Protection et sécurité des données

Quelques fondamentaux et questions brûlantes

mercredi, le 18 novembre 2026

Daniel Wyss, Bureau pour la protection des données (BPD)



Quelle: Gegen den Strich - Caricatura Galerie

Point de départ : un aspect constitutionnel

droits fondamentaux

dignité humaine
égalité de traitement
liberté personnelle
protection de la sphère privée
liberté de conscience de de croyance
liberté d'opinion et d'information
…





tâches publiques

sécurité et ordre public,
formation, recherche et culture,
environnement, aménagement du territoire, circulation, eau, énergie
économie, travail, logement,
sécurité sociale, santé, gestion des finances …

Droit fondamentaux …

Art. 13 Cst. Protection de la sphère privée

1 Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.

2 Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.

Art. 11 Cst. Protection des enfants et des jeunes

1 Les enfants et les jeunes ont droit à une protection particulière de leur intégrité et à l'encouragement de leur développement.

2 Ils exercent eux-mêmes leurs droits dans la mesure où ils sont capables de discernement.

… et tâches publiques

Art. 62 Cst. Instruction publique

1 L'instruction publique est du ressort des cantons.

2 Les cantons pourvoient à un enseignement de base suffisant ouvert à tous les enfants. Cet enseignement est obligatoire et placé sous la direction ou la surveillance des autorités publiques. Il est gratuit dans les écoles publiques.

Art. 43 ConstC Ecoles

1 Le canton et les communes entretiennent des jardins d'enfants et des écoles. […].

2 […].

Droit de la protection des données - généralités

Loi fédérale sur la protection des données (LPD):

s'applique au traitement effectué par

a. des personnes privées;

b. des organes fédéraux.

protection de la personnalité (art. 28 CC)

Loi cantonale sur la protection des données (LCPD):

s'applique au traitement entrepris

par des autotriés cantonales et communales

protection d'un droit fondamental

Droit sur la protection des données = « règles du jeu » dans un État de droit

Art. 18 ConstC Protection des données

1 Toute personne a le droit de consulter les données qui la touchent et de demander la rectification de celles qui sont inexactes et la destruction de celles qui sont inadéquates ou inutiles.

2 Les autorités ne peuvent traiter des données personnelles que s'il existe une base légale et pour autant que ces données sont nécessaires et adéquates à l'accomplissement de leurs tâches.

3 Elles s'assurent que les données traitées sont exactes et elles les protègent contre un emploi abusif.

Droit de la protection des données - spécificités

dispositions sur le traitement de données personnelles

lois, ordonnances et règlements de la Confédération, du canton et des communes (→ actes législatifs spécifiques)

Droit interne

1 État - Peuple - Autorités
2 Droit privé - Procédure civile - Exécution
3 Droit pénal - Procédure pénale - Exécution
4 École - Science - Culture
5 Défense nationale
6 Finances
7 Travaux publics - Énergie - Transports et communications
8 Santé - Travail - Sécurité sociale
9 Économie - Coopération technique

41 École

410 Espace suisse de formation

410.2	Loi fédérale du 30 septembre 2016 sur la coopération entre la Confédération et les cantons dans l'espace suisse de formation (Loi sur la coopération dans l'espace suisse de formation, LCESF)
410.21	Convention du 16 décembre 2016 entre la Confédération et les cantons sur la coopération dans l'espace suisse de formation (CCoop-ESF)

411 École primaire

411.3	Loi fédérale du 17 juin 2022 sur les contributions à l'École cantonale de langue française de Berne
411.4	Éducation physique →415.0 art. 12 →415.01 art. 48 à 50

Recueil systématique (RSB)

Déplier | Replier

- **1** - État, peuple, autorités
- **2** - Droit privé, procédure civile, exécution
- **3** - Droit pénal, procédure pénale, exécution
- **4** - Église, culture, éducation et sciences
  - **41** - Église
  - **42** - Culture
  - **43** - Éducation et sciences
    - **430** - Dispositions générales
    - **431** - Orientation en matière d'éducation
    - **432** - Ecole obligatoire
      - **432.2** - École obligatoire
        - **432.21** - Dispositions générales
        - **432.27** - Mesures de pédagogie spécialisée ordinaire
        - **432.28** - Offre spécialisée de l'école obligatoire
      - **432.3** - Ecole de musique
    - **433** - École moyenne, école de maturité spécialisée, école du degré diplôme
    - **435** - Formation professionnelle, formation continue et orientation professionnelle
    - **436** - Université
    - **437** - Gymnastique et sport
    - **438** - Subventions de l'État, subsides de formation et fondations
    - **439** - Conventions intercantonales

Définitions-clés – art. 2 LCPD

données personnelles:	informations relatives à une personne identifiée ou identifiable ;
traitement:	toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, en particulier le fait de les collecter, de les enregistrer, de les conserver, de les utiliser, de les modifier, de les communiquer, de les archiver, de les effacer ou de les détruire ;
communication:	le fait de transmettre des données personnelles ou de les rendre accessibles, notamment par l'autorisation de leur consultation, la fourniture de renseignements, leur transfert ou leur publication.

