educa.Guides

Protection des données

Les données personnelles à l'école

École et TIC

Mentions légales

Éditeur educa.ch

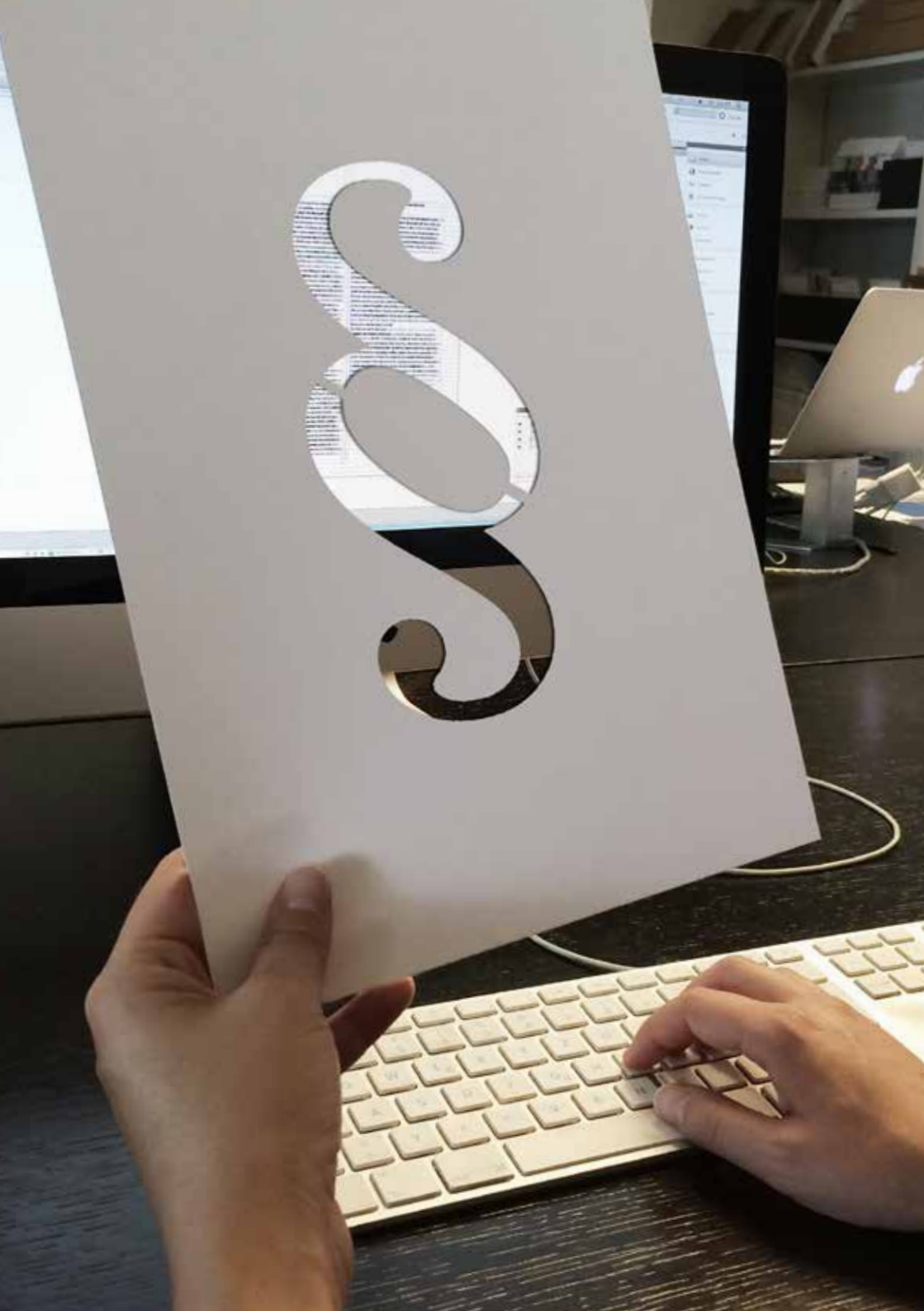
Extraits reproduits avec l'aimable autorisation de :
- Direction de l'instruction publique du canton de Berne : Lignes directrices sur la protection des données personnelles dans les écoles du canton de Berne (document de référence)
- Préposé fédéral à la protection des données et à la transparence (PFPDT) : Protection des données, Observations concernant les sites de réseautage social, Renseignements concernant la sécurité WLAN

Photos büro z {grafik design}, Berne

Novembre 2009

Ce guide dispose d'une page Internet sur educa.ch. Vous trouverez à cet endroit un fichier PDF du guide, que vous pouvez également consulter en ligne, ainsi que des informations complémentaires et des liens vers des sites proposant du matériel pédagogique. Ces informations et liens sont mis à jour régulièrement. La date de publication ainsi que celle d'une éventuelle actualisation sont indiquées sur le PDF.

