, a DLP policy is a set of rules that monitor data at various locations (e-mail, files, chat messages, etc.) and look for specific types of content (such as credit card numbers or keywords such as "Privileged") that should be protected.

Before implementing DLP policies, organisations must first understand what data they hold, where they reside, and their sensitivity. This necessitates the creation and maintenance of an Information Asset Register (IAR), a foundational inventory of the organisation's critical information assets. An IAR catalogues data types, ownership, storage locations, and classification levels. It is the prerequisite for any meaningful data protection strategy, including DLP. Without an IAR, DLP policies can be misaligned, targeting irrelevant assets while ignoring critical ones. Therefore, completing the IAR should precede the implementation of DLP, ensuring that protection policies are appropriately scoped and prioritised based on actual data risks.

One of the strengths of Microsoft's DLP solution is its broad coverage throughout the productivity suite and beyond. A single DLP policy can be applied to content in Exchange Online (emails and attachments), SharePoint Online sites, OneDrive for Business folders, Microsoft Teams chats/files, and even local devices (Windows 10/11 endpoints) and certain cloud apps via integration with Defender for Cloud Apps. Using the same types of sensitive information

and classification definitions as Purview's data map, DLP policies can consistently identify sensitive content no matter where it is located. For example, an organisation can establish a DLP rule: "If an email or document contains 10 or more customer National Insurance numbers, prevent it from being shared externally and notify the compliance officer." The DLP engine performs deep content analysis using pattern matching, keyword proximity, and machine learning to detect these conditions [8]. Importantly, it is not just a simple text scan; it uses built-in intelligence (such as Luhn checksum validation for credit card numbers, or context to distinguish a nine-digit number as a Social Security number versus a random number) to improve accuracy [8].

When the conditions of a DLP policy are met, the system can take a variety of *actions*. Common actions include: blocking the content from being shared or sent (for instance, not delivering an outbound email, or stopping a file from being accessed by external users), displaying a warning or policy tip to the end-user, and logging the event for audit. In some cases, DLP can also automatically encrypt the content or quarantine it. These enforcement actions directly contribute to preventing data leakage. From a compliance standpoint, DLP is a technical measure that supports obligations under laws like GDPR Article 32 (security of processing) by mitigating the risk of accidental or unauthorised disclosure of personal data. Indeed, Microsoft provides prebuilt DLP policy templates for common regulations (e.g., GDPR, HIPAA, PCI-DSS) to help organisations quickly implement relevant rules.

However, the flip side is that DLP can be one of the most visible security controls to end-users, and thus a source of the usability-security friction. Unlike back-end processes (such as quietly encrypting a file in storage), DLP often directly interacts with a user's attempt to do something. For example, if a user tries to email a spreadsheet externally and it contains something that triggers a DLP rule, the email might be blocked, and the user will receive a notification. If this occurs frequently or with false positives, users can become frustrated. In the employee survey mentioned earlier, many respondents reported that these transmission controls (which include DLP and related mechanisms) were obstructive [2]. From an organisation's perspective, there is a delicate balance: they want to prevent truly risky data exfiltration (such as an employee unintentionally emailing a client list to the wrong person or a malicious insider trying to steal data), but they do not want to interfere with everyday communications.

Microsoft's DLP solution attempts to address usability by allowing *policy tuning and user override*. Administrators can configure thresholds and exceptions, for instance, perhaps only trigger the rule if a significant amount of sensitive data is detected, to avoid stopping an email just because of one incidental ID number. They can also enable override: a policy tip might say 'This message contains sensitive info. Are you sure you want to send?', allowing the user to justify or report why it is necessary. The event would still be logged, but the user is not completely blocked if they have a valid business reason. This approach recognises that users sometimes need flexibility, and forcing them to seek cumbersome approval every time can impede productivity. Another strategy is phased deployment: initially running DLP policies in "audit mode" where they do not actually block content, but only log incidents and maybe alert users. This helps calibrate the policies by seeing how often they would trigger and whether those triggers are genuine risks or false alarms.

