Microsoft® Online Services

Customer Data Flows in Office 365
Europe, Middle East, Africa

This document describes where Microsoft stores and accesses customer data in the course of providing the Office 365 services for customers with addresses in Europe, the Middle East, or Africa (EMEA). Specifically, it provides information regarding:

- The locations of primary and backup data centers for the Office 365 services.
- The service logs used by engineering teams to support Office 365.
- General customer support for Office 365.
- Other data handling issues associated with Office 365.

Overview

For customers with ship-to addresses in EMEA, Microsoft will store customer data on the service in the European Union, the United States, and Canada, except that a limited amount of customer data may in some cases be accessed from or transferred to other countries in order to provide support services as described in more detail below. Whenever we store, transfer or permit access to data, we follow applicable law. Additionally, Microsoft abides by the Safe Harbor Framework for transfer of data between the European Union and the United States.

As we optimize the efficiency of our service operations over time, we may need to alter data flows, though we will do so only after careful consideration and in compliance with applicable law. If you would like to receive information about changes to data flows, please sign up for "Compliance Notifications" in the Microsoft Online Services Portal.

Microsoft's Primary Data Centers

A primary data center is where the application software and the customer data running on the application software are hosted. Office 365 uses several primary data centers.

Microsoft's data center in Ireland is the primary data center for ForeFront Online Protection for Exchange. Microsoft's data center in the Netherlands is its primary data center for SharePoint Online. This includes the Office Web Apps when used as part of SharePoint Online. Microsoft also uses its data centers in Ireland and in the Netherlands interchangeably as primary data centers for Exchange Online (including the Office Web Apps when used as part of Exchange Online) and Lync Online.

Microsoft maintains multiple data centers in the United States.   It uses these data centers, along with its data center in Ireland, as the primary data centers for the Microsoft Online Portal and for all Office 365 services' directory data, with data replicated between locations. However, if you are accessing the Microsoft Online Portal from a region other than the U.S. or the EU, then web-pages you are viewing will be hosted in that region's data center. Microsoft also uses data centers in the U.S. to host a small amount of data, including user email addresses, which is used for routing Lync Online communications.

Microsoft® Online Services

Microsoft also uses its U.S. data centers to load balance with its primary data center in Ireland for ForeFront Online Protection for Exchange. Finally, Microsoft uses one or more U.S. data centers as primary data centers for all Office 365 services' authentication (this includes storing end users' names, usernames, Online ID passwords, and universal identifiers used to log into the Office 365 services), and for Office Professional Plus.

Microsoft's Backup Data Centers

A backup data center is used for failover purposes. If the primary data center ceases functioning for any reason, the application software and customer data running on that application software will also be available from the backup data center. Customers may not be notified when failover occurs. Depending on the particular service, this may not result in any service interruption. Customers should assume that at any given time their data may be processed in either the primary or the backup data center.

Microsoft uses its data center in Ireland as the backup data center for SharePoint Online. This includes the Office Web Apps when used as part of SharePoint Online. Microsoft also uses its data center in the Netherlands interchangeably with its data center in Ireland as a backup data center for Exchange Online (including the Office Web Apps when used as part of Exchange Online) and Lync Online.

Microsoft maintains multiple data centers in the United States. It uses these data centers, along with its data center in the Netherlands, as backup data centers for the Microsoft Online Portal and for all Office 365 services' directory data, with data replicated between locations. Microsoft also uses one or more of these data centers in the U.S. as backup data centers for all Office 365 services' authentication, for ForeFront Online Protection for Exchange, and for Office Professional Plus.

Access to Service Logs Containing Customer Data

Office 365 has been designed to be provided and maintained using service logs that record errors and performance issues, rather than using direct access to customer data. These service logs may contain customer data used for trouble shooting such as email addresses, subject lines of emails, file names and site URLs, to identify the source of the error or performance issue being resolved. Service logs do not contain non-public customer data such as customer documents, email message bodies or attachments, website content, or IM/voice conversations.

When problems occur with the Office 365 services, Microsoft personnel may access these service logs in order to troubleshoot and solve problems. Specifically:

- Microsoft personnel in Ireland, the Netherlands, and the United States can access these logs in the form they are stored in our data centers.
- Microsoft personnel in Microsoft's Canadian facilities who support ForeFront Online Protection for Exchange have access to logs for the Forefront Online Protection for Exchange service.
- Microsoft personnel in other jurisdictions either do not have access to these logs or have access only to logs that have been filtered to remove customer data.

Microsoft®Online Services

Customer Support

Microsoft stores Office 365 customer support information on customer support systems in the United States. These systems are used when providing phone, email, and web customer support for Office 365. The support information stored on the Office 365 customer support systems includes any information submitted by customers through support request systems, and may also include information from the Office 365 service that is used to provide support such as directory information and relevant service logs. Currently, Microsoft uses support personnel in Bulgaria, Ireland, and the United States to provide customer support. In addition, the ForeFront Online Protection for Exchange service also uses support personnel in Canada.

Support personnel may, in certain cases, need to escalate issues to Microsoft support engineers in other locations. In doing so, customer information entered in the support ticket may be transferred to these other locations. Customers may always ask support personnel where they are located.

While an escalation may entail access to data included in a support ticket, support engineers are trained not to access or copy customer data from Office 365 itself, except within the European Union, and the United States.

The foregoing does not apply to support or consulting services purchased separately from the Online Services. Customers who purchase such additional support or consulting services should consult their contracts or documentation for further information.

Other Data Flows

Administrator contact information and other administrator data may be used by Microsoft for general account management and support purposes and as otherwise described in the *Account Management and Billing Information* section of the Microsoft Online Services Trust Center.

Finally, the following types of data are outside the scope of this document:

- logs and other data that are devoid of customer data, either because they never contained it or because they have been anonymized or filtered to remove it;
- network packet headers and IP addresses;
- illegal content and data that violates our acceptable use policy, which includes email that is identified as spam or other malware; and
- data that Microsoft is required to transfer to comply with applicable law or regulations.

NOTICE AND DISCLAIMER

This document is for informational purposes only. While we strive for accuracy and the content is believed accurate as of the date of publication, this information is subject to change at any time and should not be interpreted to be a commitment or guarantee on the part of Microsoft.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.