Kanton Bern
Canton de Berne

Direction de l'instruction publique et de la culture
Office de l'école obligatoire et du conseil
Section de l’offre ordinaire de l’école obligatoire, partie francophone (Section francophone)

NOTICE RELATIVE À GOOGLE WORKSPACE FOR EDUCATION

Table des matières

1 Introduction

La présente notice est destinée aux services responsables des établissements de la scolarité obligatoire souhaitant utiliser le produit « Google Workspace for Education » en tant que service (« *Software as a Service* »). Elle vise à fournir un panorama général de la procédure, des clarifications préliminaires requises et des mesures à prendre pour assurer une utilisation de Google Workspace for Education aussi conforme que possible à la législation sur la protection des données. Elle tient notamment compte des risques liés au traitement de données sur le Cloud et énonce les mesures à prendre s'agissant du traitement de données personnelles particulièrement dignes de protection.

La présente notice complète le lexique du canton de Berne « Protection des données à l'école obligatoire ».

2 Responsabilités

Les communes sont seules responsables de l'utilisation de l'infrastructure requise pour Google Workspace for Education au sein de leurs établissements scolaires. Les autorités communales de surveillance de la protection des données étudient les stratégies ad hoc et, le cas échéant, définissent des améliorations. En cas de questions, elles peuvent s'adresser au Bureau cantonal pour la surveillance de la protection des données.

3 Niveau contractuel

Pour les autorités responsables, l'utilisation de Google Workspace for Education à l'école obligatoire s'accompagne de risques accrus dans le domaine de la protection des données[1].

Le contrat-cadre conclu avec Educa constitue un instrument important pour réduire ces risques au minimum. Régi par le droit suisse, il stipule que le for juridique est en Suisse et que les serveurs doivent être situés au sein de l'Union européenne ou en Suisse.

Malgré ce contrat-cadre, certains risques demeurent concernant le traitement des données particulièrement dignes de protection et des données secondaires de communication collectées par Google. Une partie de ces risques peuvent être éliminés au moyen de mesures techniques complexes. D'autres risques, dits résiduels, peuvent tout au plus être limités, mais pas supprimés. Ils doivent donc être identifiés et communiqués clairement à l'échelon de direction compétent. La direction peut et doit accepter les risques résiduels qu'elle juge tolérables (acceptation du risque).

Il convient de noter que les dispositions contractuelles, en particulier la durée du contrat, sont périodiquement examinées et, le cas échéant, les renouvellements sont planifiés en conséquence.

4 Stratégie

Avant d'introduire et d'utiliser Google Workspace for Education, il y a lieu d'élaborer une stratégie portant sur le contenu des points 4.1 à 6, notamment le traitement des données envisagé et les mesures de protection prévues à cet effet[2].

Ce faisant, il convient de tenir compte en particulier des points suivants :

[1] Cf. nouvelle version révisée de l'aide-mémoire « Risques et mesures spécifiques au cloud » de privatim.
[2] Le Conseil en informatique scolaire de la PHBern aide les écoles à élaborer une stratégie d'utilisation du Cloud.

- Scénarios d'utilisation

  Quelles données peuvent être traitées, dans quel but et selon quelles modalités ?
- Classification des données

  Quel est le besoin de protection des données identifiées ?
- Choix des services appropriés

  Quels scénarios d'utilisation prévoit l'école et quels sont les services de Microsoft nécessaires à cet effet ?
- Identification des risques et mise en œuvre de mesures de protection

  Quels risques comporte le traitement des données personnelles ?
  Quelles seraient les mesures indiquées pour éliminer ou tout au moins limiter ces risques ?
- Indication des risques résiduels

  Certains risques, dits résiduels, ne peuvent être éliminés par aucune mesure. Ils doivent être identifiés et communiqués clairement à l'échelon de direction compétent. La direction peut et doit accepter les risques qu'elle juge tolérables (acceptation du risque).

