dsb

datenschutzbeauftragte
kanton zürich

Guide

Microsoft 365 pour le domaine de l'éducation

Inhalt

1 Introduction

Ce guide s'adresse aux écoles primaires, aux écoles secondaires supérieures et aux établissements d'enseignement supérieur qui souhaitent utiliser Microsoft 365. Il donne un aperçu des procédures, des clarifications préliminaires et des mesures qui doivent être mises en œuvre avant et dans le cadre de l'utilisation des services afin de garantir une utilisation conforme à la protection des données. Il a été tenu compte des risques particuliers liés à l'utilisation du nuage pour le traitement des données et des mesures spéciales qui doivent être mises en œuvre lors du traitement de données sensibles, c'est-à-dire des données personnelles spéciales.

2 Contrat-cadre / déclaration d'adhésion

2.1 Contrat-cadre

educa.ch a signé un contrat-cadre avec Microsoft pour l'utilisation de Microsoft 365 dans les écoles primaires et secondaires ainsi que dans les écoles secondaires supérieures et SWITCH un accord-cadre avec Microsoft pour l'utilisation de Microsoft 365 dans les hautes écoles. Elle règle les aspects juridiques tels que le droit suisse applicable et le for juridique suisse. Microsoft s'engage à stocker les données dans les pays européens, à savoir l'Irlande et les Pays-Bas.

Chaque école souhaitant utiliser ces services doit également signer une déclaration d'adhésion. L'enregistrement direct par les élèves disposant d'une adresse électronique scolaire pour utiliser Microsoft 365 sans signer les contrats correspondants n'est pas conforme à la réglementation sur la protection des données.

2.2 Déclaration d'adhésion des écoles primaires et secondaires de niveau II

Pour les établissements d'enseignement couverts par l'contrat-cadre educa.ch, la déclaration d'adhésion se fait par la signature d'un contrat de licence en volume Microsoft, disponible auprès du partenaire éducatif agréé Microsoft responsable de l'établissement. L'école doit indiquer explicitement qu'une déclaration d'adhésion est souhaitée par l'utilisation du contrat-cadre educa.ch, faute de quoi les conditions cadres spéciales de protection des données n'entreront pas en vigueur.

2.3 Déclaration des universités membres

Pour les établissements d'enseignement supérieur tels que les universités, les hautes écoles pédagogiques et les hautes écoles spécialisées, le document « Accord de Mise en OEuvre de Solutions Éducation » doit être signé par Microsoft, y compris le contrat-cadre. Un partenaire agréé Microsoft Licensing Solution Partner en est responsable.

3 Concept pour l'utilisation de Microsoft 365

Avant d'utiliser les services, il convient d'élaborer un concept qui inclut tous les points essentiels concernant le traitement futur des données, en particulier

- le type d'utilisation
- le produit adapté au type d'utilisation
- la nature et l'étendue des données à traiter
- les responsabilités
- les mesures à mettre en œuvre pour protéger les données, telles que l'accès, le cryptage, etc.

3.1 Type d'utilisation

Avant de choisir les produits, l'école ou la direction de l'école doit décider à quelles fins elle souhaite utiliser les services ou quelles tâches scolaires elle doit effectuer. Par exemple, ne devrait-on sauvegarder que les feuilles de travail ou les élèves devraient-ils être capables de faire leurs devoirs ? Il est à noter que c'est le but qui détermine la sélection et non l'inverse.

3.2 Choix des services

Microsoft 365 fournit une gamme de services (voir point 9). Le choix dépend des besoins de l'école. Il convient de noter que seuls les services couverts par le ontrat-cadre peuvent être utilisés pour le traitement des données à caractère personnel (voir points 9.1 et 9.2).

3.3 Sélection et classification des données

L'école doit déterminer à l'avance pour chaque service sélectionné quelles données doivent être traitées. Tout ce qui est possible n'est pas permis. Le traitement des données doit dépendre des tâches et des finalités éducatives. Il convient de veiller à ce que seules les données nécessaires à la tâche et à la finalité respectives soient traitées.
Le comportement d'apprentissage ne doit pas être surveillé et évalué. Des exceptions sont possibles, par exemple si le produit est utilisé pour un travail de groupe noté.

