Kanton Bern
Canton de Berne

Direction de l'instruction publique et de la culture
Office des écoles moyennes et de la formation professionnelle

Protection des données lors de l'utilisation du cloud

Lignes directrices pour le corps enseignant du degré secondaire II

Date de modification	30 septembre 2021
Version	1
Statut du document	réceptionné
Classification	non classifié
Auteur-e	Equipe du projet sous la direction de Lukas Ritter, gibb
Nom de fichier	Leitfaden_Datenschutz_Cloudnutzung_V1_fr.docx

Table des matières

1 Objectif du document

Les descriptions suivantes s'appliquent à la classification et à la gestion, par le corps enseignant du degré secondaire II, des données contenues dans les services de cloud.

1.1 Contexte et objectif

1.1.1 Contexte

- Le travail avec des outils électroniques pose des exigences élevées en matière de sécurité de l'information et de gestion des données.
- Les utilisateurs et utilisatrices recourent à leurs propres supports TIC et travaillent avec ces supports dans des réseaux à l'extérieur mais aussi à l'intérieur de leur propre infrastructure TIC.
- L'ensemble des dispositions légales et impératives relatives à la protection des données doivent être respectées.

1.1.2 Objectif

Les informations et les systèmes des écoles du degré secondaire II, de leurs clients et clientes, des partenaires et du personnel sont gérés de manière à ce que :

- la confidentialité soit assurée là où cela est nécessaire,
- les capacités requises soient garanties,
- les conditions légales et contractuelles soient respectées.

1.2 Termes et abréviations utilisés

Terme	Définition	Abréviation
Approche AVEC	« Apportez votre équipement personnel de communication »	AVEC
Technologies de l'information et de la communication	Transcription de l'anglais « information and communication technologies » (ICT), est une expression, principalement utilisée dans le monde universitaire, pour désigner le domaine de la télématique, c'est-à-dire les techniques de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications qui permettent aux utilisateurs et utilisatrices de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre l'information sous différentes formes : texte, musique, son, image, vidéo et interface graphique interactive (IHM). [1]	TIC

1.3 Autres informations sur ce thème

- Ligne directrices sur la protection des données personnelles dans les écoles du canton de Berne[2]
- Datenschutz.ch[3] – site Internet des personnes déléguées à la protection des données du canton de ZH
- Educa.ch – contrats-cadre

[1] Source : wikipedia

[2] https://www.erz.be.ch/erz/fr/index/kindergarten_volksschule/kindergarten_volksschule/ict_an_den_schulen.assetref/dam/documents/ERZ/AKVB/fr/09_Schulleitungen_Lehrpersonen/sl_lp_Unterlagen_datenschutz_leitfaden_f.pdf

[3] www.datenschutz.ch

2 Conditions générales

2.1 Conditions cadre

Les présentes lignes directrices portent uniquement sur les plateformes et les services qui ont fait l'objet d'un contrat-cadre entre educa, l'agence spécialisée mandatée par la Confédération et les cantons, et le prestataire correspondant. Il s'agit à l'heure actuelle des prestataires privés suivants :

Editeur/trice	Produit
Adobe	Creative Cloud K12
Google	G Suite for Education
Microsoft	Microsoft 365 for Education
Univention	UCS

Educa a conclu avec ces prestataires privés des contrats-cadre qui créent les conditions permettant aux institutions de formation d'utiliser ces produits en conformité avec le droit. L'aspect suivant figure au premier plan :

- Les conditions contractuelles sont soumises à la juridiction suisse et constituent les bases pour une utilisation conforme au droit.

Cette façon de procéder apporte aux écoles une plus grande sécurité juridique et permet de réduire les risques que comporte l'utilisation de services numériques. Néanmoins, un contrat-cadre ne libère pas les écoles de leur responsabilité d'examiner si les conditions qui y sont convenues correspondent aux exigences du droit cantonal, compte tenu des utilisations prévues pour les écoles.[4]

2.2 Classification des informations

- Tous les propriétaires d'informations sont toujours responsables du contenu des informations qu'ils transmettent.
- Ils sont également responsables de la classification correcte de leurs informations vis-à-vis des utilisateurs et utilisatrices.
- La classification se fait par échelons, en fonction des besoins de protection et des conditions de protection qui en découlent.

[4] https://www.educa.ch/fr/activites/contrats-cadre/informations-pour-les-ecoles

2.3 Echelons de classification et gestion des données et informations contenues dans les services de cloud

Echelon	Mention	Description	Sauvegarde	Partage avec le groupe cible	• **Exemples** (listes non exhaustives)
public	Non	Publication sur Internet, dans le cloud ou sur d'autres plate-formes de partage d'informations	Avec authentification simple	Tous	• Horaire, calendrier des vacances • Informations générales sur l'école • Procès-verbaux de groupe d'experts (sans données personnelles) • Préparation des cours • Fiches de travail (sans données personnelles) • Communication destinée au public (manifestation scolaire, etc.)
confidentiel	Oui	Informations non liées à la personne	Cryptage et authentification simple	Personnes impliquées et personnes concernées	• Procès-verbaux de la direction d'école • Communication relative à des personnes, sans contenus d'ordre psychologique ou médical • Procès-verbaux (sans données personnelles) • Examens (non remplis)

