# Office 365

## Microsoft NZ's standard response for the NZ Office of the Privacy Commissioner's Cloud Computing Checklist and Guide

Overview

The Office of the Privacy Commissioner (OPC) published a Cloud computing checklist and Cloud Computing – A guide to making the right choices in February 2013. Both resources are available from http://privacy.org.nz/using-the-cloud/.

Microsoft New Zealand Limited has prepared this standard response to help organisations assess the Office 365 cloud service against the OPC checklist and guide. We will discuss each of the topics in the checklist and guide in the order they are presented in the OPC resources.

We have summarised relevant information as of April 2013. For more current and complete information, including definitions of key terms used in this response, please refer to http://trust.office365.com/ and your Office 365 service agreement.

We believe that Office 365 can help you meet or exceed all the requirements in the OPC checklist and guide. We hope that Office 365 will be able to play a part in helping many New Zealand organisations improve privacy, security, and service continuity disciplines in a cost effective way.

"Please note: Pop-outs formatted as per this note are Questions from the OPC Checklist and Guide. Microsoft answers are directly beneath each question."

## Contents Page

## 1. Figure out which cloud services will work for you and what your current risk level is

> "Think of what risks you currently have with handling personal information. Will using the cloud increase or decrease those risks?" (OPC)

The OPC checklist and guide provide a useful framework to compare current systems with the Office 365 services. We often hear from customers that the privacy, security, and service continuity disciplines of Office 365 far exceed what they can provide in-house.

> "What matters in terms of privacy is what is happening to the information - where it goes, where it's stored, who can see it and who can use it." (OPC)

Whether you are a business, a Government agency, an NGO, or an educational institution, we hope that this document will help you understand the privacy, security, and service continuity disciplines that are engineered into the Office 365 cloud services. These disciplines are designed to help you satisfy information management and regulatory requirements, including privacy laws.

You will need to answer some parts of the checklist yourself, where they relate to your organisation and responsibilities that can't be delegated to others.

## 2. Know what information you'll be sending to the cloud

> "Work out what information you'll be putting in the cloud, so you know what to focus on and what you can relax about. ... The more harm it could cause [if the information was lost], the more care you have to take to check it's protected." (OPC)

As well as compliance with legal obligations, it's good practice for any organisation to be careful with personal, confidential, and sensitive information. The integrity of financial and customer records, trade secrets, and contracts can be critical to business continuity.

It is useful to consider how well this information is secured and backed up before and after any computer system change.

If you look at the privacy, security, and service continuity disciplines your organisation applies today, and how often are these disciplines updated, audited, and tested to ensure that they are robust, are you confident that the physical and software security systems you have in place now are adequate?

## 3. Recognise that the responsibility is ultimately yours

> "Your cloud provider may have some responsibility for handling the information safely – check the contract." (OPC)

In the Online Services Use Rights, Microsoft makes a contractual commitment to implement reasonable and appropriate technical and organisational measures, as set out in the security overview applicable to the relevant Office 365 service, to help secure customer data against accidental or unlawful loss, access, or disclosure. Microsoft makes contractual commitments to:

- use customer data only for the purpose of providing the Office 365 services to you (and not to build advertising products out of customers' data, for example);
- comply with all laws applicable to the provision of Office 365, including applicable security breach notification law; and
- not disclose customer data to third parties (including law enforcement, other government entities, or civil litigants, but excluding Microsoft subcontractors) except as you direct or required by law.

In the Office 365 Privacy Statement (which is linked from Online Services Use Rights), Microsoft outlines how it will respond to certain security incidents that involve customer data. Microsoft also explains how it will handle administrator data, payment data, and support data, which are other types of data (separate from customer data) that are used in conjunction with the Office 365 services.

The Online Services Use Rights form part of the Microsoft Online Services Agreement, or MOSA, which is the standard agreement for New Zealand organisations who purchase Office 365 plans from Office365.com.

Office 365 has also been engineered so that Microsoft can agree to European Union Model Clauses, and the US HIPAA Business Associate Agreement that is designed to safeguard protected health information. All Office 365 customers benefit from this engineering work, whether or not European or United States regulations apply to them.