→ Page Internet



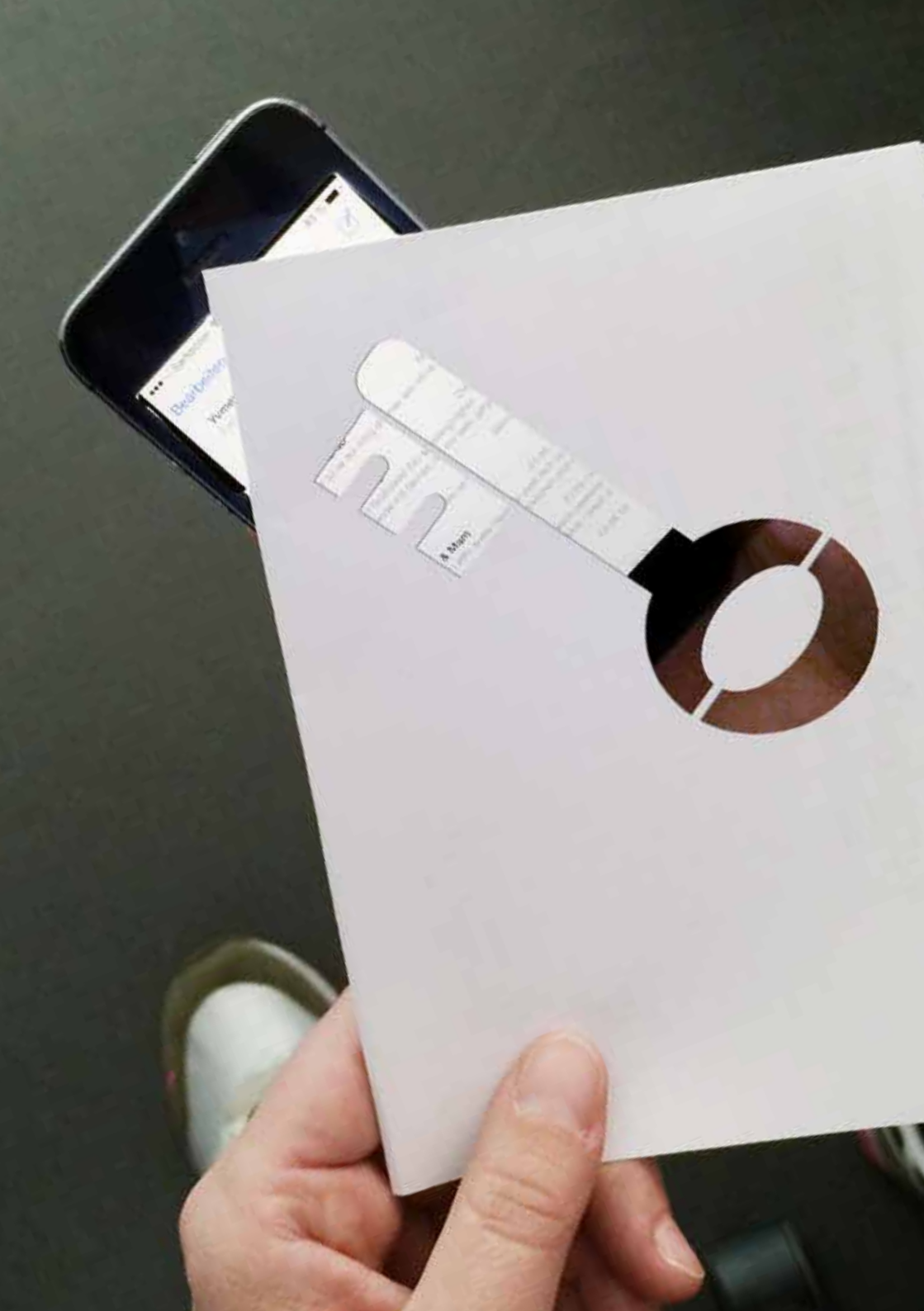
Introduction

Le terme de « Protection des données » ne désigne pas dans ce contexte la protection des données en tant que telles, comme l'expression le laisse supposer à tort. Il s'agit, en fait, de la protection des personnes contre tout emploi abusif de leurs données personnelles dans leur vie quotidienne. Depuis que les applications Web 2.0 ont fait leur entrée dans les salles de classe, la protection des données personnelles des apprenantes et apprenants – mais aussi des enseignantes et enseignants – est devenue un enjeu dont l'importance ne cesse de grandir. Beaucoup d'enseignants sont encore malheureusement trop peu conscients du caractère brûlant de cette thématique. En effet, à l'époque de l'introduction des services Web 2.0, ce sont surtout les directions d'écoles et les services de l'administration en charge de l'éducation qui ont eu à s'occuper de ce sujet. Ils devaient, par exemple, s'occuper de transférer les données personnelles d'écoliers d'un poste administratif à un autre. Depuis lors, le sujet de la protection des données concerne toutes les personnes qui interviennent dans le cadre scolaire. En effet, à notre époque, on peine à imaginer que quelqu'un renonce complètement à l'utilisation des services internet interactifs.