Les données doivent être classées dans les catégories suivantes afin de déterminer les mesures de protection appropriées :

données factuelles	Informations non liées à des personnes Exemple : Fiches de travail
données à caractère personnel	Informations relatives à des personnes identifiées ou identifiables Exemple : Nom, prénom, adresse
Données personnelles spéciales	Informations qui, en raison de leur importance, de la nature de leur traitement ou de la possibilité qu'elles soient liées à d'autres informations, présentent un risque particulier de violation de la personnalité Exemple : Résultat de l'examen du médecin de l'école ou de l'examen de clarification psychologique à l'école

3.4 Sécurité de l'information

L'école doit mettre en œuvre des mesures techniques et organisationnelles pour garantir la confidentialité, l'intégrité, l'authenticité et la disponibilité des données. Plus les données sont sensibles, plus les mesures de sécurité de l'information sont complètes. Cela vaut en particulier pour les données soumises au secret professionnel (voir point 4). En particulier, les points suivants sont pris en compte.

3.4.1 Chiffrement de données personnelles spéciales

Les données personnelles sensibles, c'est-à-dire spéciales, doivent être cryptées (document en allemand). Le transport ainsi que le stockage des données sont déjà cryptés avec Microsoft 365, dont Microsoft a la clé. Pour d'autres options de cryptage avec protection supplémentaire, voir section 4.

Lorsque des informations quittent Microsoft 365, par exemple lors de l'envoi de courriels, les mécanismes de cryptage suivants sont disponibles. Ils peuvent faire l'objet de frais. Le chiffrement peut avoir lieu au niveau du document ou au niveau de l'environnement Microsoft 365 (locataire) :

- Document : cryptage du fichier Office (Word, Excel, OneNote ou Powerpoint) lui-même ou utilisation d'une archive 7-Zip

3.4.2 Enregistrement

Lors de l'utilisation des services, les données relatives aux utilisateurs et à leurs activités peuvent être collectées et stockées automatiquement. C'est ce qu'on appelle l'enregistrement. Cependant, cette fonction doit être activée par l'école.
Les données du protocole ne peuvent être traitées que si cela est nécessaire au fonctionnement du système. En cas de soupçon de mauvaise utilisation des services par les utilisateurs, les données du protocole peuvent être évaluées de manière aléatoire et après information préalable des personnes concernées.

Renseignements supplémentaires
- Rechercher dans le journal de surveillance de Microsoft 365 Security & Compliance Center

3.4.3 Authentification et mots de passe

Microsoft 365 offre essentiellement trois types d'authentification :

- Utilisation de l'authentification Microsoft 365 intégrée
- Synchronisation du mot de passe de l'Active Directory interne à Microsoft 365 (ou Azure AD)
- Utilisation d'un service interne Active Directory Federation Service (ADFS)

Le type d'authentification est déterminé dans le cadre d'une analyse des risques. La finalité et l'étendue du traitement des données ainsi que le type de données traitées sont pris en compte.

L'authentification à deux facteurs est requise pour les administrateurs ou lorsqu'il s'agit de données personnelles spéciales. Celle-ci peut être activée dans Microsoft 365 et est gratuite pour les produits Microsoft 365. Les étapes nécessaires sont expliquées ici. Toutefois, la procédure TAN ou les mots de passe uniques peuvent également être utilisés.

Les mots de passe ne doivent pas être visibles en texte clair et doivent être changés et chiffrés régulièrement.

Renseignement supplémentaires
- Synchronisation et authentification d'identité Microsoft 365
- Intégration dans Azure Active Directory

3.4.4 Rôle et concept d'autorisation

Avant l'utilisation, l'école doit définir par écrit dans un concept de rôle et d'autorisation quels groupes de personnes (enseignants, élèves, spécialistes, psychologues scolaires, concierges, directeurs, administrateurs, administrateurs de cours, etc.) peuvent accéder à quels services et à quelles données. Le rôle et le concept des autorisations doivent être vérifiés régulièrement.

Si la case postale client est activée, le responsable doit être enregistré dans le concept des autorisations (voir ch. 4).

3.4.5 Supprimer

La suppression des documents s'effectue de la même manière que pour la version papier. Les enseignants ou autres personnes responsables de la suppression peuvent eux-mêmes supprimer ou demander aux élèves de supprimer les répertoires ou documents concernés après les délais applicables à l'école ou de les transférer sur d'autres supports de stockage. Ce processus peut être automatisé. L'automatisation peut être simple ou définie de manière très approfondie. L'administrateur peut, par exemple, déterminer pour l'ensemble de l'école que tous les documents sont supprimés après une certaine période s'ils ne sont pas explicitement prolongés par les enseignants.

Les données des élèves ou des enseignants qui n'utilisent plus leur compte doivent être supprimées par l'école.

Les données du protocole sont supprimées automatiquement. La période de stockage est de 90 jours.