Moreover, DLP in Microsoft 365 is closely tied to the classification labels discussed earlier. A sensitivity label can itself be used as a condition in a DLP policy. For example, if a document is labelled 'highly confidential', a DLP policy can automatically prevent it from being shared externally, regardless of content. This is a powerful combination of user-driven (or auto-driven) classification and machine-enforced handling. It also helps usability: if users diligently label documents, the DLP engine does not have to rely on guessing from content, which could be error-prone; it will simply respect the intended handling of the label. Of course, that shifts some responsibility to users or auto-labelling algorithms to get the label right in the first place.

In summary, Microsoft 365 DLP provides robust tools to curtail inappropriate data sharing. It significantly improves an organisation's control over data outflows by monitoring a wide range of channels. This undoubtedly strengthens security postures and helps demonstrate compliance (showing regulators that preventative controls are in place). The trade-off is that if DLP policies are too rigid or noisy, they can disrupt workflows. Effective DLP deployment therefore involves stakeholder training (so people understand *why* certain actions are blocked), iterative tuning of rules, and possibly an incident response process to handle cases where business needs conflict with policy (e.g., a manager can quickly grant an exception for a particular case). Crucially, these controls must be based on a solid understanding of the organisation's information assets, as defined in the IAR. By identifying and classifying sensitive data early, organisations lay the groundwork for precise, impactful, and low-friction DLP controls.

4. Access Control and Conditional Access

Beyond data classification and content-based policies, controlling *access* to data is a fundamental aspect of information governance. Microsoft Azure Active Directory (Azure AD, now part of Microsoft Entra ID) provides Conditional Access policies that help organisations ensure that only the right people under the right conditions can access sensitive resources. Conditional access is described as operating on an "if-then" basis: If certain signals or conditions are met (user identity, location, device compliance status, etc.), then allow or deny access, or require additional proof of identity [6]. These policies are a cornerstone of a Zero Trust security model and directly contribute to preventing unauthorised data access or transfer. For example, a Conditional Access policy might require multifactor authentication (MFA) for any user accessing Office 365 from outside the corporate network, or block access entirely if coming from a high-risk sign-in (detected by anomaly detection in Azure AD).

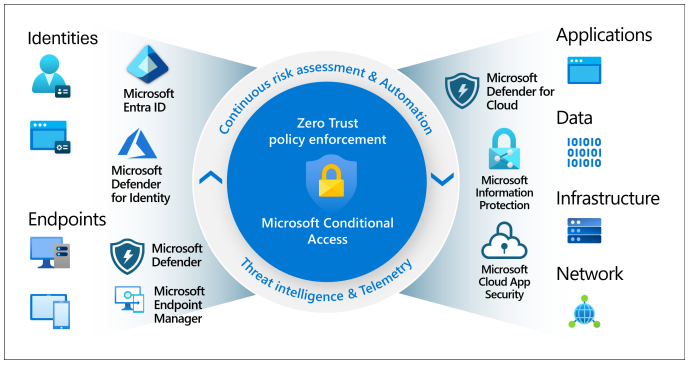

Figure 3. Microsoft's Zero Trust architecture places Conditional Access at the centre of your organisations security policy enforcement. Continuous risk assessment and automation feed into this control layer, integrating with security tools across identities (e.g. Entra ID, Defender for Identity), endpoints (e.g. Microsoft Defender, Endpoint Manager), applications, data (e.g. Microsoft Information Protection), infrastructure, and networks. This model enables dynamic, context-aware access control based on real-time threat intelligence and telemetry.

In the context of data sharing and DLP, Conditional Access adds a layer of *contextual security*. While DLP looks at *what* data being sent and to *whom*, Conditional Access looks at *who* is accessing data and *how*. Consider a scenario: an employee is trying to download a set of customer records (which are sensitive) from a SharePoint site. Even if those data are labelled and protected, Conditional Access can ensure that this download only occurs under safe conditions (say, on a company-managed device that has up-to-date security patches and is not a personal device). If the employee tries the same on an

untrusted device or from an unusual location, the policy could block the download or ask for additional authentication. This significantly reduces the risk of data leakage, because even valid users cannot access certain data in potentially risky circumstances. Microsoft provides fine-grained controls; for instance, integration with Microsoft Defender for Cloud Apps (formerly Cloud App Security) can impose session-based restrictions, like disabling the ability to download or copy content when accessed via a web session on an unmanaged device, rather than outright blocking access to view the content.

