

Privacy Considerations in the Cloud



Your data is your business. In a time when your customers' transactions are increasingly taking place online, it becomes even more important to your business that the information your customers provide through the use of a cloud service is stored and used in a way where they are protected, and your business's intellectual property is too. It only takes a look at the daily news headlines in the past few years to understand what a contested issue access control for customer data is. For your customers, they

want to know who can see their online activity. For your business, you need to protect your systems against malicious attacks.

That's why it's more important than ever that you trust your cloud provider. When you select a cloud provider, you're not just choosing a service; you're entrusting them with your, or your customer's, most precious commodity. Here are questions you should ask prospective cloud providers about privacy and control.

Privacy and control

Do you use customer data responsibly and allow choices for how customer data is used?

Microsoft's cloud services incorporate privacy by design. We are transparent about our privacy practices and offer meaningful privacy choices. Our cloud services allow you to control who has access to your data, and how it's shared. We offer enterprise customers a regional approach to where your business data is stored. And you can take your data with you when you leave.

Industry standards

How do you ensure your services meet industry standards?

Microsoft's Cloud Infrastructure and Operations (MCIO) organization delivers the infrastructure and network for more than 200 consumer and enterprise cloud services. We created the Online Services Security and Compliance (OSSC) team within the MCIO to work with the services that rely on them to help ensure our cloud services have strong security, meet the privacy requirements of customers, and comply with applicable laws, regulations and international standards.

Access control

Who can access my data?

Microsoft adheres to stringent policies and procedures when it comes to accessing your data. We have automated a majority of our service operations so that only a small set require human interaction. Microsoft operates on a "need-to-know-basis", which means that access to your data by Microsoft personnel is restricted and can only be accessed when it is necessary for these operation. After that access rights are immediately revoked. In the case of government surveillance, Microsoft has taken steps to ensure that there are no back doors and no direct or unfettered government access to your data.

No advertising use

Will customer data be used for other purposes?

Microsoft's Enterprise business model does not include exploiting your customer data for purposes unrelated to providing the cloud service. We do not use your customer data for advertising or similar commercial purposes.

Third-party requests

What happens if law enforcement or another third-party asks Microsoft for my customer data?

We do not disclose your data to a third party except as directed by you or required by law. When permitted, we attempt to redirect any requests for your data directly to you.

Data location

Will I know the physical location of my data center?

Microsoft is transparent about where we store your data, and we make this information available through the Trust Center. This is important if you are operating in regulated industries, where data protection laws require you to know the geographic location of your data. We maintain an expanding network of cloud-scale datacenters in locations around the globe, and verify that each one meets strict security requirements.

Data portability

Can I take my data with me when my subscription ends?

Yes. Our Online Services Terms details what happens when you leave the service or your subscription expires, including data portability. You can retrieve a copy of all of your data for any reason. You do not need to notify Microsoft or ask for assistance before deleting your data.

Deletion of data

What is your policy for deleting data? Can you assure me it will be completely removed?

Microsoft follows strict standards for overwriting storage before reuse. If you delete your data or terminate your contract, we will ensure your data is deleted in accordance with your contract with us. In the event a hard drive fails, it will be physically destroyed in a way that makes data recovery impossible.

International data transfer

How does Microsoft comply with international data protection laws regarding cross-border transfers of personal data?

If your data is being transported or stored across international borders, you can be assured that Microsoft has taken steps to ensure the transfer is compliant with applicable laws.

References

- To learn more about how Microsoft protects your data: Visit the Microsoft Trust Center at www.microsoft.com/trustcenter
- Microsoft Trusted Cloud: Visit our website at www.microsoft.com/trustedcloud
- Microsoft Trust Center: Your privacy policy center: www.microsoft.com/trustcenter
- Protecting Customer Data: Up-to-date national news: www.microsoft.com/transparencyhub
- Microsoft Online Services Terms: Terms of use governing Microsoft's Online Services: aka.ms/microsoftonlineserviceterms
- Microsoft on the Issues blog, featuring Brad Smith and other Microsoft executives: blogs.microsoft.com/on-the-issues