Renseignements supplémentaires
- Conservation, suppression et destruction des données dans Microsoft 365

3.4.6 Synchronisation des données utilisateur avec Microsoft 365

Pour diverses raisons, comme l'activation de la licence Microsoft 365, les données doivent être synchronisées avec Microsoft 365. En cas de synchronisation, seules les données utilisateur nécessaires à l'utilisation de Microsoft 365 doivent être transmises. Un filtrage correspondant doit être effectué dans le service de synchronisation.

Renseignements supplémentaires
- Azure AD Connect Synchronisation : Configuration du filtrage

3.4.7 Sauvegarde des données et planification d'urgence

Les exigences relatives à la disponibilité de Microsoft 365 sont définies. Si nécessaire, des mesures appropriées de sauvegarde des données et de planification d'urgence doivent être mises en œuvre.

3.4.8 Données de diagnostic Microsoft 365 Proplus

Lorsque Microsoft 365 Proplus est utilisé localement sur l'ordinateur, il y a, selon l'option sélectionnée, transmission de données à Microsoft. C'est pourquoi l'administrateur doit mettre en œuvre les mesures de protection des données correspondantes. Cela signifie en particulier qu'il faut :

- utiliser en permanence la version actuelle de Microsoft 365
- activer l'option « ni ni » pour les données de diagnostic
- configurer et désactiver si possible du point de vue central les expériences liées à l'option
- désactiver la participation au programme d'amélioration de la facilité d'utilisation (Microsoft Customer Experience Improvement Program, CEIP)

4 Données couvertes par le secret professionnel

Les informations concernant les médecins scolaires et les psychologues scolaires sont soumises au secret professionnel. Ces données sont protégées par le droit de la protection des données ainsi que par le droit pénal. Elles ne doivent pas ou seulement dans des circonstances particulières être portées à la connaissance de tiers, c'est pourquoi les points suivants doivent être pris en compte en plus des mesures énumérées au point 3.

4.1 Accès aux données avec consentement

Lors de l'utilisation des services Microsoft 365, le cryptage de base est implémenté pour le transport et le stockage. Cependant, Microsoft a la clé. Par conséquent, le processus « Customer Lockbox » doit être activé. Microsoft ne peut ainsi accéder aux données que sur demande explicite et avec le consentement explicite de l'administrateur dans les cas de support.

Customer Lockbox est un service payant. Le responsable de ce processus doit être enregistré dans le concept de rôle et d'autorisation.

4.2 Chiffrement avec sa propre clé

Les écoles qui ont une certaine taille, une infrastructure informatique appropriée ou un savoir-faire technique peuvent implémenter leur propre clé (Bring Your Own Key) pour les données dans Microsoft 365.
Cette clé est gérée par Microsoft dans un coffre à clés (Azure Key Vault). Pour cette raison, le processus «Customer Lockbox» doit également être activé (voir paragraphe 4.1). Les phrases de passe et les paires de clés utilisées doivent être générées et stockées en toute sécurité.

5 Adresses électroniques

Si des adresses électroniques doivent être attribuées, il convient d'utiliser des noms abrégés ou des pseudonymes. Les pseudonymes compliquent l'abus de comptes par des tiers.
Si la pseudonymisation ne peut pas être effectuée par l'utilisateur, des tiers externes proposent des solutions pour utiliser Microsoft 365 avec un pseudonyme. Lors de l'utilisation d'un tel service, les aspects de l'externalisation doivent également être pris en compte.

6 Sélection de pays

Lors de l'utilisation de services individuels, une sélection de pays doit être effectuée. Les lieux de stockage doivent être choisis de manière à ce que les données ne soient stockées que dans des pays disposant d'une réglementation adéquate en matière de protection des données, c'est-à-dire de préférence en Suisse ou en Europe. Vous trouverez ici un aperçu des emplacements de stockage.

7 Formation et sensibilisation

Toutes les personnes qui traitent des données avec ces services doivent être informées de la façon dont chaque service peut et doit être utilisé. Les élèves doivent être informés exhaustivement de la façon dont l'école travaille avec Microsoft 365 et de la façon dont ils peuvent légalement l'utiliser.

8 Information pour les parents

Dans un souci de transparence, les parents doivent être informés de ce nouveau type de traitement des données dans le cadre de l'école primaire. D'une part, il est possible de tirer des conclusions sur les élèves sur Internet, par exemple au moyen d'adresses électroniques qui relient le nom à l'école, et d'autre part, les élèves utilisent également Internet pour l'école à la maison.