From a GDPR and data protection point of view, Conditional Access helps enforce the principle of *least privilege and adequate security*. It ensures that personal data are accessed only by authorised persons and in a secure manner, thereby reducing the chance of compromised accounts leading to breaches. For example, if an attacker steals a user's password, they would still be thwarted by MFA requirements and device checks in many cases. In terms of compliance, these controls can be part of a Data Protection Impact Assessment mitigation strategy, demonstrating that the organisation has technical measures to prevent unauthorised access to personal data.

However, Conditional Access, like other security measures, can affect the user experience. Users may find themselves prompted for MFA frequently if policies are not tuned, and this can cause frustration, especially if the prompts occur during travel or off-hours access when the system flags the sign-in as atypical. In a British English context, one might say that users could be 'put off' from using the correct channels if it becomes too much hassle. Indeed, if someone is repeatedly blocked from accessing a needed document on their personal phone due to strict device policies, they might resort to sending that document to a personal email or some other insecure workaround (the classic shadow IT issue). Therefore, while Conditional Access greatly strengthens security, it must be designed with an understanding of user work patterns. Microsoft recommends a balanced approach: for example, using conditions like 'trusted locations' or managed device compliance to reduce unnecessary MFA requests for low-risk scenarios and only enforce the strictest controls when truly needed (such as accessing highly sensitive data from an unknown network) [6].

One feature to note is that these access policies can also incorporate *sensitivity labels* and the context of the content in certain ways. Through integration of Purview Information Protection with Azure AD, organisations can use label-driven access policies. As a hypothetical example, a highly confidential document stored in SharePoint could be configured such that only users in a specific Azure AD group (say, top management) can access it, and only from compliant devices. This marries content classification with identity-based security. Although not trivial to set up, it is possible through a combination of Microsoft 365 E5 Compliance features and Azure AD dynamic groups or SharePoint site sensitivity-based access rules. The result is a very tight control over sensitive information.

In terms of user impact, a well-implemented Conditional Access policy is often not noticeable until it needs to be. That is, under normal conditions (employee in office on a company laptop), everything works seamlessly; but the moment something is outside the norm (login from abroad, or an unmanaged device), the user encounters a security hurdle. Communicating the rationale for these hurdles is important. IT departments often roll out these policies accompanied by guidance, e.g. "To protect company and client data, we require MFA when you're signing in from outside the UK" or "Access to certain applications will be limited on personal devices". This transparency helps users understand that these are protective measures, not arbitrary barriers.

In summary, Conditional Access in Azure/Office 365 adds a crucial layer of defence by ensuring that data access itself is governed based on risk conditions. It complements content-centric controls (like DLP) by guarding the front door, so to speak. By imposing conditions such as MFA, device compliance, and location-based restrictions, it significantly reduces the likelihood of unauthorised data sharing or theft. However, as with other measures, finding the sweet spot is necessary: too lenient and it will not stop threats; too strict and it may hinder legitimate access, potentially leading users to circumvent policies. The evolving best practice in industry is to employ adaptive risk-based policies using Microsoft's tools to assess session risk in real time and only challenge the user when the risk is above a threshold. This minimises friction while maintaining strong security postures.

5. Compliance with GDPR and UK Data Protection Regulations

Ensuring compliance with data protection regulations is one of the main drivers behind the adoption of robust information governance and DLP controls. The GDPR of the European Union, which came into effect in 2018, and the UK's Data Protection Act 2018 (which implements similar requirements post-Brexit), impose legal obligations on organisations with respect to personal data. Key principles include data minimisation, purpose limitation, storage limitation, integrity and confidentiality of personal data, and accountability. Failure to comply can result in heavy fines and reputational damage. Microsoft's cloud services, including Azure and Office 365, have been developed with these regulations in mind, offering features that help organisations meet their compliance duties.