> "For most businesses, the staff are the key to handling personal information properly. Figure out what your staff need to know. Talk to them about your move to the cloud, and what's involved. Give them any training or advice they need so they can help you keep personal information safe." (OPC)

Most of the privacy, security, and service continuity disciplines built into Office 365 apply automatically without the need for you or your staff to do anything more.

Administrative credentials for any computing service, including Office 365, need to be carefully managed in your organisation.

The Office 365 services include a number of specialised security options that customers can take advantage of if they wish, such as enabling data auditing policies, running eDiscovery, data loss prevention tools to reduce the risk of sensitive documents being emailed outside the organisation, and the management of data "spills".[1]

[1] Please refer to the Office 365 Security White Paper for further information.

## 4. Security - lock it down

"Be clear on which aspects of security are your responsibility, and which are the provider's." (OPC)

It is your responsibility to assess whether the privacy, security, and service continuity disciplines for the Office 365 services meet your requirements. In many cases we hear that these disciplines far exceed what organisations can provide in-house.

It is important to understand what is not included in the services, so that you know what you will still need to manage yourself.

For example, you will remain responsible for the actions of your staff, including anyone in your organisation who has administrative access to the Office 365 services.

Your organisation will also remain responsible for ensuring that aspects such as the security of the devices that your staff use is maintained in good order (for example, by using the Windows Intune cloud service), that staff keep their credentials secure, and that data is not misused after your staff extract it from Office 365 (for example, with help from Information Rights Management).

"Make sure the information is protected both while it travels and when it's at the provider's end." The provider should tell you whether "data is automatically encrypted when it is being transferred between your organisation and the cloud provider." (OPC)

Data is automatically encrypted with industry-standard TLS and SSL protocols when it is transferred between your organisation and Office 365.

In addition to physical and network security for data that is stored in Office 365, Microsoft also uses
BitLocker 256-bit AES 'encryption at rest' for the hard drives of servers that are used to store email.

The provider should tell you "the measures that it takes to ensure physical and digital security (the Cloud Security Alliance Cloud Controls Matrix provides a comprehensive list that you can ask providers to respond to)" (OPC)

Office 365 is secured in five layers – data, application, host, network, and physical. An executive summary of security measures is offered in the Office 365 Security White Paper, and answers to the comprehensive Cloud Security Alliance Cloud Controls Matrix are also available for Office 365.[2] Office 365 has been designed according to Microsoft's Security Development Lifecycle, a comprehensive security assurance process that informs every stage of design, development, and deployment of Microsoft software and services.

[2] The Office 365 Security White Paper provides an executive summary of Office 365 security disciplines.
Technical details are available in the Cloud Security Alliance cloud control matrix response for Office 365.

The provider should tell you "the independent audit or certification process that the provider undertakes and the results of those tests (there are internationally recognised standards in place, such as ISO/IEC 27001)" (OPC)

Microsoft's cloud services are audited and certified by reputable third parties.

Detailed audits look into every area of the security of the cloud services to ensure they meet or exceed high standards. Office 365 has been certified for ISO 27001, and SSAE16 SOC1 (type II), and has FISMA Authority to Operate.

Audits play a critical role because it is not possible for all Office 365 customers to visit Microsoft datacentres. These certifications show that leading experts have visited Microsoft datacentres to review the services and found that they meet the required standards.

The provider should tell you "are these certification current and do they require independent verification"(OPC)

The Office 365 certifications mentioned above are current. They are based on independent verifications by security audit experts.

The provider should tell you "what physical security measures they have - for example do they have surveillance, guards or restricted access" (OPC)

Physical security is a key part of the overall strategy Microsoft uses to ensure its cloud services are safe and reliable. To do this, Microsoft uses multiple measures including smartcards, biometric scanners, on-premises security guards, and continuous video surveillance.

Staff with access to facilities or IT systems that store customer data are thoroughly vetted and subject to comprehensive background checks.

## 5. Check out your provider

"Do an internet search on the cloud provider you're thinking of using – along with words like 'breach' and 'privacy'." (OPC)

This is a step you should undertake yourself for each provider you are considering.

"Are they regularly and independently audited?" (OPC)

Yes, please refer to the response on independent audits and certifications in section 4 (above).

## 6. Know exactly what you're signing up for

"Check the contract. Make sure your key concerns are covered in the contract (if you have the ability to negotiate) or in the standard terms and conditions." (OPC)

We believe the Office 365 contract terms are competitive with comparable cloud services, but this is an aspect that you will need to consider for yourself.

"Check that you know whether the provider has to tell you if something goes wrong (for instance if there is a security breach)" (OPC)

In the Office 365 Privacy Statement Microsoft commits to notifying Office 365 customers if it becomes aware of:

- unlawful access to any customer data stored on Office 365 equipment or facilities, or
- unauthorised access to Office 365 equipment or facilities resulting in loss, disclosure, or alteration of customer data.

If these security incidents occur, Microsoft notifies customers of the incident, investigates it, and provides affected customers with information about the incident.

Microsoft also commits to take reasonable steps to mitigate the effects and to minimise any damage resulting from the incident. Microsoft reporting or responding to incidents is not an acknowledgement of any fault or liability with respect to an incident.

As with any IT system, incidents could occur due to human error or a security breach within your organisation that is unrelated to Office 365 and outside Microsoft's control, so you will still need to ensure that security disciplines within your organisation are sufficient.

"Check that you know how you would notify your customers if their data is lost or stolen" (OPC)

Notifications of security incidents would be delivered to your nominated Office 365 administrators by email or other means that Microsoft chooses.

It's up to you to make sure that you maintain accurate contact information on the Office 365 Services portal so that service notifications reach you, and that you in turn inform your customers when it is appropriate to do so.

"Check that you know how you're going to know whether the provider is living up to the terms of the agreement (for example does it get regular independent audits done that you'll be able to check?)" (OPC)

Please refer to the response on independent audits and certifications in section 4 (above).

"Check that you know who is liable and what the penalties are if something goes wrong" (OPC)

*Performance and availability issues*

Microsoft provides financial backing to the commitment to achieve and maintain the service levels for Office 365. If service levels for Office 365 do not meet the Service Level Agreement for Microsoft Online Services, customers may be eligible for a credit towards a portion of their monthly service fees.[3]

*Other issues*

For other issues, the Office 365 service agreement for New Zealand organisations who buy Office 365 plans from Office365.com (the Microsoft Online Subscription Agreement, or MOSA) sets out the contractual liability in the event something goes wrong. The liability position is mutual, which means that Microsoft and Office 365 customers are liable to one another to the same extent, on the same terms.

The general rule is that liability in connection with an Online Service, such as Exchange Online, is limited to direct damages up to the amount paid under the MOSA for the Online Service giving rise to that liability during the 12 months before the liability arose, and specified types of losses are not recoverable (such as loss of revenue and consequential damages). There are some limited carveouts to this general rule (for example, where the breach is a violation of intellectual property rights).

You are provided with an opportunity to review the full terms and conditions of the MOSA when you sign-up for Office 365 via Office365.com, and we encourage you to review the terms and conditions carefully so that you know what you're signing up for. We believe the liability position is competitive when compared with that offered by comparable cloud services, but this is a comparison that you will need to undertake for yourself.

"Check that you know what country's law applies if there is a legal dispute and who the appropriate regulator might be?" (OPC)

If the legal dispute is about the Office 365 contract (the Microsoft Online Subscription Agreement, or MOSA), then the interpretation of the contract is governed by the laws of the US State of Washington, without regard to Washington law's conflict of laws principles.

Washington State is where Microsoft has its global headquarters, and Microsoft contracts under Washington law because it's the "home territory" for the company. As a global, enterprise-grade cloud service provider, Microsoft needs certainty that contracts will be interpreted in the same way all around the world.

Other countries' laws could also be relevant in some circumstances. For example, if the legal question was whether Microsoft had complied with a foreign privacy law that was applicable to the company as the provider of Office 365, then it would be necessary to consider the foreign privacy law and how it is enforced.

[3] Details are in the Service Level Agreement for Microsoft Online Services.

If the dispute is between you as a customer and an individual in New Zealand about how you handled personal information collected in New Zealand and stored using Office 365, then the relevant law for you is New Zealand law, and the appropriate regulator will be the New Zealand Privacy Commissioner.

Use of Office 365 does not change the fact that a New Zealand organisation will need to adhere to New Zealand laws.