9 Annexe – aperçu des services de Microsoft 365

9.1 Services fournis par Microsoft 365 au titre des contrats-cadres

Service	Description	Alternatif local
Delve	Analyse et visualise son propre usage et apporte au sein de Microsoft 365 des informations et des documents intéressants pour les utilisateurs.	
Exchange Exchange Online	Courriel, Calendrier, Contacts, Tâches	x
Flow	Outil d'automatisation des processus métier pour créer des workflows automatisés entre applications et services, afin de recevoir des notifications, synchroniser des fichiers, saisir des données, etc.	
Forms	outil de formulaire Exemple : contrôle d'apprentissage ; indique ce qui ne va pas.	
Groups	Permet de former des groupes d'utilisateurs avec lesquels partager les différents services.	
OneDrive for business	Stockage de documents personnels pour vos propres documents	x
OneNote	bloc-notes Exemples : Préparation des leçons, tableau noir électronique, etc.	x
Notes de cours OneNote	Le cahier de notes de cours OneNote offre des fonctions supplémentaires à OneNote. Exemples : Distribuer des feuilles de travail aux élèves, correction des devoirs, etc.	
Planner	Outil de travail en équipe pour des tâches telles que la création de plans, l'organisation et l'assignation de tâches, la libération de fichiers, la discussion de tâches en chat et l'échange d'informations.	
Powerapps	Permet la création d'applications professionnelles personnalisées	
PowerBI	Business Intelligence Ensemble d'outils d'analyse et de visualisation des données stockées sur SharePoint et de partage des résultats.	

Project, Project on line	Outil complet de gestion de projet	x
School Data Sync	School Data Sync est un service Microsoft 365 pour les établissements d'enseignement qui lit les listes des écoles et des services à partir du système d'information des élèves d'une école. Il crée automatiquement des groupes Microsoft 365 pour Exchange Online et SharePoint Online, Class Teams for Microsoft Teams et OneNote Class notebooks.	
SharePoint, SharePoint on line	Emplacement de stockage pour les documents partagés avec d'autres utilisateurs dans des groupes prédéfinis (voir « Groups »).	x
Skype for Business	Chat, téléphonie, visioconférence, partage de l'écran et des applications, etc. L'appel téléphonique n'est pas sauvegardé, seulement le chat (sur le serveur Exchange). Les appels vidéo peuvent être enregistrés et transférés vers SharePoint.	x
Stream	Plate-forme vidéo interne de l'école : enregistrer, parcourir, partager des vidéos	
Teams	Environnement de travail basé sur le chat dans Microsoft 365 Consolidation des services Microsoft 365, avec un accent particulier sur l'interaction en équipe Exemple : combinaison de Skype, SharePoint et OneNote	
To-Do	To-Do est intégré à Microsoft 365 et aide à la gestion des tâches, organisant la routine quotidienne.	

9.2 Autres services au titre des contrats-cadres

Service	Description
Azure Cloud Plattform	Infrastructure as a Service (IaaS) : Machines virtuelles, mise en réseau, stockage Plate-forme as a Service (PaaS) : banques de données, Intelligence and Analytics Software as a Service (SaaS) : Applications d'entreprise
Dynamics 365	Customer Relationship Management (CRM) et Enterprise Resource Planning (ERP) Service de gestion des ressources telles que la comptabilité, la gestion d'entrepôt, les employés, les apprentis, les contrats, etc. Exemple : Aperçu du moment où les clients ont appelé.
EMS E3 for Intune	Composant pour le contrôle des identités et des accès dans le cloud, la gestion des appareils mobiles et des applications Exemple : assurer que tous PC de l'école sont à jour et sont protégés contre tout accès non autorisé.
Intune	Gestion des applications et des périphériques Fait partie de la suite Enterprise Mobility Suite (EMS)
Intune for Education	Intune for Education offre une interface utilisateur simplifiée par rapport à Intune. Il peut être utilisé indépendamment ou en combinaison avec l'environnement complet disponible dans Intune pour la gestion des périphériques.

9.3 Services non couverts par des contrats-cadres

Les services suivants ne peuvent pas être utilisés conformément aux dispositions relatives à la protection des données. Ils stockent notamment tout ou partie de leurs données en dehors de l'UE.

service	Description
OneDrive (Consumer Version)	Stockage de documents pour les documents privés Les écoles ne peuvent utiliser que OneDrive for Business pour un référentiel de documents conforme à la protection des données (voir 9.1).
Skype (Consumer Version)	Communication : chat, téléphonie, partage d'écran, etc. Les écoles ne peuvent utiliser que Teams ou Skype for Business comme outil de communication conforme à la confidentialité (voir 9.1).
Sway	Outil de création de présentation en ligne qui fonctionne comme un site web.
Yammer	Médias sociaux pour les entreprises

dsb

datenschutzbeauftragte
kanton zürich

Datenschutzbeauftragte
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh