# Hosting Exception – detailed walktrough

## Introduction

When you sign up as a customer of Microsoft by accepting the Microsoft Customer Agreement, the general rule in the Microsoft Customer Agreement is that you as a customer are allowed to use the Online services:

“solely for Customer’s own use and business purposes and are non-transferable and you are not entitled to distribute, sublicense, rent, lease, or lend any Online services, in whole or in part, or use them to offer hosting services to a third party”.

Meaning you are as a general rule not allowed to share the power of Microsoft Online-services with third parties. According to the Product Terms you are however as a customer allowed to:

“create and maintain a Customer Solution and, despite anything to the contrary in Customer’s volume licensing agreement, combine Microsoft Azure Services with Customer Data owned or licensed by Customer or a third party, to create a Customer Solution using the Microsoft Azure Service and the Customer Data together. Customer may permit third parties to access and use the Microsoft Azure Services in connection with the use of that Customer Solution. Customer is responsible for that use and for ensuring that these terms and the terms and conditions of Customer’s volume licensing agreement are met by that use”.

The definition of “Customer Solution” is:

**“Customer Solution** means any application that the Customer makes available to its end users consisting of Customer’s applications and the [Microsoft Azure Services](https://www.microsoft.com/licensing/terms/product/Glossary/all), whereby Customer’s application adds primary and significant functionality and is not primarily a substitute to the [Microsoft Azure Services](https://www.microsoft.com/licensing/terms/product/Glossary/all). Customer applications that only provide billing, license management, and/or infrastructure services (e.g., virtual machines, containers, storage, or management for such infrastructure services) do not constitute “primary and significant functionality.”

The definition of “Customer Data” is:

“ **Customer Data** means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data”.

This means that if you build a “*Customer Solution”*, e.g. you have developed or you are licensed to offer an application as a service to end customers, and you use Microsoft Azure Services as your hosting platform, , you are allowed to do so, even though you indirectly share the power of Microsoft Online-services with third parties. But you can only do it when your offering to end customers is the application (SaaS) as such, and not access to Microsoft Azure services disconnected from the SaaS offering (for instance Office 365/allowing end-customer to host its own applications etc). The end-customer does not get its own subscription in this situation, nor administrative access to the Azure tenant.

**Note – if you use Azure as your hosting platform for your services, but the end-customers does actively store own data in the solution, for instance you have a IOT offering that monitors defined data such as radon, then you should focus on understanding Microsoft Customer Agreement in general, and not these additional considerations for SaaS solutions.**

## Benefit and possible risks

When using the hosting exception as your legal basis for “reselling” Microsoft Online Services, the most obvious benefit is that you may set-up a multitenant offering towards your end-users.

Also you do not have to ensure that your end-customers accept Microsoft Customer Agreement and enter into an agreement directly with Microsoft (as is required of you as a CSP). We see that a lot of the large international SaaS providers are choosing this way when offering its own SaaS solutions to end customers.

Not having to mirror Microsoft Customer Agreement towards the end users, may seem appealing, as it will save the individual end customer the “time and trouble” of having to review the agreement and adhere to it (and having a direct contractual relationship with Microsoft). E.g. it may seem as a way to simplify the end-customers contract process.

However, Microsoft Online Service Terms, and the “hosting exception” clearly states that even if you are allowed to “*permit third parties to access and use the Microsoft Azure Services in connection with the use of that Customer Solution”,* you as the Customer of Microsoft and the SaaS provider to your end customer are however “*responsible for that use and for ensuring that these terms and the terms and conditions of Customer’s volume licensing agreement are met by that use”.*

As the “hosting exception” clearly states that you are obliged to, and are responsible for ensuring that your end customers adhere to your obligations as a customer in Microsoft Customer Agreement, you should flow down the same obligations, restrictions and limited warranties, towards your end customers, or you will not be able to ensure compliance with your obligations towards Microsoft etc. At least you will have the financial risk.