4.1 Scénarios d'utilisation

Les scénarios d'utilisation de Google Workspace for Education constituent le cœur du projet. Ils précisent les besoins de l'école dans le domaine de la numérisation. Si de nouveaux besoins sont identifiés postérieurement à l'introduction de Google Workspace for Education, la stratégie devra être complétée.

Les scénarios d'utilisation doivent être élaborés de concert avec toutes les parties prenantes au sein de l'école.

Lors de l'élaboration des scénarios, il convient de prendre en compte les points suivants :
- Scénarios d'utilisation dans le cadre de l'exécution des tâches légales de l'école
  - Il importe de vérifier au préalable l'affectation à des buts précis :
    - Exemple d'affectation à des buts **légitimes** : *« L'enseignante ou l'enseignant consigne des observations concernant une ou un élève. »*
    - Exemple d'affectation à des buts **non** légitimes :
      « L'ensemble des enseignantes et enseignants d'une classe souhaitent être informés du niveau d'apprentissage des élèves dans toutes les disciplines. »
- Groupes de personnes impliqués / concernés
- Produits et données obtenus

Exemples de scénarios d'utilisation avec affectation à des buts précis (liste non exhaustive) :

	Scénario	**Personnes concernées**	**Produits/données**
1	Résultats de travaux individuels ou de groupe (formes de travail collaboratives) SANS référence à des personnes	Élèves, membres du corps enseignant	Site Internet, documents, enregistrements audio et vidéo
2	Organisation de contrôles des connaissances	Élèves, membres du corps enseignant	Documents, tableaux (évaluations)
3	Informations destinées aux parents d'élèves (par ex. camps et manifestations scolaires)	Directions d'école, membres du corps enseignant, personnes détenant l'autorité parentale	Documents, courriels

4	Saisie des coordonnées des parents (n° de téléphone, adresse électronique) et transmission de celles-ci aux élèves, aux membres du corps enseignant et aux personnes détenant l'autorité parentale	Élèves, membres du corps enseignant, personnes détenant l'autorité parentale	Documents, courriels
5	Documentation de l'entretien d'évaluation périodique (EEP)	Directions d'école, membres du corps enseignant	Documents
6	Élaboration de projets pédagogiques dans le domaine de l'intégration et des mesures de pédagogie spécialisée ordinaires et de mesures de soutien relevant de l'offre ordinaire de l'école obligatoire (MO, anciennement IMEP)[3]	Membres du corps enseignant, notamment maîtresse ou maître de classe, Service psychologique pour enfants et adolescents, personnes détenant l'autorité parentale	Documents, courriels

4.2 Classification des données : définition du besoin de protection

Les écoles se fondent sur une procédure de classification pour déterminer le besoin de protection nécessaire pour les données.
Les objectifs visés sont les suivants :

- Fournir une base pour la sensibilisation des utilisatrices et utilisateurs (formations)
- Évaluer les scénarios au moyen d'une matrice de risques
- Déterminer le besoin de protection pour les données sans référence à des personnes

Il peut être utile de se fonder sur le système de feux tricolores de la PHBern[4] pour établir la classification des données.

Par analogie avec l'ordonnance sur la classification, la publication et l'archivage des documents relatifs aux affaires du Conseil-exécutif (OCACE)[5], les produits et données correspondant aux divers scénarios sont classifiés comme suit :

Besoin de protection	Classification	Description
Aucun besoin de protection	Public	Cette catégorie concerne les données factuelles, par ex. le matériel d'enseignement sans référence à des personnes ou les données personnelles anonymisées.
Besoin de protection normal	Interne	Cette catégorie recouvre les données personnelles ordinaires. Exemples : nom, prénom, adresse électronique, etc.
Besoin de protection élevé	Confidentiel	Les données personnelles particulièrement dignes de protection et les recueils volumineux de données personnelles ordinaires ou de profils de personnalité ont un besoin de protection élevé. Exemples : maladies, infractions pénales, liste en cas d'urgence dans la classe (numéros de téléphone supplémentaires et éventuellement informations concernant des maladies), vue d'ensemble de la classe avec données pertinentes pour l'évaluation. Il peut également s'agir de données factuelles relevant du secret professionnel ou de fonction.