"Check that you know whether mediation or arbitration is available. This might be cheaper and more practical than going to court" (OPC)

As mentioned above, the service contract for Office 365 (the Microsoft Online Subscription Agreement, or MOSA) provides for going to court if Microsoft or a customer needs to take legal action. There's nothing in the contract that prevents Microsoft and a customer from having settlement discussions prior to, or alongside, court proceedings, in appropriate cases.

"Check that you know whether your provider is insured against privacy breaches" (OPC)

Microsoft has insurance related to Office 365 privacy breaches.

"Check that you know what the provider's disaster recovery plan covers." (OPC)

Office 365 has sophisticated service continuity disciplines to help ensure that outages to customers of the service are kept at a minimum. Office 365 disaster recovery disciplines are consistent with industry and Microsoft best practices, and include:

- assignment of key resource responsibilities,
- notification, escalation and declaration processes,
- recovery time objectives and recovery point objectives,
- continuity plans with documented procedures,
- a training program for preparing all appropriate parties to execute continuity plans, and testing, maintenance, and revision process.

Service continuity provisions are also built into Office 365. For example, customer data is stored in an environment with robust backup, redundancy, restore, and failover capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are implemented, ranging from redundant disks to guard against local disk failure, to continuous, full data replication to a geographically distant datacentre to reduce the impact of natural disasters.

"You may not have much clout when it comes to negotiating contract terms, but you probably have a choice of providers - compare the protections they're able to offer." (OPC)

We believe the Office 365 contract terms are competitive with comparable cloud services, but this is a comparison that you will need to undertake for yourself.

## 7. Be as up front with your clients as you can

"Wherever you can, tell the people concerned what you're doing with their personal information." (OPC)

The Office of the Privacy Commissioner has some suggestions on its website about how to approach disclosure proactively or through privacy policies.

With Office 365, Microsoft makes a contractual commitment to use customer data only to provide the Office 365 service to you – in other words, to maintain and provide the service Office 365 customers have purchased (or in the case of schools, that they may be using free of charge). This could also include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the Office 365 services, and the improvement of features that detect, and protect against, emerging and evolving threats to the user (such as malware or spam).

We think this use limitation is important because customer data could include personal information of your staff, clients, patients, customers, or students. Microsoft's policy is not to use Office 365 customer data for other purposes, such as user profiling for advertising services or to improve advertising services.

On our reading of the Privacy Act, Microsoft holds customer data "for the sole purpose of processing the information on behalf of another agency, and does not use or disclose the information for its own purposes" in terms of section 3(4)(c) of the Privacy Act which means that "the information shall be deemed to be held by the [Office 365 customer] on whose behalf that information is so held or, as the case may be, is so processed".

This makes your privacy compliance for Office 365 considerably simpler than it may be for other cloud services that leave open the provider's ability to use customers' data for other purposes, such as the provider's new product development or advertising services.

Using Office 365 to manage your IT does not mean you're using information for a "new purpose", and for Privacy Act purposes, information stored by you in Office 365 is held by you (not Microsoft).

"Work out how you would respond to a customer's request to see information about themselves."(OPC)

As well as providing normal access to data that is stored in the service through client software and the web interface, Office 365 includes administrative functions such as eDiscovery that can help you to respond to legal requests under the Privacy Act or otherwise.[4]

[4] Please refer to the Office 365 Security White Paper for further information.

## 8. Location - where will the information be?

"If possible, work out where your information is going and what privacy laws apply." (OPC)

For customers who provide a New Zealand address when they sign up for Office 365, data will be stored in datacentres that serve the Asia Pacific region.[5]

The Singapore and Hong Kong datacentres are the primary Asia Pacific datacentres for the following Office 365 services:

- Exchange Online (email and calendars),
- SharePoint Online (document collaboration), and
- Office Web Apps (working with Office documents online).

Microsoft uses United States datacentres as the primary location for Lync Online (instant messaging, presence and conferencing). For data associated with the Office 365 Online Portal (the website from which the Office 365 services are accessed and managed), Active Directory (a rights management service), and Global Address Book (a directory service within Exchange Online), see the Asia Office 365 Geographic Boundaries document for further details.

Microsoft's regionalised datacentre strategy means that customer data generally remains within the chosen primary data storage region. As noted above, this will be Asia Pacific for customers who provide a New Zealand address when they sign up for Office 365.