Journée européenne de la protection des données

Organisée une fois par an – chaque 28 janvier –, à l'initiative du Conseil de l'Europe, la Journée de la protection des données a pour but d'expliquer aux citoyens quelles données à caractère personnel les concernant sont collectées et traitées et pourquoi, et quels sont leurs droits par rapport à ce traitement.

→ coe.int



Notions fondamentales

Le premier chapitre consiste en une introduction au domaine de la protection des données. Il répond aux questions suivantes : quelles données sont à protéger ? quelles sont les dispositions légales relatives à la protection des données ?

Droit à l'autodétermination informationnelle

Ce que l'on appelle le droit à l'autodétermination informationnelle constitue un principe important de notre ordre social. L'autodétermination informationnelle est le droit pour chaque individu de décider lui-même de la communication et de l'emploi des informations le concernant.

À quoi sert la protection des données ?

On pourrait dire en simplifiant : le premier but de la protection des données doit être de défendre le droit à l'autodétermination informationnelle de la personne.

Cette tâche n'est pas toujours simple : des intérêts légitimes peuvent en effet limiter ce droit à l'autodétermination, comme par exemple dans le cas d'enquêtes policières.

Proportionnalité
La protection des données doit garantir fondamentalement que dans chaque cas isolé de traitement de données, la proportionnalité soit préservée. En aucun cas, on ne doit donc rassembler plus de données personnelles qu'il n'est absolument nécessaire pour l'exécution d'une tâche donnée, limitée dans l'espace et dans le temps. Cette garantie implique également que la personne concernée puisse contrôler autant que possible – et au besoin empêcher – le traitement des données qui la concernent.

Droit de regard
A la demande de chaque individu, les responsables des fichiers doivent rendre compte des données qu'ils ont traitées, concernant cette personne à titre personnel. À cette fin, la loi sur la protection des données fixe un droit de regard sur les données personnelles que l'on peut faire valoir auprès des responsables de fichiers.

Quelle définition dans la loi ?

L'art. 13 de la Constitution fédérale dispose formellement que toute personne a droit au respect de sa vie privée et familiale, de son habitation ainsi que de sa correspondance postale et téléphonique, qu'elle a droit également à la protection contre un usage abusif de ses données personnelles.

Ce ne sont pas les données comme telles que la protection des données protège de la sorte mais les droits fondamentaux des personnes.

Loi fédérale sur la protection des données

La loi fédérale sur la protection des données (LPD) fut adoptée en vue d'assurer à cette protection un ancrage légal. Elle est en vigueur depuis le 1er juillet 1993. L'ordonnance correspondante (OLPD) règle les détails.

La loi fédérale sur la protection des données (LPD) s'adresse à l'administration fédérale ainsi qu'à toute personne privée qui traite des données à caractère personnel.

Lois cantonales sur la protection de données

D'autres lois contiennent en outre nombre de dispositions visant à la protection de la personnalité. Les articles 28 – 28l du code civil par ex. déterminent comment l'on procède juridiquement dans le cas d'atteintes à l'identité d'une personne.

Les lois cantonales sur la protection de données règlent le traitement de données par des administrations cantonales et forment la base des règlements communaux de protection des données. Ceux-ci à leur tour deviennent une référence juridique pour les écoles gérées par les communes.

Données personnelles

Les données personnelles sont des informations concernant une personne précise. Le terme « informations » est à comprendre au sens le plus large. S'y rattachent les constatations de faits et les jugements de valeur, sans tenir compte de la technique utilisée (signal analogique ou numérique, parole, image, son ou leur combinaison) ni du mode de transmission (entre personnes présentes, par courrier ou transmission électronique). En revanche, ce qu'une personne sait sans l'avoir consigné ou enregistré quelque part n'entre pas en ligne de compte. Une fois enlevés le nom et tous les autres éléments qui permettent l'attribution à une personne déterminée, il ne s'agit plus de données personnelles.

Traitement de données personnelles
Le terme « traitement » comprend toute opération relative à des données personnelles, en particulier l'acquisition, la conservation, la modification, l'association, la communication ou la destruction.

Communication de données personnelles
Par « communication » de données personnelles, on entend toute manière de rendre accessibles des données personnelles, en particulier le fait d'autoriser la consultation, la communication de renseignements, la transmission ou la publication.

Données personnelles « sensibles»
Dès qu'il s'agit de « données personnelles sensibles », une prudence spéciale est indiquée.
Sont considérés comme des données personnelles « sensibles » :
– informations sur les opinions, l'appartenance et l'activité religieuses, philosophiques ou politiques
– informations touchant au domaine intime, en particulier sur l'état de santé psychique, mental ou physique
– informations sur le fait d'être tributaire de l'aide sociale ou dépendant d'une prise en charge sociale
– informations sur des enquêtes policières, des procédures pénales en cours, etc.