Exemple de classifications dans la stratégie :

[3] Cf. ordonnance régissant les mesures de pédagogie spécialisée ordinaires et les mesures de soutien relevant de l'offre ordinaire de l'école obligatoire (OMO ; RSB 432.271.1), http://www.belex.sites.be.ch/app/fr/texts_of_law/432.271.1
[4] https://kibs.ch/datenschutz/ampelsystem
[5] RSB 152.17.

	Scénario	Personnes concernées	Produits/données	Classification
1	Résultats de travaux individuels ou de groupe (formes de travail collaboratives) SANS référence à des personnes	Élèves, membres du corps enseignant	Site Internet, documents, enregistrements audio et vidéo	Public
2	Réalisation d'examens / de tests, y c. évaluations	Élèves, membres du corps enseignant	Documents, tableaux (évaluation)	Confidentiel
3	Informations destinées aux personnes détenant l'autorité parentale (camps scolaires, manifestations spéciales, etc.)	Directions d'école, membres du corps enseignant, personnes détenant l'autorité parentale	Documents, courriels	Interne
4	Saisie des coordonnées des personnes détenant l'autorité parentale (n° de téléphone, adresse électronique) et transmission de celles-ci aux élèves, aux membres du corps enseignant et aux personnes détenant l'autorité parentale. Hors listes de maladies ou d'allergies.	Élèves, membres du corps enseignant, personnes détenant l'autorité parentale	Documents, courriels	Interne
5	Liste des élèves (noms et photos) destinée aux enseignantes et enseignants de la classe	Élèves, membres du corps enseignant	Documents	Interne
6	Documentation de l'EEP	Direction d'école, membres du corps enseignant	Documents	Confidentiel
7	Élaboration de projets pédagogiques dans le domaine de l'intégration ainsi que mesures de pédagogie spécialisée ordinaires et mesures de soutien (MO, anciennement IMEP)[6]	Membres du corps enseignant, notamment maîtresse ou maître de classe, Service psychologique pour enfants et adolescents, personnes détenant l'autorité parentale	Documents, courriels	Confidentiel

[6] Cf. OMO.

8	Oubli du mot de passe	Ensemble des utilisatrices et utilisateurs	Données	Interne

Il est en outre possible de classifier différemment certains produits au sein d'un même scénario.

Exemple :

	Scénario	Personnes concernées	Produits	Classification
5.a	Liste des élèves (noms et photos) destinée aux enseignantes et enseignants de la classe	Élèves, membres du corps enseignant	Documents	Interne
5.b	Liste des élèves (noms et photos) destinée aux enseignantes et enseignants de la classe (intégration d'élèves présentant des handicaps visuellement indentifiables)	Élèves, membres du corps enseignant	Documents	Confidentiel

4.3 Choix des services appropriés

Google Workspace for Education offre une large palette de services. Le choix des services dépend des besoins de l'école (point. 4.1). À noter toutefois que seuls les services couverts par le contrat-cadre peuvent être utilisés.

Il importe de préciser que, compte tenu des risques encourus, les données personnelles de la catégorie « confidentiel » ne doivent généralement pas être traitées dans le cadre des services de Google Workspace for Education. Le cas échéant, il y a lieu d'inclure dans la stratégie d'autres applications spécialisées compatibles avec le traitement de données confidentielles.

Exemple de services retenus dans la stratégie :

Classification des données	**Service choisi**
Public et interne	Google Workspace for Education Google Docs, Google Sheets, Google Slides, Drive, Meet, Chat, Agenda, Contacts, Classroom
Confidentiel	Évaluation21, l'application d'évaluation du canton de Berne[7] Lehreroffice, Tresorit, Protonmail, Klapp, Threema, Scolaris, etc. (nécessité d'un contrôle préalable par la commune)

4.4 Identification des risques et mise en œuvre de mesures de protection

Les différents scénarios d'utilisation et les produits et données qui en résultent doivent être soumis à une évaluation réaliste des risques fondée sur la classification. Il n'est pas nécessaire de contrôler les scénarios comprenant des produits ou données appartenant à la catégorie « public ».