However, from time to time, the requirements of providing Office 365 may mean that some data is moved to, or accessed by, Microsoft staff outside the primary storage region.

For example, to address latency, routing data may need to be copied to different datacentres in different regions. In addition, staff who have the most technical expertise to troubleshoot service problems may be located in a different region.

"The provider should tell you "whether there is a privacy law that applies in the country or countries where your data is stored or processed" (OPC)

Yes, there are privacy laws in Singapore and Hong Kong, where the primary Asia Pacific datacentres for Exchange Online, SharePoint Online and Office Web Apps are located.

Microsoft holds itself to the same privacy procedures for Office 365 all the way around the globe.

[5] Please refer to the Asia Office 365 Geographic Boundaries document for further details.

As a global, enterprise-grade provider of cloud services, Microsoft runs the Office 365 service with common operational practices and features around the world. What this means for you is that Microsoft treats your data in Office 365 the same way, irrespective of where your data is located and what local privacy laws exist. This gives you certainty about how your data will be handled.

Microsoft's baseline privacy commitments to Office 365 customers are set out in the Online Services Use Rights, which:

- reaffirm Microsoft's commitment to comply with all laws applicable to its provision of Office 365, including applicable security breach notification law,
- include an obligation on Microsoft to use customer data only for the purpose of providing Office 365 to you (and not to build advertising products out of customers' data, for example),
- set out that Microsoft will not disclose customer data to third parties (including law enforcement, other government entities, or civil litigants, but excluding Microsoft subcontractors) except as you direct or required by law, and
- contain promises about Microsoft's implementation of reasonable and appropriate technical and organisational measures, as set out in the security overview applicable to the relevant Office 365 service, to help secure customer data against accidental or unlawful loss, access, or disclosure.

In the Office 365 Privacy Statement (which is linked to from Online Services Use Rights), Microsoft outlines how it will respond to certain security incidents that involve customer data. Microsoft also explains how it will handle administrator data, payment data, and support data, which are other types of data (separate from customer data) that are used in conjunction with the Office 365 services.

The Online Services Use Rights form part of the Microsoft Online Services Agreement, or MOSA, which is the standard agreement for New Zealand organisations who purchase Office 365 plans from Office365.com.

Please note: this section is out of date, as the Office 365 Data Centres for New Zealand will be located in Australia, at the Australia East and Australia South-East Datacentres.

"The provider should tell you "whether that privacy law is equivalent to New Zealand's privacy law" The provider should tell you "whether the law applies to the cloud provider and to your information (some privacy laws exempt some types of businesses, or do not apply to the personal information of foreigners)" (OPC)

Microsoft holds itself to the same privacy procedures for Office 365 all the way around the globe. However, information about the main countries in which datacentres for Office 365 services delivered to organisations with a New Zealand billing address are provided for completeness.

### Singapore

Singapore's privacy law has a number of features in common with New Zealand's privacy law. Both laws reflect the principles of international and regional privacy guidance such as the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, and the APEC Privacy Framework. The main data protection provisions of the Singapore law are due to come into effect in mid 2014.

Singapore's privacy law will apply to Microsoft in its provision of Office 365 services from Microsoft's Singapore datacentres – Microsoft will be regulated as a 'data intermediary'. Singapore's privacy law does not distinguish between the personal data of Singaporean residents and foreigners. So organisations that process personal data in Singapore, including personal data that relates to New Zealanders, will be protected by the Singapore privacy law.

### Hong Kong

In our view, Hong Kong's privacy law provides similar protection to New Zealand's privacy law when the Hong Kong privacy law applies.

Hong Kong's privacy law will not apply to Microsoft in its provision of Office 365 services from Microsoft's Hong Kong datacentres. This is because (much like the New Zealand position) the onus for ensuring compliance with the law rests principally with the data user, not the data processor.

An organisation will be a data user under Hong Kong privacy law if that organisation controls the collection, holding, processing or use of personal data in or from Hong Kong. For most New Zealand organisations, this control is likely to be exercised from New Zealand (with the result that the relevant organisation is not a data user under Hong Kong's privacy law). You'll need to consider your organisation's circumstances to form your own view on this point.