One fundamental requirement under GDPR is to know what personal data you have and where it resides (this aligns with the principle of accountability and facilitating data subject rights). Microsoft Purview's data discovery and classification capabilities directly support this need. By automatically identifying and tagging personal data across an organisation's files and databases, Purview helps create the inventory needed for compliance. For example, if a data subject issues a Subject Access Request (SAR/DSR) asking for all their personal data, the organisation can leverage Purview's catalog and eDiscovery tools to locate that information across Exchange emails, SharePoint documents, Teams messages, and so on. Microsoft provides specific guidance and tools for Data Subject Requests in Office 365, enabling administrators to search through user mailboxes and OneDrive, and to collect data for review [9]. These capabilities mean that what could be an overwhelming manual task is partly automated, thus improving compliance while controlling the administrative burden.

Another core principle is **storage limitation** – i.e. not keeping personal data longer than necessary. Office 365 addresses this through retention policies and labels. Organisations can configure Microsoft 365 retention policies to automatically delete or archive content after a defined period, according to legal requirements or business needs. For instance, an organisation might set a policy to delete emails after 7 years unless they are flagged for legal hold. Microsoft's documentation highlights that retention labels can 'help you keep personal data for a certain time and delete them when they are no longer needed' [4]. This directly supports GDPR's requirement to dispose of data that is no longer required for the purpose it was collected. The UK ICO similarly expects organisations to have data retention schedules. Using these Office 365 features, companies can demonstrate that they have technical controls to enforce their data retention policies. A practical example is using an 'Employee record - Delete after 6 years' label applied to HR documents, which the system will then remove once that time elapses, automatically handling the lifecycle.

Security of processing (Article 32 GDPR) is clearly addressed by the combination of encryption, DLP, and access controls discussed in previous sections. Encryption (both at rest and in transit) is enabled by default in Office 365 and Azure for data in the cloud, which protects against certain types of breach (e.g., if someone somehow got physical access to the storage, the data is encrypted). More granularly, the sensitivity labels can apply encryption so that only certain identities can open a document (for example, a file labelled 'Confidential Finance' can be encrypted to allow only members of the Finance team to open it, even if it was leaked outside). This is a strong security measure

that ensures confidentiality. DLP policies, by preventing accidental leaks, also uphold the integrity and confidentiality of personal data. These tools exemplify the 'appropriate technical and organisational measures' required by GDPR to protect personal data. It should be noted that GDPR does not mandate specific technologies, but expects measures proportional to risk. Implementing Microsoft's advanced security features can be seen as meeting or exceeding industry standard protections, which would typically be considered sufficient unless special categories of data require even more stringent controls.

The **accountability** principle in GDPR (and mirrored in UK law) requires that organisations not only comply but are able to demonstrate compliance. Microsoft's Compliance Centre (part of Purview) provides dashboards and audit logs that help in this regard. The Microsoft 365 Compliance Centre offers a unified interface to manage compliance-related tasks and view the status of various controls. It even includes a Compliance Score / Manager tool that maps the controls implemented in the organisation to regulatory requirements and gives a score that indicates progress [5]. For example, it might show how many recommended GDPR controls (out of the Microsoft-provided control set) the organisation has adopted. Features such as audit logs are invaluable in forensic investigations and in showing regulators that you monitor data access. If a potential incident occurs, detailed logs of who accessed or attempted to share personal data can demonstrate that the organisation tracks activities and can identify the scope of a breach, as required by GDPR's breach notification rules.

It is important to note that while Microsoft provides the tools, the responsibility ultimately lies with the organisation (the data controller) to configure and use them properly. Microsoft acts as a data processor for many services, and they have contractual commitments to GDPR themselves (for example, offering data processing agreements, terms for international transfers, etc.). But if an organisation does not turn on DLP or does not classify any data, simply using Office 365 does not automatically make them compliant. Technology must be used properly according to an internal governance strategy. Fortunately, Microsoft's official guidance and templates make it easier to get started. There are built-in policy templates for GDPR that can be imported: these include, for example, detection of European national IDs, health information, and other personal data categories defined by GDPR as sensitive. An administrator could use the DLP template 'GDPR Data' to quickly create rules that trigger when EU personal data is shared externally [4]. Such features reduce the barrier to compliance implementation and reduce the need for deep expertise, which is especially helpful for smaller organisations (as indicated in the "GDPR simplified guide" for small businesses provided by Microsoft).