Les prises de vues et de sons
Les prises de vues et de sons ne font pas partie en principe des données personnelles « sensibles ». Elles ne sont sensibles que dans la mesure où elles contiennent l'une des informations mentionnées ci-dessus (si par exemple les symptômes de maladies sont reconnaissables sur des images ou si, à partir d'une image, on peut conclure à une appartenance religieuse).

Même si les prises de vues ou de sons ne font pas partie de la catégorie des données « sensibles », il faut néanmoins se montrer très prudent. La publication de photos de personnes sur l'internet notamment peut avoir des répercussions sérieuses et difficilement prévisibles sur les droits de la personnalité des personnes concernées, par ex. par l'emploi abusif des photos sur d'autres sites web, par la diffamation des personnes représentées à l'aide de logiciels de traitement de l'image, etc.


AF-L
AF-L
OK

Protection de données dans l'enseignement

Ce chapitre s'adresse en premier lieu aux enseignantes et enseignants ainsi qu'aux apprenantes et apprenants. Il démontre en particulier les différents dangers qui vont de pair avec l'utilisation de services internet interactifs, ce qu'on appelle les applications Web 2.0. Ce chapitre propose aussi une liste de recommandations pour l'utilisation des applications Web 2.0, une telle liste concernant tout le monde à l'école.

Sensibilisation insuffisante aux problèmes de sécurité

La technologie de l'information permet de saisir d'énormes quantités de données personnelles et de les relier entre elles. Souvent, malheureusement, la sensibilisation de ceux qui traitent les données aux problèmes de sécurité ne suit pas le rythme des nouveautés techniques. En outre, la plupart des gens – que ce soit ceux qui traitent les données ou les personnes dont les données sont traitées – ne sont pas encore suffisamment sensibilisés aux questions de la protection de la personnalité. On est bien trop léger dans le maniement de ses données personnelles, que ce soit sur Internet ou en remplissant des formulaires de questionnaire ou de concours, pour ne citer que deux exemples.

Surfer, réseaux sociaux, chat

Les utilisatrices et utilisateurs de l'internet sont de moins en moins des « consommateurs », qui cherchent et téléchargent sur des sites web statiques les informations mises à disposition par les fournisseurs. Ils utilisent au contraire l'internet de façon interactive et collaborent à des sites web dynamiques. Le terme Web 2.0 résume ce développement.

Dans ce contexte, différents sites de réseautage (SRS) ou de networking social (SNS : Social Networking Sites) ont vu le jour. Il s'agit de portails importants où des utilisatrices et des utilisateurs inscrits se rencontrent, nouent des « amitiés » et échangent des nouvelles, des photos et des films.

Les SRS confrontent la protection de données à de nouveaux défis. À l'origine, les lois de protection des données visaient à protéger les données personnelles d'un traitement illégal ou excessif par l'État, plus tard aussi par des entreprises commerciales. Avec les SRS, deux aspects fondamentalement nouveaux sont maintenant apparus :

– Les informations personnelles citées sont fournies par les utilisateurs eux-mêmes et donc téléchargées sur les profils internet avec leur accord.
– Des personnes privées accèdent en détail aux données personnelles d'autres personnes privées. Il peut en résulter différents risques.

Opérer avec des données personnelles dans les SRS

Les sites de réseautage social (SRS) recèlent beaucoup d'avantages pour la société comme, par exemple, la possibilité de pratiquer du réseautage, de nouer des contacts par-delà les frontières ou de publier ses propres contenus. Ces explications ne visent donc pas à condamner par principe les SRS. Le but est bien plus de sensibiliser les services administratifs et les utilisateurs à une gestion des données personnelles dans les réseaux sociaux qui soit conforme à la protection des données. Car, si les services de réseautage social sont de fait gratuits la plupart

du temps, ce ne sont pas pour autant des organisations d'intérêt public. Un « commerce » a lieu : des prestations de services pour les utilisatrices et les utilisateurs en échange de leurs données. Derrière les portails se tient une puissance de marché concentrée, les entreprises internationales, qui sous la pression des investisseurs et des actionnaires doivent générer des profits croissants. La seule chose qu'un service de réseautage social puisse offrir à ses investisseurs, ce sont des données personnelles – et la valeur boursière d'un SRS en dit long sur leur intérêt.