The provider should tell you "how the cloud provider will deal with any requests for information that it receives from government agencies, courts etc. For example will the provider only disclose information in response to a court order? … Will the provider let you know if it has to disclose information in response to a request? … Make sure that they tell you how they deal with government requests, whether they demand a search warrant before giving access to information on their servers, and your rights to be notified if they pass the information on to somebody else." (OPC)

Microsoft will not disclose Office 365 customer data to a third party except as the customer directs or unless required by law. Third parties means law enforcement agencies, other government agencies, and those involved in civil litigation (but not Microsoft subcontractors who form part of the staff working to support the Office 365 service).

If a third party approaches Microsoft directly with a request for customer data, Microsoft will try in the first instance to redirect the third party to request the data directly from the customer, so that the customer has an opportunity to determine how to respond. As part of that, Microsoft might provide your basic contact information to the third party.

If Microsoft is compelled to disclose customer data to a third party, Microsoft will use commercially reasonable efforts to notify the customer in advance of a disclosure unless Microsoft is prohibited by law from doing so.

Microsoft's commitments around third party data requests are set out in the Online Services Use Rights and the Office 365 Privacy Statement.

Microsoft has recently started publishing transparency reports to disclose the number of requests received. In 2012, there were just eleven requests worldwide relating to enterprise customers of services like Office 365. Microsoft either rejected or was successful in redirecting seven of these eleven requests, and in the four instances where Microsoft disclosed some enterprise customer information, the company either obtained the customer's consent before complying, or disclosed the information pursuant to a specific contractual arrangement to process such requests on behalf of the customer.[6]

The provider should tell you "will the cloud provider notify you if data is lost or stolen, for instance if the provider is hacked?" (OPC)

Yes, please refer to the answer and the discussion of security incidents in section 6 above.

The provider should tell you "who can you or your clients complain to if there's a breach of privacy?" (OPC)

You and your clients can contact Microsoft if they wish to raise any privacy concerns. We welcome your comments and feedback. The best way to contact Microsoft is via http://support.microsoft.com/contactus/.

[6] Please refer to the latest Law Enforcement Requests Report for further information.

## 9. Use and disclosure - who sees the information and what will it be used for?

> "Any use of personal information should be directly related to the purpose for which you've got the information in the first place. If it's being used for a new purpose, that should almost always be authorised by the person the information is about … Make sure you know what the provider will be doing with the information (if anything)." (OPC)

The Office of the Privacy Commissioner has some suggestions on its website about how to approach disclosure proactively or through privacy policies.

With Office 365, Microsoft makes a contractual commitment to use customer data only to provide the Office 365 service – in other words, to maintain and provide the service Office 365 customers have purchased (or in the case of schools, that they may be using free of charge). This could also include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the Office 365 services, and the improvement of features that detect, and protect against, emerging and evolving threats to the user (such as malware or spam).

We think this is important because customer data could include personal information of your staff, clients, patients, customers, or students. Microsoft's policy is not to use Office 365 customer data for other purposes, such as user profiling for advertising services or to improve advertising services.

On our reading of the Privacy Act, Microsoft holds customer data "for the sole purpose of processing the information on behalf of another agency, and does not use or disclose the information for its own purposes" in terms of section 3(4)(c) of the Privacy Act which means that "the information shall be deemed to be held by the [Office 365 customer] on whose behalf that information is so held or, as the case may be, is so processed".

This makes your privacy compliance for Office 365 considerably simpler than it may be for other cloud services that leave open the provider's ability to use customers' data for other purposes, such as the provider's new product development or advertising services.

Using Office 365 to manage your IT does not mean you're using information for a "new purpose", and for Privacy Act purposes, information stored by you in Office 365 is held by you (not Microsoft).

You should also review the Office 365 Privacy Statement to understand how Microsoft handles administrator data, payment data and support data. These are separate types of data to customer data.

> "The provider should tell you, what purposes the provider may need access for, if any?" (OPC)

Microsoft strictly prohibits staff from accessing the customer data unless they can demonstrate there is a valid operational reason, such as:

- operational procedures such as database tuning,
- troubleshooting problems affecting the operation of services, or
- detecting and preventing security attacks, including malware or spam.

Access to customer data is strictly controlled and logged. Sample audits are performed both by Microsoft and third parties to attest that access is only for appropriate business purposes.