Concerning the *UK Data Protection Act 2018 and the UK GDPR*, after Brexit, the UK retained the core GDPR framework. All the above measures relevant to GDPR apply equally to UK law, with perhaps additional attention to UK-specific codes of practice or guidance from the UK Information Commissioner's Office (ICO). One consideration is data residency and sovereignty: Some UK organisations prefer or are required to keep data within UK datacenters. Microsoft has responded by offering region-specific data residency (for instance, Office 365 tenants can be anchored to UK data centres). Although this is more of an infrastructure aspect than a Purview feature, it is worth noting as part of compliance. Data residency helps address legal concerns about cross-border data transfers, which is a hot topic under GDPR (e.g., data going to the US). Microsoft's cloud has options like Multi-Geo to keep certain mailboxes or sites in a chosen geography. Ensuring these settings align with organisational policy is another piece of the governance puzzle.

In practice, companies often undertake a *Data Protection Impact Assessment (DPIA)* when deploying cloud services such as Office 365 to process personal data, especially if it is a new or high-risk use. Microsoft provides detailed documentation to assist controllers in this process, explaining how Office 365 handles data, what security features are available, and how to configure them to mitigate risks [1]. A DPIA might conclude, for example, that enabling DLP and encryption for certain sensitive data categories is necessary to reduce risk to an acceptable level, thus recommending the use of those Purview features. It might also highlight any residual risks: perhaps the risk of user error if not all data can be automatically classified, and hence administrative or training controls would be added.

Microsoft Azure and Office 365 are well aligned with GDPR and UK data protection requirements. They offer a broad toolkit that, if properly used, can greatly ease the burden of compliance: from discovering and cataloguing personal data, protecting it with appropriate technical measures (encryption, access control, DLP), to facilitating the handling of data subject rights, and demonstrating compliance via audits and reports. The trade-off is that these protections must be thoughtfully integrated into business operations. Compliance must not be achieved at the expense of completely hampering day-to-day work. Regulators themselves recognise the need for balanced approaches: GDPR talks about appropriate measures, implicitly understanding that there is a point where controls can become impractical. Using Microsoft's tools, organisations have the flexibility to adjust the dials (security versus usability) to meet legal obligations while still empowering users. The best results often come when organisations foster a culture of compliance: employees understand the importance of these controls and cooperate with them, rather than view them as an adversary. Achieving this culture is easier when controls are not overly onerous, which is why fine-tuning and user-centric design of policies, as discussed earlier, is critical.

6. Conclusion

Data sharing and collaboration in the cloud era introduce significant governance challenges, but with the right tools and policies, organisations can strike a viable balance between usability and security. In the Microsoft Azure and Office 365 environment, the suite of Purview-driven governance solutions, DLP policies, information protection labels, and Conditional Access controls provide a comprehensive framework to protect sensitive data and adhere to regulations such as GDPR. These tools enable centralised governance – discovering where data lives, classifying their sensitivity, and enforcing rules and protections consistently across the ecosystem – which is invaluable for maintaining control in large, complex data estates. They also embody privacy-by-design principles, giving organisations out-of-the-box capabilities to encrypt data, prevent leaks, and tightly manage access.

However, as we have emphasised, every security measure comes with a usability impact. The effectiveness of an information governance programme is not measured only by how strict the controls are but by how well they are adopted and respected in practice. If employees find ways to circumvent policies due to frustration, the organisation could end up less secure than if a slightly more permissive, but respected, policy were in place. Therefore, implementing Microsoft's data governance tools must be accompanied by an empathetic understanding of business workflows. Administrators should leverage features such as policy tips, user override with justification, and adaptive access policies to involve users in the security process rather than unilaterally blocking them. Training and awareness campaigns are also key: When users understand *why* that a certain file cannot be shared externally, they are more likely to comply or seek appropriate approvals, rather than finding shadow IT solutions.