## What are the most important risks to mirror:

The most important regulations in Microsofts T&Cs that should be mirrored towards the end customers (and which we assume is the highest risk of breaking) are:

* the **Acceptable Use Policy** in Product Terms (which have prohibitions against illegal content, using the online services for illegal purposed, to spam and distribute malware etc),
* the **Use Restrictions** (don’t reengineer, work around technical limitations, impear Microsofts IPR or share the online services with third parties etc., and
* the **Export Control** regulations,
* Relevant parts of Microsoft **Product terms** - as the end-customers do not get their own tenant in Azure, with administrative privileges, you do not necessarily have to flow down the entire Microsoft T&C’s, Product Terms etc, as the end-customer does not control which services are used, nor which license metrics that are relevant. You should however always review the applicable Product Terms and assess whether:
* specific use limitations for the online-services you plan to use, allows you to host your application in Azure and provide this as a SaaS to your end-customers the way you have planned
* specific use limitations should be mirrored towards end-customers, for instance as part of your subscription fee model, depending on which Online-services you use. For instance, if you as the customer pay per core, how should this be reflected in the pricing against your end-customers if you have a per user subscription fee?

You should as a minimum also consider to mirror or address:

* the **Limited Warranty** Microsoft gives for its Online-services, including limitations of liability, so you are not liable towards your end-customers for errors, defects, downtime etc in the Online-services, which may affect your SaaS services.
* the unilateral right for Microsoft to change or sunset its online-services from time to time, as this may affect the SaaS service towards your end-users
* and possible address towards the end-customers how your SaaS subscription fee may change, if you need to make significant changes in your set-up because Microsoft changes or sunsets parts of the online-services (e.g. leading to significant cost in redesign of your set-up).
* Since you, as a customer of Microsoft, will be liable towards Microsoft for any breach of Microsoft T&C’s made by your own customers, you should also mirror such liability in your end customer agreement, for instance write:

“End Customer agrees to indemnify you against any claim from Microsoft under the Microsoft Customer Agreement, to the extent such claim arises due to end customers failure to adhere to the obligations in the Microsoft Customer Agreement which apply for end-customer”.

* No data processor agreement is established between Microsoft and the individual end-customer with Microsoft. You will therefore have to treat Microsoft as a sub processor in your own DPA towards the end-customers, and to build in appropriate clauses in your own DPA to deal with this.

When you are using Microsoft as such a sub processor, you will as processor need to carry out a risk assessment in accordance with article 32 in the GDPR. The end-customer will, as part of the end-customer’s obligations under the GDPR, have to request this risk assessment from you and include this assessment in the end-customer's own needed risk assessment also in accordance with article 32 in the GDPR.

Since Microsoft often use service technicians and/or provides services from outside EEA without adequacy decision, personal data will most probably be exported to such counties. You must therefore assess whether You or Microsoft is the exporter and the transfer mechanism that will be used, respectively by You and/or Microsoft. You have to decide whether you need to conduct a TIA (Transfer Impact Assessment) or whether it is sufficient that the transfer is evaluated in the risk assessment in accordance with article 32. The end-customers will request information about such assessments from You as part of the end-customer’s own risk assessment in accordance with article 32 in GDPR. Therefor you should:

You should check whether the Azure services used to offer your SaaS offering in fact depend on either transfer of personal data to countries outside of EEA and or countries without adequacy decision, including use of service technicians outside of this area. If so, you should as a minimum inform your end customers so they are aware and so they may make their own assessments and request potential documentation from you.

If you want to be 100% sure that there is no gap between your obligations towards Microsoft and what you mirror against your SaaS end customers, you can mirror the entire Microsoft Customer Agreement (with all additional agreement documents which are linked to therein, such as the SLA and Product Terms etc).

## Is the “Hosting Exception” an ideal model from an end-customer perspective?

The consequence for end-customers, of you being a customer yourself with Microsoft and since the individual end-customer does not establish its own direct agreement with Microsoft is:

* that the end-customer gets no protection from Microsoft in case third party infringement claims. Only the “Customer” is for instance protected under the MS Customer Agreement “against third party claims”, not “third parties” if directly sued such as your end Customers.

**Mitigations to consider:** You should therefore be careful to offer a full indemnity to your end customers for infringement claims related to Microsofts Online services, and state that a condition for such indemnity is that Microsoft protects you and compensates the same towards you.

* As end-customer does not enter into a DPA directly with Microsoft, but Microsoft is handled as a sub processor, end-customers get no protection under the Microsoft data processing agreement for any loss due to breach thereof. Only you as the “Customer” is given the opportunity to claim damages in case of breach by Microsoft of the DPA, and not the end-customer as the controller.