Données personnelles sensibles – personnes physiques

- les données sur les opinions et les activités religieuses, philosophiques, politiques ou syndicales ;
- les données sur l'origine ethnique ;
- les données sur la santé et la sphère intime ;
- les données génétiques ;
- les données biométriques identifiant une personne physique de manière univoque;
- Les données sur des mesures d'aide sociale ou des mesures de protection de l'enfant et de l'adulte ;
- Les données relatives à des poursuites ou des sanctions administratives ou pénales.

Données personnelles sensibles – personnes morales

- les données relatives à des poursuites ou des sanctions administratives ou pénales;
- les secrets professionnels, d’affaires ou de fabrication.

Principes du droit sur la protection des données

applicables à tous traitements de données personnelles:

- légalité ;
- finalité ;
- proportionnalité ;
- exactitude et exhaustivité ;
- transparence (→ information / accès) ;
- sécurité des données.

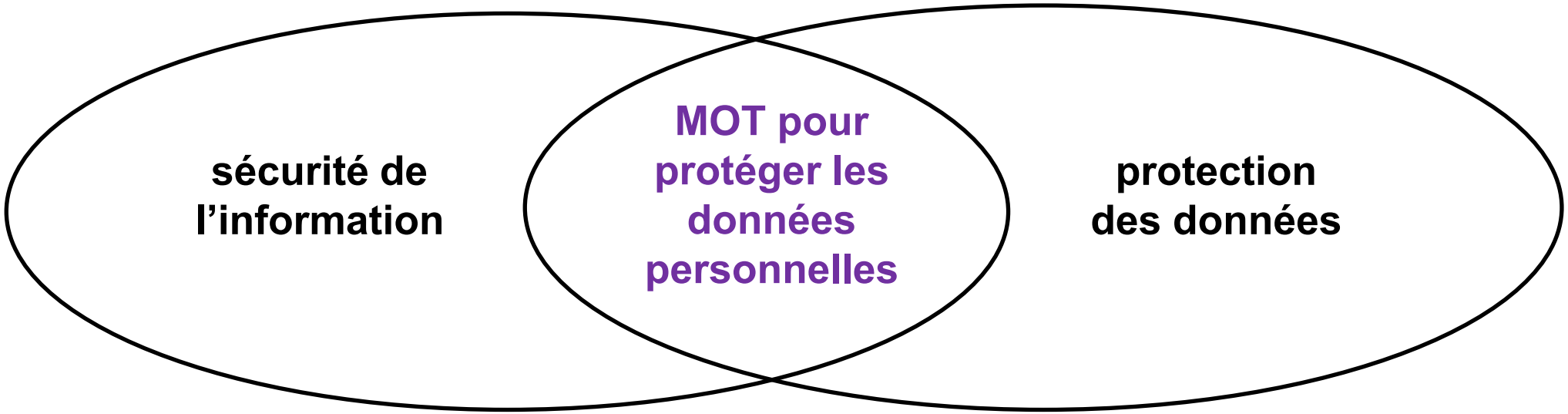
Sécurité de l’information – art. 4 LISC

Les buts de la sécurité de l’information sont les suivants :

– confidentialité ;
– intégrité ;
– disponibilité ;
– traçabilité.

Sécurité de l’information

Les but de la sécurité de l’information doivent être garantis par des mesures organisationnelles et techniques appropriées (MOT).



Sécurité de l’information

- mesures techniques : prévenir des violations de la protection des données par des mesures de sécurité concrètes (par ex. portes et armoires verrouillées, enveloppes scellées, cryptage, mots de passe à plusieurs éléments) ;
- mesures concernant l’organisation : garantir la sécurité de l’information pour autant qu’elles soient respectées (par ex. règlement concernant l’organisation, les responsabilités, les procédures ou les conditions d’utilisation).

Sécurité de l’information et digitalisation – ce qui change

- les données sont invisibles tout comment les risques qu’elles comportent ;
- des attaques possibles de n’importe où : de nouvelles formes d’attaques et de comportements répréhensibles liés aux outils de travail connectés et virtualisés – provenant de n’importe quel endroit dans le monde ;

Sécurité de l’information et digitalisation – ce qui change

– de nouvelles dépendances : fournisseurs, prestataires de services cloud et produits deviennent des facteurs de risque critique (risques liés à des tiers) ;
– des dommages souvent invisibles : fuites de données et manipulations passent souvent inaperçues pendant un certain temps – les dommages se produisent à l’insu de tous.