The Office 365 Privacy Statement explains the purposes for which Microsoft uses administrator data, payment data, and support data.

"The provider should tell you, are optimisation or other analytical processes carried out by the provider's staff, or are they automated?" (OPC)

Most optimisation and other analytical processes are automated. Manual intervention is only used on occasions when automated processes cannot resolve a service maintenance or upgrade issue.

"The provider should tell you, which staff have access to the information? How is that access controlled and monitored? Does the provider maintain an audit trail for who accesses the information and what for?" (OPC)

This table summarises the types of staff involved in running the service and whether or not they can access content.

Access to Content

| | |
|---|---|
| Operations Response Team (limited to key personnel only) | Yes, by exception |
| Support Organization | No |
| Engineering | No |
| Partners | Only with customer permission |
| Others in Microsoft | No |

Content is defined as customer data for which customers may have an increased expectation of confidentiality and that, when the Office 365 service is used normally, is transferred encrypted over the Internet. It specifically includes: the body of Exchange Online email messages and attachments, SharePoint site content and documents, instant messaging and voice conversations, and CRM business data.[7]

All Microsoft staff access to the IT systems that store customer data is strictly controlled via role-based access control based on the principle of granting least privilege. IT service

[7] Please refer to the Office 365 Administrative Access site for further details.

engineers request access for tasks they need to perform into a lock box, which has a defined duration and level of access. Lock box requests are logged and are auditable.

Customers can view audit information online or request a copy of it from Office 365 support services.[6]

"Can the provider use your information to develop its own products or for its own commercial gain - such as collecting statistics from your data to sell as a product to others?" (OPC)

With Office 365, Microsoft uses customer data only to do what customers pay us to do – in other words, to maintain and provide the service they have purchased. This can also include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the Office 365 services, and the improvement of features that detect, and protect against, emerging and evolving threats to the user (such as malware or spam).

Microsoft's policy is not to use Office 365 customer data for other purposes, such as user profiling for advertising services.

"Make sure you know if your cloud provider will be passing the information to a third party." (OPC)

The Office 365 Privacy Statement provides a detailed explanation of the limited circumstances when Microsoft shares customer data, administrator data or payment data with third parties.

Please also refer to the response in section 8 above regarding third party requests for access to customer data.

"Who will be able to see or use the information?" (OPC)

Except as detailed in the responses above, only those with customer user credentials will be able to see Microsoft's use of that user's information, and only those with customer administrative credentials will be able to access all of the customer's information.

It is important that you ensure your organisation and its staff treat user and administrative credentials with care to prevent misuse of those credentials.

## 10. Ability to exit, and deleting information

"The provider should tell you whether you can take the information with you if you choose not to use the service any longer … Can you get the information out, in a form that you can use, if you decide to switch providers? … The provider should tell you whether you will get the information in a format that you can use elsewhere - and how quickly the provider will get you the information" (OPC)

Office 365 customers can use their administrative access to take a copy of all of their data at any time and for any reason, without any assistance from Microsoft.

It is important that you ensure your organisation and its staff treat user and administrative credentials with care to prevent misuse of those credentials.

The information exported from Office 365 utilises formats widely supported by third parties including on-premises server products, and other cloud providers. There is also a rich eco-system of providers that allow customers to migrate data from one solution to another.

"The provider should tell you who will bear the cost for the process of switching to a new supplier" (OPC)

The customer will bear the cost of switching to a new provider. Microsoft provides administrative tools that customers can use to extract their information from Office 365. Data can be extracted from Office 365 at any time and for any reason.

"Will the provider delete the information or will they try to keep it? … The provider should tell you whether your information will be kept on the provider's systems after you move on, or whether it will be securely deleted. … The provider should tell you how the provider will verify for you that the information has been deleted." (OPC)

Microsoft will not keep customer data relating to Office 365 except to give customers time to extract their data from the service.

By default, Microsoft retains customer data on Office 365 for 90 days after a customer's agreement ends to give customers enough time to extract their information. After this period customer information is deleted. Cached or backup copies are purged within 30 days of the data being removed.

For Office 365, Microsoft uses processes, which are checked by Microsoft's auditors, to delete, wipe or destroy all media that are used to hold customer data. A detailed record of all destructions and deletions is maintained.