Pour la catégorie « confidentiel », il convient de fixer des exigences accrues concernant la protection de la confidentialité des données et de les intégrer dans l'évaluation des risques.

[7] www.beurteilung.apps.be.ch

La matrice de risques ci-après présente les risques devant être limités par des mesures de protection supplémentaires.
Les chiffres de l'axe « Probabilité de survenue » doivent être multipliés par les chiffres de l'axe « Effet / étendue du dommage ». Les résultats se lisent généralement comme suit :

- 1 et 2 : aucune mesure nécessaire
- 3 à 6 : mesures techniques et organisationnelles
- 8 à 16 : choix d'une application spécialisée spécifique ou mise en œuvre de mesures techniques et organisationnelles (au niveau de l'école) supplémentaires.

Probabilité de survenue	**4 certaine**	4	8	12	16
	3 très vraisemblable	3	6	9	12
	2 vraisemblable	2	4	6	8
	1 improbable	1	2	3	4
		1 négligeable	**2 minime**	**3 critique**	**4 catastrophique**
	Effet / étendue du dommage				

Exemples de risques fréquents et de mesures de protection possibles :

	Scénario/risque	Étendue du dommage	Probabilité de survenue	Risque	Mesures de protection (exemples divers dans la perspective de l'école)
2.a	Produit : contrôles des connaissances, y c. évaluations (prédicat/notation) Les résultats sont divulgués dans l'école.	2	3	6	Les membres du corps enseignant sont formés à ne pas faire figurer les évaluations dans le même document, mais à les documenter dans l'application spécialisée prévue à cet effet.
2.b	Documentation d'évaluations/d'estimations pronostiques La divulgation de ces évaluations est susceptible de nuire durablement aux personnes concernées, notamment dans le cadre du choix professionnel.	3	3	9	La stratégie de l'école stipule que ces données confidentielles peuvent être traitées uniquement dans l'application spécialisée spécifique. La sensibilisation/formation dans ce domaine est indiquée dans le document « [Referenzen anfügen] ». Un mode d'authentification à deux facteurs est requis pour utiliser l'application spécialisée.
7.a	Élaboration de projets pédagogiques dans le domaine de l'intégration ainsi que mesures de pédagogie spécialisées ordinaires et mesures de soutien (MO, anciennement IMEP), et sauvegarde dans Google Docs / Drive. Les administratrices et administrateurs de Google Workspace peuvent avoir accès à ces données. Il n'existe aucune possibilité de contrôler si les autorités américaines consultent ces données (en vertu du *CLOUD Act*).	3	4	12	Les enseignantes et enseignants élaborent les projets pédagogiques sur leur ordinateur, dans un programme de traitement de texte différent de Google Docs, puis les sauvegardent dans l'application spécialisée spécifique
7.b	Les projets pédagogiques sont envoyés par courriel à la direction d'école ou aux personnes détenant l'autorité parentale. Lors de la saisie d'une adresse électronique, le risque d'erreur est élevé. Le dommage pour la personne concernée peut être considérable (harcèlement, cyberharcèlement).	3	4	12	1re possibilité : le contenu des courriels et les annexes envoyés à des adresses électroniques externes sont cryptés. Le mot de passe est transmis via un deuxième canal. Une signature numérique est utilisée (S/MIME). 2e possibilité : un service de messagerie distinct offrant un cryptage supplémentaire est utilisé pour transmettre les contenus. Exemple : Protonmail. Ce service de messagerie requiert une authentification à deux facteurs. 3e possibilité : les données sont communiquées uniquement sous forme de liens par le biais d'un troisième serveur sécurisé. Le mot de passe est envoyé séparément. Exemple : Proton Drive ou Tresorit / Tresorit Send
8	Oubli du mot de passe Une administratrice ou un administrateur peut réinitialiser en tout temps les mots de passe des utilisatrices et utilisateurs, voire donner à ces derniers l'accès aux données concernées. Les listes de mots de passe comportent un risque de piratage des comptes.	2	3	6	Le rôle d'administratrice ou d'administrateur est inscrit dans le plan des rôles et des droits d'accès. Une convention supplémentaire réglemente les droits et les obligations. Les utilisatrices et utilisateurs reçoivent un mot de passe par défaut et doivent en créer un nouveau à leur prochaine connexion.

