



dsb

datenschutzbeauftragte
des kantons zürich

Guide

Google Workspace for Education

Contenu

1	Introduction	2
2	Contrats cadres avec Google	2
3	Concept	2
3.1	Genre d'utilisation.....	2
3.2	Sélection des services et des pays.....	3
3.3	Sélection et classification des données.....	3
3.4	Sécurité de l'information.....	3
3.4.1	Chiffrement de données personnelles spéciales.....	3
3.4.2	Enregistrement.....	4
3.4.3	Authentification et mots de passe.....	4
3.4.4	Rôle et concept d'autorisation.....	4
3.4.5	Supprimer.....	5
3.4.6	Synchronisation des données d'utilisateur.....	5
3.4.7	Sauvegarde des données et planification d'urgence.....	5
4	Secret professionnel	5
5	Adresses électroniques	6
6	Formation et sensibilisation	6
7	Information pour les parents	6

1 Introduction

Ce guide s'adresse aux établissements de l'éducation qui veulent utiliser Google Workspace for Education. Il donne un aperçu de la procédure à suivre pour garantir l'utilisation conforme à la protection des données.

2 Contrats-cadre avec Google

Educa a signé avec Google un contrat-cadre pour l'utilisation de Google Workspace for Education dans les écoles primaires et secondaires, les écoles du degré secondaire II ainsi que dans la formation professionnelle supérieure. Les critères de participation convenus par contrat sont applicables. Les licences pour Google Workspace for Education sont disponibles exclusivement via des revendeurs autorisés par Google. Les informations sur le contenu du contrat et les conditions d'acquisition peuvent être consultées sur la [page internet d'Educa](#).

SWITCH a conclu un contrat-cadre pour les établissements des hautes écoles universitaires comme les universités, les hautes écoles pédagogiques et les hautes écoles spécialisées. Afin d'utiliser les services du contrat-cadre de SWITCH et par conséquent conformément à la protection des données, il faut signer le formulaire «Google Workspace Affiliate Order Form», disponible via l'adresse procurement@switch.ch. Une fois rempli et retourné à SWITCH, le formulaire est transmis à Google et le service est activé.

Les hôpitaux universitaires et les instituts de recherches comme sous-domaine d'une haute école peuvent également adhérer au contrat-cadre.

La référence aux contrat-cadre permet une utilisation conforme à la protection des données par

- l'applicabilité du droit suisse,
- un for suisse,
- la sélection du lieu d'enregistrement des données (UE/non UE).

Les contrats-cadre ne règlent que l'utilisation de Google Workspace for Education Plus. La version gratuite de Google Workspace for Education Fundamentals ne peut pas être utilisée conformément à la protection des données.

3 Concept

Avant l'utilisation des services, il convient d'élaborer un concept qui tient compte en particulier des points suivants :

- le type d'utilisation
- le produit adapté au type d'utilisation
- le genre et l'étendue des données à traiter
- les responsabilités
- les mesures à mettre en œuvre pour la protection des données comme les accès, le chiffrement, etc.

3.1 Genre d'utilisation

Avant de choisir les produits, les établissements d'éducation doivent décider à quelles fins ils souhaitent utiliser les services ou quelles tâches scolaires ils doivent 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 Sélection des services et des pays

Google Workspace for Education Plus met à disposition une série de services. Le choix se base sur les besoins des établissements d'éducation. D'autres descriptions du produit sont disponibles ici.

Les dispositions contractuelles ne sont applicables qu'aux services principaux de Google Workspace, par ex. Gmail, calendrier Google et Google Classroom. Les écoles doivent déterminer à quels services les élèves ont accès. Il convient de noter que lorsque d'autres services comme Youtube etc. sont utilisés via Google Workplace, les conditions générales d'utilisation et de protection des données de Google sont de nouveau applicables.

[Google Workspace for Education Plus permet de sélectionner le lieu d'enregistrement des données \(UE/non UE\). Il convient de sélectionner l'UE.](#)

3.3 Sélection et classification des données

L'établissement d'éducation doit déterminer à l'avance pour chaque service sélectionné quelles données doivent être traitées. Le traitement des données doit dépendre des tâches et des finalités légales. Il convient de veiller à ce que seules les données nécessaires à la tâche et à la finalité respectives soient traitées. Il n'est pas permis de traiter ou d'évaluer le comportement d'apprentissage dans le sens d'une surveillance.

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 personnelles	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 : Résultats de l'examen du médecin scolaire, certificat médical

3.4 Sécurité de l'information

L'établissement d'enseignement 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 doivent être complètes. Cela vaut en particulier pour les données soumises au secret professionnel (voir point 4). En particulier, les points suivants doivent être 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 Google Workspace for Education, dont Google a la clé. Pour des mesures supplémentaires, voir point 4.

Lorsque des informations quittent Google Workspace for Education, par exemple lors de l'envoi de courriels, le mécanisme de cryptage 7-Zip-Archiv peut être utilisé.