Risques et dangers

L'utilisation de réseaux sociaux présente différents dangers connus. Des malfaiteurs peuvent à cette occasion mettre à leur profit le fonctionnement spécifique de ces réseaux, où les notions de confiance et de caractère confidentiel sont souvent mis à mal. Dans ces réseaux, en simulant des faits inexistants ou même en revêtant une fausse identité, il est facile de devenir l'« ami » de quelqu'un et de parvenir de la sorte à des informations que l'interlocuteur ne communiquerait sans doute pas autrement. Selon ce type de réseaux, il s'agirait seulement d'un déplacement sur l'internet de la communication quotidienne propre aux amis. Une telle affirmation suggère une intimité qui n'existe pas en réalité d'autant que les obstacles empêchant l'accès au réseau sont aisés à franchir.

Utiliser les SRS de façon inconsidérée et sans mesures préventives expose aux risques suivants :

Comptes d'utilisateurs, profils

En pratique, on ne peut jamais effacer un compte de façon irrévocable. D'abord, les profils sont seulement « désactivés » et non effacés. Ensuite, les utilisateurs actifs laissent beaucoup d'informations supplémentaires sur d'autres pages du réseau. Les effacer toutes absolument est pratiquement impossible. Les utilisatrices et utilisateurs perdent ainsi le contrôle de leurs données.

Données personnelles

L'internet ne sait pas ce qu'est l'oubli : des profils d'utilisateur peuvent être téléchargés et enregistrés par d'autres utilisateurs. Ce faisant on rend pour ainsi dire inutile l'effacement du profil originel, car les données demeurent toujours conservées quelque part. Il se constitue une multitude de fichiers privés qui rendent possible l'exploitation des données en recourant à la catégorisation selon certains critères par l'intermédiaire d'une fonction de recherche. Ceci accroît le danger que ces données soient mises en œuvre ailleurs que là où il était prévu qu'elles le soient. Une fois divulguées en dehors des SRS, elles peuvent causer à la personne concernée un tort considérable.

Métadonnées

Les fournisseurs de SRS ont accès non seulement aux données personnelles mais encore aux métadonnées. Chez beaucoup de fournisseurs de SRS, il est difficile de savoir ce qu'il advient de métadonnées telles que par ex. le temps de connexion, l'origine géographique de l'adresse IP, le temps de présence et les mouvements sur le site, etc. Une fois regroupées, les données personnelles et les métadonnées peuvent donner des profils de personnalité détaillés.

Photos, images

Des photos avec des personnes reconnaissables, comprenant leurs noms, permettent l'identification indiscutable de ceux que l'on a photographiés. À l'aide d'un logiciel spécial de reconnaissance du visage, on peut scruter les SRS et d'autres plateformes à la recherche de personnes spécifiques. Il est alors possible de les identifier même là où elles veulent rester anonymes, par ex. sur un site de rencontre.

CBIR

La recherche d'images par le contenu (en anglais, content based image retrieval : CBIR) présente le même type de danger : la reconnaissance automatique de caractéristiques à l'arrière-plan d'une image. Un tableau spécifique ou une maison peuvent, par exemple, conduire à la localisation géographique d'une situation de photo et avoir pour conséquence la communication de l'adresse, le harcèlement obsessionnel ou d'autres actes criminels.

Liaisons

Plusieurs SRS permettent des liaisons étendues avec des profils ou des adresses électroniques de tierces personnes – et aussi sans aucun doute de personnes qui ne sont pas membres du réseau – sans bien sûr leur demander la permission. Ceci peut devenir un danger pour la sphère privée de toute personne.

Single Sign On

Les utilisateurs de plusieurs SRS peuvent simplifier l'exploitation de leurs boîtes de réception en les regroupant toutes sur une seule application internet. À l'aide de leur nom d'utilisateur et de leur mot de passe, ils peuvent de la sorte consulter d'un seul coup d'œil les dernières nouvelles de leurs profils, ce qui peut être pratique mais pose la question de la sécurité.

Actes criminels

Dans la plupart des SRS, la procédure d'enregistrement est très simple : on donne quelques informations sur la personne qui ne sont pas vérifiées et peuvent dès lors être inventées. Une fois parvenu à l'intérieur, il est dans ces conditions très facile de nouer des contacts et d'être admis dans les « cercles d'amis » d'autres personnes. Il en suit des risques d'infiltration de ces communautés à des fins douteuses ou même franchement criminelles :

Usurpation d'identité
Il est simple d'usurper une identité : on se constitue un profil avec le nom d'une personne connue et l'on profite de sa célébrité – ou l'on entame sa réputation en se comportant mal. De la même façon, on peut créer un profil au nom d'une personne de l'école ou du voisinage et lui nuire en la ridiculisant ou en envoyant des méchancetés en son nom.

Font partie des formes criminelles d'usage abusif de données ce qu'on appelle le phishing, le vol de données à des fins criminelles, et de plus le cyberstalking et le cyberbullying.

Phishing
Le terme Phishing désigne le vol de données à l'aide de courriels et de formulaires Web falsifiés : on fait croire à l'utilisateur qu'il communique ses données à l'aide d'un formulaire fiable (par ex. de sa banque) et en fait il fournit ses données personnelles (par ex. identifiants, mots de passe, code TAN, codes PIN, etc.) à un voleur de données.