4.5 Identification des risques résiduels

La mise en œuvre des mesures énoncées ne permet pas d'écarter tous les risques (risques résiduels). À l'heure actuelle, la plupart des risques résiduels résultent de l'absence de mécanismes de contrôle. Ils doivent être identifiés et communiqués clairement à l'échelon de direction compétent. La direction peut et doit accepter les risques qu'elle juge tolérables (acceptation du risque).

Exemples
Risques résiduels liés au contrat :

- Impossibilité de contrôler l'accès aux données par Google ou des sous-traitants de Microsoft
- Impossibilité de contrôler l'accès aux données par les autorités de sécurité américaines (en vertu du *CLOUD Act)*
- Impossibilité pour l'autorité compétente de contrôler que les données personnelles pouvant être utilisées pour l'authentification à deux facteurs (nom, prénom, adresse électronique professionnelle et, dans certains cas, numéro de téléphone portable privé) sont bel et bien supprimées de manière irrévocable à l'expiration de la durée de conservation prévue dans le contrat
- Impossibilité pour l'autorité compétente d'exclure avec le contrat-cadre Educa la collaboration de Google avec des sous-traitants
- Saisie des noms et prénoms des utilisatrices et utilisateurs (risque de profilage)
- Impossibilité de contrôler la non-utilisation, réglementée dans le contrat, des données de diagnostic par Google
- Modifications de contrat unilatérales par Google.

Risques résiduels liés à l'organisation de l'école :

- Gestion des mots de passe des élèves du premier cycle par l'enseignante ou l'enseignant compétent pour la classe
- Risque que les commentaires concernant les travaux des élèves contenus dans un même document soient interprétés comme une évaluation formative.

4.6 Cryptage

Lors de l'utilisation de Google Workspace for Education, les données transmises et sauvegardées sont cryptées conformément aux normes applicables en la matière (données en transit [« *data in transit* »] et données au repos [« *data at rest* »]). Google, qui dispose de la clé correspondante, peut en principe accéder aux données cryptées se trouvant sur le Cloud. Les données en cours de traitement dans le Cloud (« *data in process* ») ne sont pas cryptées.

Il est possible de limiter le risque d'accès non autorisé à des données par les employées et employés de Google (ou des entreprises sous-traitantes concernées) en activant le processus « Access Approval » ou en utilisant une clé propre aux autorités (par ex. pour le traitement de données confidentielles). Le processus « Access Approval » peut être activé dans Google Workspace for Education Plus. Google s'engage alors par contrat à n'utiliser la clé qu'avec le consentement exprès de l'autorité. Le nom de la collaboratrice ou du collaborateur habilité au sein de l'école à accorder ce consentement doit figurer dans le document définissant les rôles et les droits d'accès.
Il n'est toutefois pas encore exclu que les autorités américaines puissent accéder aux données enregistrées en vertu du *CLOUD Act*.

Des solutions de sauvegarde des données ou de courriel dotées des technologies de sécurité les plus puissantes sont par ailleurs disponibles sur le marché. Le cas échéant, il importe de vérifier que l'entreprise a son for juridique en Suisse et que les serveurs sont situés en Suisse ou au sein de l'UE, et de veiller à la convivialité d'utilisation dans le contexte scolaire.