Il est également possible d'envoyer des courriels en mode «confidentiel» afin de garantir un cryptage de bout en bout et une transmission exclusive aux personnes concernées. Voir sous ([Protéger les messages Gmail grâce au mode confidentiel – Google Workspace Admin Help](#))

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 ou «Log». 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.

Autres informations

- [Audit-Log sur les activités de connexion](#)

3.4.3 Authentification et mots de passe

Google Workspace for Education offre essentiellement trois types d'authentification :

- Utilisation de l'authentification intégrée
- Synchronisation du mot de passe de l'Active Directory interne à Google Workspace for Education (voir ch. 3.4.6)
- Utilisation d'un service interne d'authentification (par exemple Active Directory Federation Service). Informations supplémentaires : [installation d'une connexion unique fédérée \(SSO\) avec SAML](#).

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 est gratuite et peut être activée dans Google Workspace for Education. Les étapes nécessaires sont expliquées [ici](#).

Il s'agit aussi de vérifier si l'accès et l'utilisation des services Google Workspace ne sont possibles que dans certaines conditions (appelées contexte) et à partir de certains types d'appareils et de configurations. Ce serait par exemple le cas si l'accès n'était possible qu'à partir d'appareils mis à disposition par l'école. On peut ainsi s'assurer que les appareils utilisés répondent aux exigences minimales en matière de sécurité, comme la protection par mot de passe ou par code PIN ou le cryptage local. Voir sous [Présentation de l'accès contextuel – Google Workspace Admin Help](#).

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) ont accès à quels services et quelles données. Le rôle et le concept des autorisations doivent être vérifiés régulièrement.

3.4.5 Supprimer

La suppression de documents se fait 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.

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

Les données du protocole sont supprimées automatiquement. La période de stockage pour la plupart des données se monte à 180 jours, exception faite des rapports suivants :

- recherche dans les protocoles de courriels (30 jours)
- téléchargement de données d'utilisation d'entités depuis l'API (30 jours)
- téléchargement de données d'utilisation de clients/utilisateurs depuis l'API (15 mois)

Informations supplémentaires

- [Conservation des données et délais - les données sont enregistrées pendant combien de temps ?](#)

3.4.6 Synchronisation des données d'utilisateur

Pour diverses raisons, par exemple l'efficacité de l'établissement de l'utilisateur, les données doivent être synchronisées avec Google Workspace for Education (noms d'utilisateurs, adresses électroniques, etc.). En cas de synchronisation, seules les données utilisateurs nécessaires à l'utilisation de Google Workspace for Education doivent être transmises. Un filtrage correspondant doit être effectué dans le service de synchronisation.

Informations supplémentaires

- [Informations sur Google Cloud Directory Sync](#)
- [Synchroniser les données d'un établissement d'éducation avec Google Workspace for Education](#)

3.4.7 Sauvegarde des données et planification d'urgence

Les exigences relatives à la disponibilité doivent être définies. Les mesures de sécurité appliquées par Google à Google Workspace sont documentées sous le lien suivant :

https://workspace.google.com/intl/fr/security/?secure-by-design_activeEl=data-centers

Si nécessaire, des mesures supplémentaires de sauvegarde des données et de planification d'urgence doivent être mises en œuvre.

4 Secret professionnel

Les informations couvertes par le secret professionnels comme les données relevant du médecin scolaire jouissent de la protection du droit pénal en sus de la protection des données. Ces données ne doivent pas ou seulement dans des circonstances particulières être portées à la connaissance de tiers, raison pour laquelle les points suivants doivent être pris en compte en plus des mesures énumérées au point 3.

Lors de l'utilisation des services de Google Workspace for Education, le cryptage de base est implémenté pour le transport et le stockage. Les données sont cryptées par le «Key Management Service» (KMS) de Google ([Google Cloud Whitepaper](#), page 6). Dans ce cas, Google gère toutes les clés.

Pour les données soumises à des obligations de secret particulières, il convient par conséquent d'implémenter l'utilisation d'un cryptage supplémentaire côté client avec contrôle de la clé côté client. Cela permet de garantir que les données ne peuvent pas être consultées ou utilisées par Google ou des tiers sans une libération explicite de la clé par l'école.

Voir sous [À propos du chiffrement côté client](#)

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.

6 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 sur le genre de traitement par chaque établissement.

7 Information pour les parents

Dans un souci de transparence, les parents ayant des enfants à l'école obligatoire doivent être informés de ce nouveau type de traitement des données, notamment sur les points suivants :

- utilisation de Google Workspace for Education dans les conditions du contrat-cadre d'educa.ch
- services utilisés
- données traitées avec ceux-ci
- conditions applicables aux élèves en-dehors de l'école.

D'une part, des conclusions peuvent être tirées sur les élèves sur internet, par exemple via des adresses électroniques, qui relient les noms à l'école. D'autre part, les élèves utilisent internet pour l'école à la maison.

Traduction du «Leitfaden Google Workspace for Education»; V 2.0 / Juin 2022