**Mitigations to consider:**  *There are none. This means that if en-customer suffers direct loss, this cannot be claimed from Microsoft (and not from you as a SaaS provider, unless you except such liability after all). Even if you have excepted such liability, this does not prevent end-customer the possibility to claim damages from Microsoft in a GDPR Art 82, nr 5 situation (end-customer is held jointly liable for damages towards data subjects, where both end-customer and Microsoft causes the breach.*

* in addition to this, since you are the Customer in this set-up, and (according to the Hosting exception) since you are “*responsible for that (end customer) use”* and for ensuringthat *“these terms and the terms and conditions of Customer’s volume licensing agreement are met by that use”*, this means that if one of your end customers breaches the Microsoft Customer Agreement (for instance Acceptable Use Policy, Export control or Use Restrictions), this will be considered a breach by you towards Microsoft, and Microsoft may suspend and/or terminate the online-services towards you, and all of your end users. The wording relating to suspension or termination does not distinguish between your different end-customers, but only addresses suspension or termination against you as the one and only customer.

Looking at the wording related to termination for cause, it states that: *”either party may terminate this Agreement on 30 days’ notice for material breach if the other party fails to cure the breach within the 30-day notice period”.* E.g if one of your end-customer breaches Microsofts T&Cs, and fails to cure within the days, this will terminate your agreement with Microsoft, and also affect all other end-customers.

Looking at the wording related to suspension, it states in the Acceptable Use Policy that: *“Violation of the Acceptable Use Policy in this section may result in suspension of the Online Service. If Microsoft suspends the Online Service, Microsoft will suspend only to the extent reasonably necessary. Unless Microsoft believes an immediate suspension is required, Microsoft will provide reasonable notice before suspending an Online Service for the reasons stated above”.* E.g if one end-customer is in breach of the AUP, Microsoft will if the breach has significant impact for Microsoft or the security of the Online-services, suspend your account immediately. This will affect all end-customers, and not only the end-customer in breach. If immediately suspension is not required, you will be notified, and you will hopefully have time to suspend the applicable customer/or allow the applicable end-customer to correct, before Microsoft suspends all services. As Microsoft does not know which end-customers you as a SaaS supplier may have, one cannot rely on Microsoft suspending only the relevant end-customer.

* # risk of **domino effect**.

**Mitigations to consider:** This risk for domino effect, may be assessed by some potential end-customers and be considered as a showstopper, for instance if the SaaS is business critical/important for life and health. You should therefor assess how you can limit the risks in this respect.

As for:

* + **Export control;** always include similar contractual wording in your agreement towards end users, and also make necessary investigations to ensure that end customers use will not be in breach of said regulations (before contracting and during the agreement term).
  + **Use restrictions;** design your SaaS offering so end customer have no possibility to reverse engineer Azure services. E.g do not allow your end-customers access to the Azure portal, design your SaaS offering so it’s protected against unauthorized access, perform penetration testing to verify that appropriate security measures are established and maintained, and also build in protection against “denial of services" attacks in your SaaS offering. Ensure also that end customer is not allowed to share your SaaS offering with third parties that does not use it only for the purpose of the applicable end customers business purpose. The latter should be ensured in your contract with the end-customer.
  + **Acceptable Use Policy,** in order to prevent end customers storing illegal content in Azure, processing content that infringes or violates third party rights, using the online services for illegal purposes or to spam and distribute malware, are using in a way that may harm the Online-services or anyone else’s use of it, or use Azure to host applications where failure in Azure could lead to death or bodily injury etc, you should design the solution so it’s not possible to do the above. For instance, you should to the greatest extent code your application so these actions cannot be done via your SaaS solution, and also design your SaaS so it monitors and detects individual end-customer violations of the above, enabling you to suspend such end-customers as soon as possible in case of breach of the AUP-

This risk for “domino effect” can however also be removed, if you have the opportunity to install the software offered as SaaS, on a unique tenant per end-customer. For instance that you enter into one customer agreement with Microsoft, per end-customer you contract with, which removes the risk of one end-customer breaching Microsoft T&C’s with detrimental effect for you and your other end-customers.

## Is the “Hosting Exception” an ideal model from your perspective av SaaS provider and Customer of Microsoft?

The risks accounted for above, are also risks that on some level applies for you as a SaaS supplier hosting in Azure, and which should be assessed by you.

In addition, you should also review the terms and conditions of the Microsoft Customer Agreement, and assess the general risks therein, and assess how you possible can mitigate them. See our review of Microsoft Customer Agreement for more information and support in such assessment.