4.7 Procès-verbal

Lors de l'utilisation de Google Workspace for Education, des données relatives aux utilisatrices et utilisateurs et leurs activités peuvent être automatiquement consignées et sauvegardées (données de connexion).

L'exploitation de ces données de connexion n'est possible que dans des conditions précises (cf. ordonnance cantonale sur les données secondaires de communication (ODSC) :

- En cas de problème technique de l'infrastructure
- En cas d'utilisation abusive soupçonnée, si les conditions suivantes sont remplies :
    - le soupçon concret d'utilisation abusive est motivé par écrit de manière suffisante ou
    - l'utilisation abusive est avérée et
    - la personne concernée a été informée par écrit.

Étant donné que la transmission automatisée des données à Google ne peut pas être désactivée, ces problèmes doivent être indiqués parmi les risques résiduels (cf. point 4.5).

4.8 Authentification et mots de passe

Une authentification à deux facteurs est nécessaire pour les administratrices et les administrateurs. Elle peut être activée gratuitement dans Google Workspace for Education.
Une authentification à deux facteurs est recommandée pour les membres du corps enseignant. En cas de connexion avec un facteur unique, le risque encouru est considérable étant donné que des tiers peuvent s'emparer illégalement du compte.

Google Workspace for Education offre deux modes d'authentification :

- Utilisation de l'authentification Google intégrée
- Recours à un service d'authentification. Pour plus d'informations : Configurer l'authentification unique pour les comptes Google gérés faisant appel à des fournisseurs d'identité tiers - Aide Administrateur Google Workspace

Le mode d'authentification doit être défini dans le cadre d'une analyse de risques tenant compte du but et de l'étendue du traitement des données et du type de données traitées.

4.9 Rôles et droit d'accès

Les rôles et droits d'accès octroyés doivent faire l'objet d'un contrôle annuel. Chaque personne doit être autorisée à accéder uniquement aux données dont elle a effectivement besoin.

4.10 Saisie des utilisatrices et utilisateurs

Google traite non seulement les données personnelles transmises dans le cadre des services de Cloud (en particulier les données de contenu) mais aussi les données générées par les utilisatrices et utilisateurs ou par ses propres services (par ex. données secondaires de communication, de télémétrie ou de procès-verbal). Ces données personnelles supplémentaires doivent être traitées avec la même diligence que les données servant à l'exécution effective de tâches.

Lors de la saisie des utilisatrices et utilisateurs, il y a donc lieu de renseigner uniquement les informations indispensables (principe du minimum de données nécessaire).

Lorsque les données sont saisies explicitement au moyen de l'authentification intégrée dans Google, aucun autre attribut en dehors du nom ne doit être indiqué.
En cas de doute ou sur demande, la pseudonymisation des données doit être proposée.

4.11 Synchronisation des données des utilisatrices et utilisateurs

L'annuaire Google peut être synchronisé avec un annuaire actif de Microsoft ou un serveur LDAP.
Seules les données d'utilisatrices et d'utilisateurs impérativement nécessaires peuvent être transmises. Il en va de même pour les attributs, y compris en cas de recours à un fournisseur d'identité (*Identity Provider*, IdP).
Exemple : utilisation d'un annuaire Google comme fournisseur d'identité pour le raccordement à Edulog.

Informations complémentaires :

- À propos de Google Cloud Directory Sync - Aide Administrateur Google Workspace

4.12 Suppression des données

La suppression des données numériques obéit aux mêmes principes que la destruction des documents papier. Les obligations prévues par le canton de Berne en matière de conservation des données s'appliquent. Les données qui ne sont plus utiles doivent être supprimées. Les utilisatrices et utilisateurs doivent avoir la possibilité de transférer leurs données sur un autre support de stockage avant leur suppression.

La suppression des données de procès-verbal s'effectue de manière automatisée. Les délais de conservation sont de 180 jours pour la plupart des données de procès-verbal.