Cyberstalking
Le cyberstalking (la traque cybernétique) est un vieux phénomène dans un nouvel emballage : les possibilités de contact électroniques des SRS peuvent être détournées de façon malveillante en vue de harceler quelqu'un. En outre, la masse de données que les utilisatrices et les utilisateurs communiquent sur eux-mêmes peut tout à fait conduire à ce que quelqu'un découvre l'adresse de sa victime, apprenne à connaître ses habitudes de vie et devienne capable de persécuter la personne dans la vie réelle.

Cyberbullying
Le cyberbullying (harcèlement, intimidation cybernétique) est la version internet d'un phénomène connu depuis longtemps dans la réalité. L'agres- seur peut se dissimuler derrière un profil falsifié et utiliser les possibilités offertes par les SRS pour harceler quelqu'un ou pour l'humilier. À cela s'ajoute que d'autres membres de la communauté peuvent en être témoins, ce qui augmente le dommage subi par la victime.

Recommandations

Utilisateures et utilisatrices
- Utilisez des identifiants et des mots de passe différents pour des services différents.
- Dans votre profil, aux paramètres qui vous sont propres, choisissez des options conformes à la protection des données. N'autorisez l'accès à vos informations et vos photos qu'à un cercle limité de personnes. Ne mettez pas de contenus délicats sur l'internet.
- Soyez prudents en publiant vos coordonnées (nom, adresse, numéro de téléphone) et d'autres informations personnelles (par ex. des convictions politiques) sur un SRS. Utilisez des pseudonymes.

– Avant de les publier, demandez-vous toujours si vous aimeriez être confrontés avec ce type de données dans un entretien d'embauche – fût-ce même dans dix ans.
– Respectez la sphère privée de tiers, ne publiez pas leurs coordonnées, n'inscrivez pas non plus leurs noms sur des photos.
– Informez-vous sur le fournisseur du portail et sur la façon dont il sécurise la sphère privée des utilisateurs. Le service dispose-t-il d'une protection des données ou d'un sceau de sécurité ?
– Lisez les conditions générales du fournisseur. Observez de manière critique le comportement du fournisseur.

Directions d'école
– Les utilisatrices et utilisateurs de services de réseautage social doivent être sensibilisés aux campagnes d'information concernant les dangers liés à ce type de services.
– Attention aux interdictions : plutôt que d'interdire l'utilisation de SRS, les écoles devraient (partiellement) l'autoriser ; de la sorte, le réseautage social ne se déroulera pas de façon totalement incontrôlée. En outre, l'information d'apprenants, d'enseignants et de parents pourrait ainsi aller de pair.

Informations européennes sur la protection des données
Plusieurs commissions européennes de protection des données se sont déjà occupées en profondeur de la thématique des réseaux sociaux.

Vous trouverez de plus amples informations sur :
→ European Network and Information Security Agency ENISA. Position Paper No. 1 : Security Issues and Recommendations for Online Social Networks. (PDF)
Editor : Giles Hogben, October 2007.
→ Report and Guidance on Privacy in Social Network Services « Rome Memorandum », Mars 2008 (PDF)

Courriel

Espaces adresse
Il arrive souvent qu'atterrissent dans la boîte de réception des courriels où l'ensemble des destinataires est visible : les adresses ayant été insérées dans l'espace « A » ou « Cc ». Pour des raisons de transparence, cette manière de procéder peut être tout à fait sensée. Par exemple dans un projet où plusieurs personnes sont concernées ou dans des constellations similaires où les destinataires se connaissent déjà. Toutefois, selon le contenu et la situation, une telle communication globale des destinataires peut être délicate, en particulier quand les destinataires ne se connaissent pas mutuellement. Dans de tels cas, l'expéditeur
doit utiliser la fonction « Cci » (copie carbone invisible). De cette façon, les différents destinataires ne savent pas qui a aussi reçu le message.

Recommandation
Lors d'un envoi de courriel à des personnes qui ne se connaissent pas mutuellement, toujours inscrire les adresses des destinataires dans l'espace « Cci ».

Risque de spam et de phishing
Tenez compte en outre du fait que toute diffusion d'adresses courriel augmente le risque de spam et le risque d'attaques de phishing : dans ce cas, un courriel trafiqué, contenant des instructions et liens internet, fait croire au destinataire qu'il communique avec un expéditeur digne de confiance.

Recommandation
Vous devriez ignorer les courriels contenant des instructions et des liens.

Blogs

La loi sur la protection des données interdit toute révélation de données concernant des tierces personnes sans accord écrit préalable des personnes concernées.