Données personnelles (informations en lien avec l'organisation concernant une personne)	Oui	Nom, prénom, adresses, numéro de tél., date de naissance, etc.	Cryptage et authentification simple [5]	Personnes impliquées et personnes concernées (en général le corps enseignant de la classe et l'administration)	• Listes de classe
					  ○ Numéros de téléphone des élèves
					  ○ Liste des absences (sans motifs)
					  ○ Adresses des élèves
					• Aperçu des notes (sans remarques sur les élèves)

				Personnes impliquées et personnes concernées (en général la classe)	• Photos et vidéos (permettant de reconnaître des personnes)
				Personnes impliquées et personnes concernées (en général le corps enseignant et l'administration)	• Procès-verbaux (avec des contenus d'ordre général sur des élèves)
Données personnelles particulièrement dignes de protection (informations privées concernant une personne)	Oui	Informations sur une personne liées aux croyances, au comportement, à l'activité et à la santé et informations ayant une valeur juridique	Cryptage et authentification à deux facteurs [6]	Personnes habilitées en vue de remplir leur mandat professionnel	• Dossiers (avec remarques sur des personnes) • Examens (effectués et évalués) • Excuses avec justification • Evaluations • Certificats médicaux • Remarques relatives aux absences • Procès-verbaux relatifs à un-e collaborateur/trice sous surveillance • Notes d'entretien avec des élèves • Informations relatives à la compensation des désavantages • Résultats d'examens d'élèves • Communication relative à des personnes, avec contenus d'ordre psychologique ou médical

[5] Le Bureau pour la surveillance de la protection des données du canton de Berne recommande de protéger également les données personnelles avec une authentification à deux facteurs.

[6] Le Bureau pour la surveillance de la protection des données du canton de Berne recommande de ne pas stocker dans le cloud les données personnelles particulièrement dignes de protection mais d'utiliser les applications spécialisées prévues à cet effet.

Annexe : informations et conseils sur la gestion des données

- La solidité d'une chaîne dépend de son maillon le plus faible. Les maillons faibles sont en l'occurrence les appareils des différents utilisateurs et utilisatrices (AVEC). C'est pourquoi il est indispensable qu'un appareil présente les caractéristiques suivantes en matière de sécurité :
  - Protection par mot de passe lors de l'identification (également possible : reconnaissance du visage ou lecteur d'empreintes digitales)
  - Cryptage du disque dur activé (activer p. ex. BitLocker pour Windows ou FileVault pour Apple ou un outil indépendant, p. ex. VeraCrypt, DiskCryptor ou 7-Zip)
  - Protection antivirus active et à jour et
  - Système d'exploitation dans sa dernière version mise à jour

- Si un appareil accède aux services de cloud d'une école, celle-ci peut en contrôler les caractéristiques de sécurité. En cas de mise en œuvre de l'approche AVEC à l'école, ce contrôle doit être autorisé, sans quoi l'accès aux services de cloud de l'école risque d'être limité voire impossible.

- Si un appareil de travail de l'école est mis à disposition, c'est le service informatique de l'école qui est responsable de la configuration des caractéristiques de sécurité sur l'appareil.

- Un téléphone portable fonctionne comme un ordinateur doté d'une connexion Internet et d'une mémoire de stockage. Ainsi, les mêmes considérations de sécurité s'appliquent que pour l'approche AVEC.

- Un mot de passe privé ne doit jamais être réutilisé dans le cadre de l'école.

- Si des données sensibles stockées dans le cloud sont téléchargées et transférées sur des supports de mémoire externes (clé USB ou autre support physique de mémoire externe), les données ne sont plus protégées là où elles sont stockées et risquent d'être perdues physiquement. C'est pourquoi ces données doivent être protégées par mot de passe partout où elles sont stockées. Cela est possible par exemple avec un programme comme 7zip.

- Le basculement du service sécurisé de l'école vers des services de cloud publics non sécurisés ne tient souvent qu'à un clic.

- Mettre en place une solution pour le travail collaboratif sur une plateforme telle que Dropbox, Slack ou WhatsApp est simple et rapide. Néanmoins, simple et rapide ne veut pas forcément dire adapté, en tout cas pour ce qui est de la protection des données. Il s'avère souvent que les services gratuits ne sont en réalité pas du tout gratuits. On « paie » de par les données que l'on cède. Il est donc important de lire attentivement les CGV des services que l'on envisage d'utiliser. En cas d'échanges via un système de messagerie instantanée, le cryptage, l'emplacement du serveur et la possibilité d'utiliser le service anonymement sont les aspects les plus importants en matière de protection des données. Il vaut mieux privilégier les prestataires implantés en Europe qui proposent un cryptage de bout en bout (par exemple Threema ou Threema Work).

Berne, le 5 novembre 2021

Office des écoles moyennes et de la formation professionnelle

Barbara Gisi, cheffe de l'office