Informations complémentaires :

- Conservation des données et temps de latence - Aide Administrateur Google Workspace

4.13 Sécurité des données et planification des urgences

Les exigences relatives à la disponibilité de Google Workspace for Education doivent être définies. En cas de besoin, des mesures de sécurité des données et de planification des urgences doivent être mises en œuvre.

4.14 Données de diagnostic

Lors de l'utilisation de Google Workspace for Education, des données sont probablement transmises à Google.

Comme les administratrices et les administrateurs n'ont aucune possibilité de prendre des mesures concernant les données de diagnostic, ils doivent identifier les risques résiduels.

5 Information des personnes concernées

Les utilisatrices et utilisateurs doivent être préalablement informés de l'utilisation prévue de Google Workspace for Education dans l'école. Il importe de communiquer les principaux risques encourus et les mesures de protection planifiées.

Les utilisatrices et utilisateurs reçoivent une liste des services de Google Workspace for Education dont dispose l'école et de leurs modalités d'utilisation.

Le Conseil en informatique scolaire de la PHBern fournit à cet effet à chaque école un dépliant personnalisable sur le modèle des feux tricolores[8].

Exemple :

5.1 Formation et sensibilisation

Les formations portant sur l'infrastructure et la sensibilisation dans des domaines d'application pertinents pour la protection des données doivent débuter dès le déploiement et l'utilisation de l'infrastructure.

5.1.1 Membres du corps enseignant

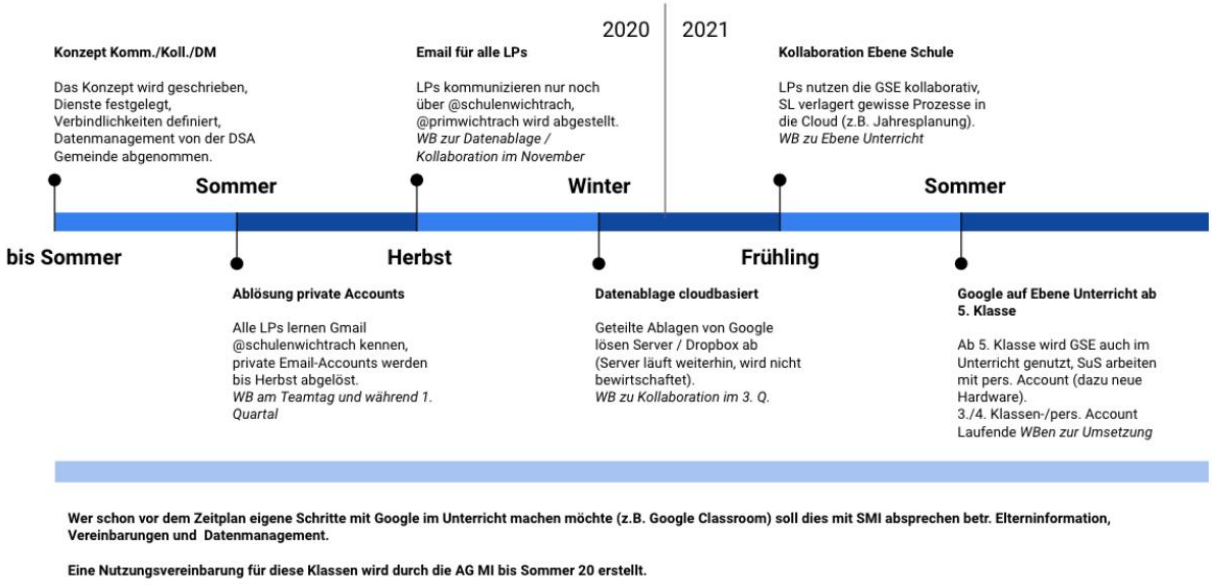
Les directives concernant la gestion des données à l'école complètent les mesures de protection techniques (cf. point 4.4 *Exemples*).
Étant donné que les écoles font face à de fortes fluctuations en matière de personnel enseignant, il est impératif de veiller à ce que les enseignantes et enseignants nouvellement engagés puissent obtenir rapidement et facilement les informations essentielles nécessaires à l'utilisation de l'infrastructure informatique scolaire.
C'est également là que le dépliant personnalisable avec les feux tricolores mis au point par le Conseil en informatique scolaire de la PHBern entre en jeu.