Recommandations

Quand vous trouvez sur un blog étranger des informations concernant votre propre personne, que vous voulez voir disparaître, contactez à cet effet en premier lieu l'auteur par formulaire de contact ou par courriel. Si cela ne donne rien, prenez contact avec le fournisseur du blog. Ne publiez en aucun cas un commentaire sur une information non souhaitée concernant votre personne. Un commentaire serait contre-productif parce qu'il renforcerait l'intérêt des lecteurs du blog pour l'information non souhaitée.

Dans le cas de blog personnel, la tentation est toutefois particulièrement grande de lancer des informations personnelles sans être conscient des dangers auxquels on s'expose. La révélation d'informations concernant sa propre personne n'est pas touchée par le droit relatif à la protection des données puisqu'elle est volontaire. Elle peut cependant avoir pour la personne qui les divulgue des conséquences négatives, comme nous l'avons évoqué dans le cadre des réseaux sociaux.

Règles de conduite

Voici des règles de conduite assurant une protection étendue :

– En vue de protéger votre blog privé d'une publicité excessive, limitez votre lectorat. Utilisez à cet effet les différentes possibilités que vous avez de protéger tout votre blog ou certaines entrées à l'aide de mots de passe ou n'en permettez l'accès qu'à des hôtes identifiés.

– Utilisez toujours des pseudonymes et ne communiquez pas de détails qui autorisent des déductions sur votre personnalité, vos habitudes, votre domicile ou votre lieu de résidence, votre employeur, etc.
– Utilisez des techniques qui préservent l'anonymat. Invisiblog.com par ex. propose gratuitement un hébergement de blog anonyme. Pour empêcher que votre adresse IP ne soit identifiée, le réseau TOR (cf. : → fr.wikipedia.org) est une ressource. Il existe en outre quantité de fournisseurs de logiciels qui se sont spécialisés dans la technique de l'anonymat, tels que par ex. → anonymizer.com.
– Utilisez un serveur Ping, si vous souhaitez rester anonymes, tandis que vous passez votre blog à différents moteurs de recherche. Pingomatic.com propose un service de ce type.
– Empêchez que des moteurs de recherche ne trouvent votre blog. Utilisez pour cela un un fichier texte Robots (robots.txt).
– Enregistrez anonymement votre nom de domaine. Online Policy Group (OPG) par ex. propose l'enregistrement anonyme.

Conseils

Celui qui le veut n'a pas problèmes à se déplacer anonymement sur Internet, dans la mesure où par principe il ne transmet ses données qu'en les codant.

Surfer : utilisez le réseau Tor (→ torproject.org), les données sont codées.

Bourses d'échange : sur des réseaux comme Bittorrent, on télécharge anonymement, grâce par ex. au service gratuit Bit Blinder (→ bitblinder.com) ou en payant pour des fournisseurs comme Torrent Privacy (→ torrentprivacy.com).

Courriel : les courriels se transmettent de façon sûre par « https: » chez tout fournisseur sérieux. En recourant à PGP, on peut coder les textes.