## Different ways to use the «hosting exception”:

As the basis for the “hosting exception”, is that you are a customer yourself of Microsoft’s online services, you should also consider under which Microsoft program you should subscribe. There are several different ways/programs to subscribe to Microsoft’s online services as a customer:

- Enterprise Agreement (EA). Can be used when you qualify for this. You need 500 SL’s or more (users and/or devices). Has traditionally been used when buying traditional software licenses, but has for several years also covered online services. Normally you lock the subscription for 3 year periods at the time, and you get pricing based on a scaled volume discount system. You also have a “true-up” once a year, where you add/pay for additional users/devices etc (without an order as such). For software licenses its normally a limited possibility to scale down, while it is to some extent possible for online services once a year. Payment for the committed consumption is upfront in full. The big “minus” with this agreement is that it consists of many different agreement documents, and is highly complex. But if you need to negotiate the terms, this is the program where Microsoft offers this as a possibility. Note that private entities are not allowed any longer to subscribe to Azure services under the EA program, so unless you are an existing EA customer, this alternative is not available (nor upon renewal).

- Government Entreprise Agreement (EA), can be used when you have 250 SL’s or more.

- Microsoft Customer Agreement (MCA) directly with Microsoft (MS Enterprise)

- Microsoft Customer Agreement (MCA) through a reseller (MCA Indirect). The CSP program does not have a 3-year commitment as the EA, but billing is as a main rule done on a month by month basis; e.g its easier to scale up and down, and as a general rule you pay your consumption monthly in arrears (but options are available. Commitment is needed to get good discounts). Your reseller/CSP will bill you and support you in case of incidents, SLA downtime, guide you as to optimizing your consumption/prices etc.

- Microsoft Online Services Agreement (MOSA). Simply register as a customer at Azure.com and enter your credit card. It seems that Microsoft is in process of abandoning this agreement type.

- Others, such as OL (open license), OSV, Select/Select+) are not available for purchase on Online-services.

## Alternative delivery models to the hosting exception

In order to avoid the above-mentioned risks, there is always the possibility to become a Microsoft reseller (and enter into a Microsoft Partner Agreement). In such situation, when you resell Azure services to your end customers, the above mentioned risks disappear, as the individual end-customer and Microsoft will enter into a direct agreement between the parties, including DPA If end-customer is in breach it will only affect such end-customer. You as a reseller are not liable for such breach towards Microsoft.

We assume that the reason why so many SaaS providers in the market are using the “hosting exception” instead of becoming a CSP, is that under the “hosting exception” the Azure tenant will belong to the SaaS provider, and the end-customers will not have one tenant each. Then it is easier to establish a multitenant solution, keeping cost down when mass distributing updates to all end customers at once etc.

When being a CSP, you will need to establish at least one tenant per end-customer (single tenant), and this may add cost in your offering. A benefit however, is that you may also sell other Azure services to the end-customer, than what you need for your own SaaS offering.

Microsoft itself obviously consider the Microsoft Partner Agreement as a possible way for SaaS suppliers to sell Azure services to its end customers as part of the SaaS offering. In the guide to the channel authorization under Microsoft Partner Agreement its stated that:

“Company (that’s you as a reseller) may provision tenants to be dedicated as the “Azure Partner Shared Services” tenants for the purpose of Company’s provisioning shared resources and to host multi-tenant SaaS solutions using Azure”.

It’s also stated that:

“Microsoft grants Company the right to access and use Azure Partner Shared Services for the above purposes and to purchase Azure services for internal consumption.”

As a SaaS provider, you may therefore use the Azure Partner Shared Services to host multi-tenant SaaS solutions, and you may (as a reseller) also purchase the Azure serviced you need. But such Azure consumption will be subject to the terms in Microsoft Customer Agreement. E.g you are bound by the T&Cs as a normal Customer, and it is important that you adhere to such terms and conditions, such as the Acceptable Use Policy, License restrictions, Export control regulations, and any use limitations in the Product Terms etc. You should assess carefully if other obligations are relevant to adhere to as well, depending on which Azure services you use.

An advantage for SaaS providers when becoming a CSP rather than being a Customer, is also that you get access to Microsoft Partner Portal and all the information therein. You are also included in Microsofts partner incentives program, for instance you will get kick-back through the Partner Earned Credits incentive. On the other side, you may as a Saas provider choosing the “hosting exception”, also be given investment funds from Microsoft, that may be used to build the SaaS/Azure combined services. Whether the one vs the other model is best for you, should be investigated further by you, by including Microsoft in the assessment.

A ”downside” of using the CSP model as SaaS supplier, vs using the hosting exception, is that each of your end-customers, also will be a customer and owned by Microsoft. Under the hosting exception, Microsoft does not know the identity of your end-customers.