Le Conseil en informatique scolaire de la PHBern a constaté par expérience que le perfectionnement continu des membres du corps enseignant dans le domaine de l'infrastructure (par ex. par les spécialistes Médias et informatique, SMI) produisait des effets plus durables qu'une formation unique dispensée par une entreprise externe.

[8] https://kibs.ch/datenschutz

Pour décharger les SMI, les écoles peuvent mettre à disposition des processus centraux ou des thèmes liés à la sensibilisation sous forme de documents ou de vidéos.

Exemple de planification de l'introduction de Google Workspace for Education sur une année



5.1.2 Élèves

La formation des élèves peut avoir lieu dans le cadre de la stratégie de mise en œuvre pour l'enseignement des contenus des plans d'études liés à l'éducation aux médias et à l'informatique.

6 Parents

Les parents doivent être informés à l'avance (avant le déploiement) de l'utilisation prévue de Google Workspace for Education.

6.1 Information des parents

Il importe d'informer les parents via plusieurs canaux. D'une part, toutes les stratégies relatives à l'infrastructure ainsi qu'aux médias et à l'informatique (cf. recommandations[9]) doivent être accessibles librement et en toute transparence. D'autre part, les parents doivent avoir la possibilité de poser des questions et d'exprimer leurs réserves.
.

6.1.1 Documents

- Stratégie de mise en œuvre pour l'éducation aux médias et à l'informatique (découlant des recommandations du canton de Berne)[10], exemples de contenus :
    - Enseignement et développement de l'enseignement
    - Développement du personnel

[9] Recommandations aux communes et aux directions d'école
[10] kibs.ch, la plateforme du Conseil en informatique scolaire de la PHBern, fournit un soutien.

    - Collaboration et communication
    - Gestion des données et aspects juridiques
    - Aspects techniques et financiers

- Stratégie relative à l'infrastructure du Cloud (requise sur la base de la présente notice)

6.1.2 Séance d'information

Il est essentiel que l'école ou la commune communiquent au sujet du traitement des données personnelles en organisant une séance d'information destinée aux parents, et ce avant la mise en place de l'infrastructure.

Lors de cette séance, en plus des informations générales, il conviendra de préciser les enseignements concernés (contenus du plan d'études liés aux médias et à l'informatique). Dans l'idéal, toutes les parties prenantes participant aux travaux stratégiques devraient être présentes (commune, autorité communale de surveillance de la protection des données, direction d'école, SMI, membres du corps enseignant, éventuellement entreprises et/ou PHBern).

La séance contribuera ainsi à dissiper les doutes et à satisfaire les demandes.

6.1.3 Prise de connaissance

Si Google Workspace for Education est déployé conformément à la présente notice, on peut partir du principe que les personnes détenant l'autorité parentale sont informées de la mise en œuvre.

7 Annexes

7.1 Services selon le contrat-cadre

Les dispositions contractuelles du contrat-cadre Educa avec Google ne s'appliquent qu'aux services principaux de Google Workspace for Education Plus.

Les principaux services sont listés ici :
Conditions d'utilisation de Google Workspace – Google Workspace

Principaux services pour une école (liste non exhaustive) :
- Services de Cloud Identity pour la gestion des utilisatrices et utilisateurs
- Gmail
- Google Agenda
- Google Cloud Search
- Google Classroom
- Google Contacts
- Google Docs avec Google Docs, Google Sheets, Google Slides, Google Forms
- Google Drive
- Google Groupes
- Google Hangouts, Chat et Meet
- Google Sites
- Google Vault