Questions	Answers
What changes are described in this FAQ?	This FAQ describes changes to the rights Swisscom has to customers' Microsoft Cloud Tenants in the Microsoft Cloud Solution Provider (CSP) programme. Microsoft will make the changes mandatory for all CSP partners worldwide as of January 2023. The aim of the changes is to increase security by reducing rights which Swisscom has as a CSP partner to the Microsoft Cloud Tenants of customers, in line with a "least privilege" model. The changes are therefore relevant for all Swisscom CSP customers.
What do DAP and GDAP stand for?	DAP stands for *Delegated Administrator Privileges*. With the help of DAP, your Microsoft CSP partner can access your Microsoft environment via the role of a global administrator. This gives Swisscom, as a CSP partner, the opportunity to identify problems quickly, qualify solutions and provide assistance rapidly. GDAP stands for *Granular Delegated Administrator Privileges*. Via GDAP, access to a Microsoft environment can be restricted functionally and temporally. This means that Swisscom's customer services only has access to the areas that are needed to resolve the problem.
How does the management of my Microsoft environment via Swisscom function at the moment (*prior to* the switch from DAP to GDAP)?	Swisscom customer services has blanket access to your Microsoft Cloud environment via DAP. This authorisation makes it possible to provide support quickly and efficiently. However, this access is – as described above – broad and very privileged, so the switch to GDAP means an improvement for security.
How will the management of my Microsoft environment via Swisscom function subsequently (*after* the switch from DAP to GDAP)?	Swisscom customer services will only have reduced access rights to your Microsoft Cloud environment, and will be able to support you with troubleshooting and fault repairs in keeping with the reduced rights. This will increase the security of the customer's environment. If these rights are not sufficient for troubleshooting, Swisscom customer services can request higher rights (temporarily). These higher rights become active

	after you have approved them as a Global Administrator on your Microsoft Cloud Tenant.
Which GDAP roles are there, and which are needed for Swisscom to provide efficient customer services?	A wide variety of Azure Active Directory (AAD) roles are available for the different activities that can be performed within a Microsoft environment. In order for Swisscom customer services to support you efficiently, the following GDAP roles are required, which will replace the DAP roles for all customers and be applied by default for new customers: • *Service Support Administrator* : This role has the rights to open/manage support tickets with Microsoft and read service health information. At the moment, only your CSP partner is technically authorised to open support tickets with Microsoft via your customer environment. To do this, Swisscom customer services will need the role *Service Support Administrator*. Without this role, customer services cannot deal with problems or faults that originate within the Microsoft environment. Especially in the case of time-critical errors, Microsoft must be made aware of existing problems as soon as possible, in order to ensure troubleshooting and resolution are not delayed unnecessarily. • *User Administrator :* This role can manage all aspects of users and groups, including password resets for restricted administrators. • *Group Administrator :* This role can manage group settings as well as view group activity and monitoring reports. • *Licence Administrator :* This role has the ability to assign, remove and update licence assignments. For licence bookings and assignments by Swisscom customer services on behalf of the customer, it is important to have these permissions. Furthermore, without

	these permissions, not all activities can be carried out smoothly via the Swisscom Marketplace. • *Global Reader :* This role has the same read permissions as a global administrator, but cannot perform any updates. The Global Reader right allows read access to your Microsoft 365 or Office 365 environment, so that the cause of problems/faults can be identified as quickly as possible. This read role, as the name already shows, has no write permissions and cannot therefore make any changes in the environment. Those with this role are also limited regarding what they can see. E-mail or OneDrive content, for example, cannot be viewed with these rights. • *Directory Readers :* This role can read basic directory information and is often used to grant directory read access to applications and guests. The Directory Reader is required to view a Microsoft Azure subscription so that help can be provided quickly in the event of problems with Microsoft Azure. Furthermore, this role is needed for smooth integration with the Swisscom Marketplace. • *Privileged Authentication Administrator*: This role can perform a password reset for administrators of the customer environment. It is often the case, especially with smaller customers, that the administrator password is no longer known. In order for Swisscom customer services to be able to reset this for you, this role is required. If this role is not available, it will only be possible to restore the administrator password via a very lengthy support