The tension between usability and security is not a zero-sum game where one must entirely trump the other. With careful design, organisations can achieve strong security with minimal disruption. The "myth" that usability must be sacrificed for security can be dispelled through intelligent, context-aware controls [2]. Microsoft's platform, especially as it continues to evolve with AI and smarter analytics, is moving toward this ideal by offering tools that can take a lot of the compliance burden off users (through automation) while keeping

them in the loop when needed. For instance, auto-classification of content can silently protect most files, and only in edge cases will a user be asked to make a decision or perform an extra step.

From a compliance perspective, the use of these modern tools is an effective way to meet regulatory requirements and demonstrate due diligence. Regulators often look for evidence that an organisation has thought about risks and implemented appropriate controls; a well-implemented suite of Microsoft 365 compliance solutions can serve as tangible evidence of that. Furthermore, audit trails and dashboards help in reporting and accountability, which are crucial under laws such as GDPR.

Microsoft Azure and Office 365 provide a rich set of capabilities to enable data sharing in a secure, governed manner. The trade-offs between security and usability can be managed by using these capabilities to their fullest extent and customising them to the needs of the organisation. By doing so in combination with the promotion of a security-conscious culture, organisations can ensure that data are available to fuel productivity and collaboration and are protected to meet legal and ethical obligations. The result is an enterprise that can confidently leverage its data for innovation and service, without constantly fearing the next data breach or compliance audit, a goal that lies at the heart of effective information governance in the cloud age.

7. Contact Novalytics for More Information

Novalytics provides strategic advisory services in information governance, digital transformation, and data strategy for small businesses in the regulated and high-risk sectors. We support organisations in modernising their operations through secure and privacy-preserving technologies - ensuring innovation is aligned with regulatory compliance, ethical standards, and long-term resilience.

For expert guidance on digital strategy, transformation planning, or information governance frameworks, please contact us at:

- Website: https://www.novalytics.co.uk
- Email: contact@novalytics.co.uk

References

[1] Microsoft, *Guidance for data controllers using office 365 - dpia*, Microsoft Compliance Documentation, Accessed 2025-05-09, 2018. [Online]. Available: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365.

[2] Y. Bertrand, K. Boudaoud, and M. Riveill, "What Do You Think About Your Company's Leaks? A Survey on End-Users Perception Toward Data Leakage Mechanisms," *Frontiers in Big Data*, vol. 3, p. 568 257, 2020. DOI: 10.3389/fdata.2020.568257.

[3] S. Ahmad, D. Arumugam, S. Bozovic, *et al.*, "Microsoft purview: A system for central governance of data," *Proceedings of the VLDB Endowment*, vol. 16, no. 12, pp. 3624–3635, 2023. DOI: 10.14778/3611540.3611552.

[4] Microsoft, *GDPR simplified: A guide for your small business*, Microsoft 365 Admin Documentation, Accessed 2025-05-09, 2023. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/gdpr-compliance.

[5] Microsoft, *General data protection regulation (gdpr) overview*, Microsoft Trust Center Documentation, Accessed 2025-05-09, 2023. [Online]. Available: https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview.

[6] Microsoft, *Building a conditional access policy (microsoft entra id)*, Microsoft Learn Documentation, Last updated 2024-05-06, accessed 2025-05-09, 2024. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policies.

[7] Microsoft, *Protect your sensitive data with microsoft purview (information protection overview)*, Microsoft Learn Documentation, Last updated 2024-06-06, accessed 2025-05-09, 2024. [Online]. Available: https://learn.microsoft.com/en-us/purview/information-protection.

[8] Microsoft, *Learn about data loss prevention*, Microsoft Learn Documentation, Last updated 2025-03-31, accessed 2025-05-09, 2025. [Online]. Available: https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp.

[9] Microsoft, *Office 365 data subject requests for the gdpr and ccpa*, Microsoft Compliance Documentation, Last updated 2025-03-07, accessed 2025-05-09, 2025. [Online]. Available: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-office365.