→ *nouvelles risques nécessitent de nouvelles mesures et des contrôles appropriés (et rapides)*

Traitement de données par mandat («Outsourcing»)

art. 12 LCPD Traitement par des tiers mandatés

[1] L'autorité peut mandater des tiers pour traiter des données personnelles à condition

a. que les données soient traitées de la même manière que l'autorité est habilitée à le faire et,

b. qu'aucune obligation légale ou contractuelle de garder le secret ne s'y oppose.

[2] Elle s'assure en particulier que les tiers mandatés garantissent la sécurité des données.

[3] Les tiers mandatés ne peuvent pas déléguer le traitement à d'autres personnes sans l'accord préalable de l'autorité.

→ Les droits et obligations des parties doivent être définis dans un accord contractuel approprié.

Utilisation de services « cloud »

par exemple : M365 pour la bureautique; Chat GPT en tant que système d'IA génératif, WhatsApp en tant qu'application de messagerie, Dropbox en tant que service de stockage den ligne

- juridiquement : traitement de données par mandat ;
- les objectifs de protection comme la confidentialité et l'intégrité ne peuvent plus être garantis ; responsabilité malgré la perte de contrôle ?
- Il faut définir des scénarios d'utilisation, identifier les risques et définir les mesures à prendre ;

→ utilisation éventuellement possible dans des limites clairement définies ; directives et autorisation par la direction – tout comme contrôle et sanctions.

Responsabilité

La responsabilité de la protection et de la sécurité des données incombe à l'autorité qui, pour accomplir ses tâches légales, traite ou fait traiter des données personnelles.

La responsabilité comprend tous les aspects de la loi :

- base légale et proportionnalité ;
- garantir les droits des personnes concernées ;
- garantir les objectifs de la sécurité de l'information.

→ Au sein d'une autorité : « La protection des données relève de la responsabilité de la cheffe / du chef ».



Der Bund, 20 mai 2023: des centaines de personnes touchées à Bâle-Ville ; des pirates ont publié des données sensibles concernant des élèves et des enseignants sur le Darknet.

Sanctions

Application du droit sur la protection des données :

– demande et, le cas échéant, recours de la personne concernée ;
– recommandations et proposition de l'autorité de protection des données ;
– mesures de droit du travail (prises par la hiérarchie).

Réparation des dommages résultant d'une violation du droit :

– le canton est les communes sont responsables des dommages résultant d'un traitement illicite des données (y compris par des sous-traitants) ;
– éventuellement, une réparation morale, lorsqu'une atteinte grave à la personnalité ne peut être réparée autrement.

Cloud et AI

- 45% des collaboratrices / collaborateurs d'entreprise utilisent des outils d'IA générative ;
- 92% de l'utilisation totale de l'IA dans les entreprises concerne ChatGPT (= outil d'IA générative) ;
- 40% des fichiers envoyés / téléversés vers des outils d'IA générative contiennent des données sensibles ;
- 77% des collaborateurs saisissent des données sensibles dans des outils d'IA générative ;
- 82% de ces téléversements proviennent de comptes personnels ;
- les collaborateurs saisissent, en moyenne, 14 fois par jour des données dans des comptes externes à l'entreprise, et au moins 3 d'entre eux contiennent des données sensibles ;

→ Le « presse papiers » est désormais la source principale de fuite de données sensibles.
→ les outils classiques de prévention des pertes de données (« Data-Loss-Prevention-Tools ») ne détectent même pas ces activités.

Source: LayerX, Enterprise AI and SaaS Data Security Report 2025

« Intelligence artificielle » - l'essentiel

👉🏻 l'autorité est responsabilité pour la protection des données et pour la sécurité de l'information ;

⚠️ les outils d'IA fonctionnent généralement sur des solutions cloud d'un géant du cloud (par ex. Microsoft Azure / Google Cloud / Amazon Web Services)
→ perte de contrôle sur le traitement des données ;

⚠️ les outils d'IA s'entraînent à partir de données de production
→ tout changement du but du traitement nécessite une base légale
→ aucune garantie que les données ne seront pas utilisées à des fins d'entraînement

« Intelligence artificielle » - l’essentiel

- ✅ Quick-Fix: pas de données personnelles réelles dans des outils d’IA (pseudonymisation)
- 🔀 Sinon : concept SIPD et un éventuel contrôle préalable auprès du BPD

Contact

Daniel Wyss, Collaborateur scientifique droit
+41 31 636 28 90 (ligne directe), daniel.wyss@be.ch

Bureau pour la protection des données (BPD)
Poststrasse 25, 3072 Ostermundigen
+41 31 633 74 10, bpd.be.ch