	process with Microsoft. Without access to your admin account, administrative tasks such as creating new users, assigning licences or removing users can no longer be carried out. Because this role is very influential, it is assigned to less than five employees within Swisscom. This is to reduce any possible misuse to an absolute minimum. • *Cloud Application Administrator*: This role can create and manage all aspects of app registration and enterprise apps. This role is needed for smooth integration with the Swisscom Marketplace. Other roles: • For Swisscom managed service customers, depending on the characteristics of the managed service, the Swisscom operating team has different permanent, higher rights. • For the purposes of setting up your customer environment or troubleshooting, Swisscom customer services will usually need higher rights for your environment on a temporary basis. Customer services will send you an individual request with the required roles and the required duration. Only after you have agreed to this can the Swisscom team access the requested areas and provide the service. • On the linked page you will find an overview of all existing Azure AD roles. What's more, Microsoft provides another overview in which the tasks are presented according to the corresponding AAD roles.
How long are the rights granted?	At the moment, GDAP rights can be granted for a period of one to 730 days. After this, renewal must be requested specifically.
When will this switch to GDAP take place?	If you currently have an existing DAP relationship with Swisscom, the move to the GDAP role as described above will probably take place by the

	end of 2022. This will ensure that your access will continue to run under the best possible security concept, and that customer services can be there for you with the expected level of quality. After that, the GDAP roles will be applied directly for new Swisscom CSP customers.
What happens if I don't want to switch to GDAP?	Microsoft has announced that it will remove inactive DAP relationships (not in use for more than 90 days) by the end of January 2023. This would mean that Swisscom customer services would no longer have any permissions. For example, it would then no longer be possible to open support tickets with Microsoft via Swisscom. This would also mean that in the licence ordering portal, the Swisscom Marketplace, not all of the activities could be carried out. For this reason, Swisscom will automatically switch existing DAP roles to the role set described above. This increases security for your environment and allows Swisscom to continue to provide service.
I have already removed the DAP relationship. Will I now be switched to GDAP?	No, that won't happen. The switch to GDAP requires an existing DAP relationship. You can, however, also benefit from GDAP without a DAP relationship. Swisscom can create a GDAP request if required, which you must confirm in the Microsoft 365 Admin Center. The recommendation is to approve a minimum set of roles to ensure smooth customer service and bookings via the Swisscom Marketplace (see the roles above). However, decisions regarding what access is granted to your environment and to whom this access is granted are made solely by you.
Can I use GDAP to remove the Foreign Principal role of Swisscom from my Microsoft Azure subscription?	No. This role is still a prerequisite for obtaining Microsoft Azure via Swisscom and is a role on Azure that is controlled separately, and which has nothing to do with the Azure Active Directory based roles (GDAP). The fact that this Azure role is still needed is related to Microsoft's current product model. Removal of this role will result in termination of your Azure subscription(s) by Swisscom. This rule is also laid down in our contract conditions.

How can I view and manage access authorizations from Swisscom customer services or other CSP partners?	To view the up-to-date status of access authorization for your Microsoft environment, log in to the Microsoft 365 Admin Center with your administrator account. There you can view and manage the authorization you have granted on the left-hand side under the tab "Settings" > "Partner relationships". Please note: Before withdrawing permissions at this point, please consider the potential consequences for booking possibilities as well as the provision of Swisscom customer services. Each request for access authorization is created by your CSP partner, you cannot initiate it yourself. Via the link sent by your partner, you can approve a new GDAP relationship in your Microsoft 365 Admin Center.
What other security measures make sense to protect my Microsoft environment?	With Azure Active Directory and the security features of Microsoft 365, you can enable basic security measures such as multi-factor authentication (MFA, we recommend this for all employees) or conditional access policies to better secure your employees' access. Furthermore, it is possible to purchase additional solutions from Microsoft, for example the Defender family. These offer advanced features for better security. Recommendations for security configurations from the US Department of Homeland Security can be found here: https://www.us-cert.gov/ncas/analysis-reports/AR19-133A What's more, Swisscom's experts (and those of our partners) will support you in all matters relating to the security of your ICT environment, for example in the implementation of security settings for Microsoft security functions.