acora
The Choice of Leaders

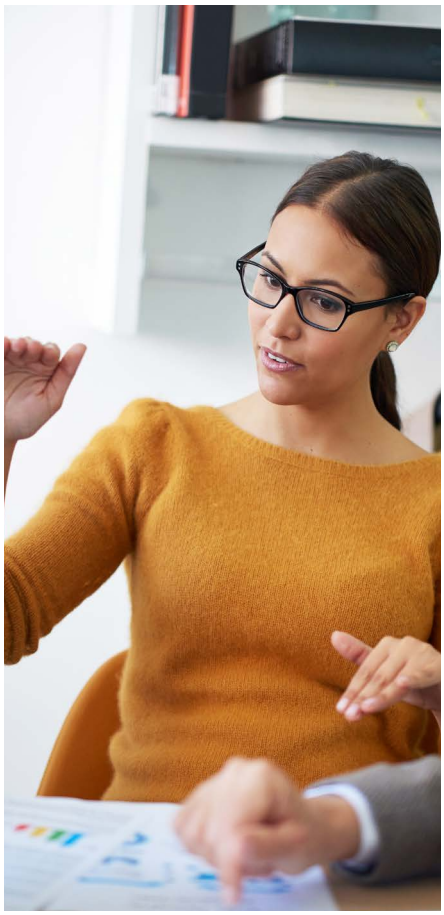
A quick guide to Office 365 and the GDPR

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

Controlling personal data

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

- **Data Loss Prevention (DLP)** in Office and Office 365 can identify over 80 common sensitive data types including financial, medical, and personally identifiable information. In addition, DLP allows organisations to configure actions to be taken upon identification to protect sensitive information and prevent its accidental disclosure.
- **Advanced Data Governance** uses intelligence and machine-assisted insights to help you find, classify, set policies on, and take action to manage the lifecycle of the data that is most important to your organisation.
- **Office 365 eDiscovery** search can be used to find text and metadata in content across your Office 365 assets—SharePoint Online, OneDrive for Business, Skype for Business Online, and Exchange Online. In addition, powered by machine learning technologies, Office 365 Advanced eDiscovery can help you identify documents that are relevant to a particular subject (for example, a compliance investigation) quickly and with better precision than traditional keyword searches or manual reviews of vast quantities of documents.
- **Customer Lockbox for Office 365** can help you meet compliance obligations for explicit data access authorisation during service operations. When a Microsoft service engineer needs access to your data, access control is extended to you so that you can grant final approval for access. Actions taken are logged and accessible to you so that they can be audited.



Protecting personal data against security threats

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.
- Finally, 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.

For more information please get in touch.

Feel free to get in touch. We're here to help.

Acora - Head Office
Acora House, Albert Drive, Burgess Hill, West Sussex, RH15 9TN T: +44 (0) 844 264 2222 W: acora.com E: sales@acora.com

acora
The Choice of Leaders