Source : Christian Bütikofer, Tagesanzeiger 18.07.2009

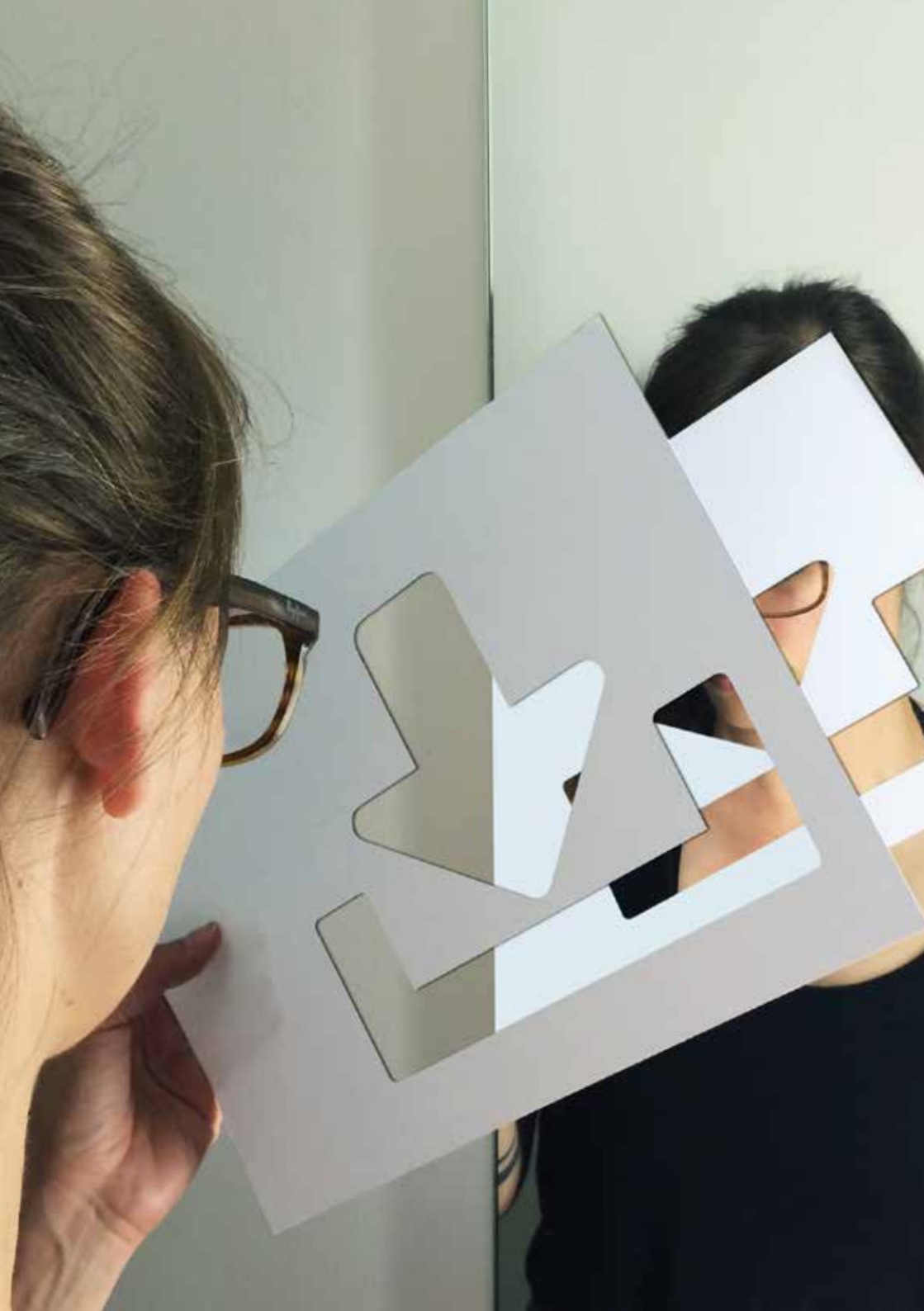
Appareils photo numériques et de portables

Prises de vues et de sons non autorisées
Les écolières et les écoliers ainsi que leurs parents sont soumis à la loi fédérale sur la protection des données. Celle-ci interdit les prises de vues et de sons qui ne sont pas justifiées par un accord personnel, une loi ou un intérêt privé ou officiel majeur. Les prises de vues et de sons enfreignent en règle générale les droits de personnalité, en particulier quand de tels enregistrements paraissent sur l'internet en combinaison avec des commentaires (par ex. sur les sites web ou les blogs d'écolières ou d'écoliers). Il appartient donc aux enseignants et aux directions d'école d'attirer l'attention des écolières et des écoliers sur ce problème et de leur indiquer en outre que la diffamation, la calomnie ou l'injure sont des actes punissables.

Prise de vues par les parents
Les prises de vues par les parents à l'occasion d'événements scolaires (fêtes, théâtre, manifestations sportives, jours de visite à l'école ou lors de classes vertes, etc.) concernent la relation juridique entre l'enfant pris en photo (ou ses parents) et la personne qui prend la photo. Il s'agit de ce fait en premier lieu d'une affaire de droit privé. Pour autant que les parents soient informés de l'événement qui est public ou accessible à d'autres parents et tant que des enseignants ne constatent pas de graves infractions à la loi (par ex. si des parents harcèlent d'autres enfants par des prises de vues), il n'existe aucun devoir d'intervenir contre la prise de vues par les parents. C'est en principe l'affaire de ceux qui sont filmés ou photographiés (ou de leurs parents) de faire valoir leurs droits et de se défendre contre une prise de vues illégale.

Visite isolée dans la classe non annoncée

Lors de visites isolées dans la classe qui n'ont pas fait l'objet d'une annonce, des prises de vues ne doivent pas avoir lieu puisque dans ce cas, au contraire d'événements scolaires, les parents n'étaient pas informés de prises de vues et ne pouvaient dès lors pas faire valoir leurs droits. Du point de vue du droit relatif à la protection des données, les personnes concernées peuvent prendre des mesures juridiques pour la protection de la personnalité dans le cas de prises de vues et de sons non autorisées. Quand l'abus est flagrant, on peut exiger l'effacement immédiat des vues prises et procéder soi-même à l'effacement en cas de refus.



Direction des affaires scolaires

Ce chapitre s'adresse en premier lieu aux directions d'écoles. Il explique les principes de la protection des données et attire l'attention sur les aspects du droit relatif à la protection des données liés à la gestion des données personnelles d'apprenants et d'enseignants dans l'utilisation de technologies basées sur le web. On traite tout à la fin un aspect plutôt technique concernant la sécurité avec WLAN.

Protection des données et secret de fonction

En tant que collaborateurs d'établissements publics, les enseignants et les directions d'écoles exercent des fonctions au service du public. Ils sont de ce fait considérés comme membres de services administratifs et sont soumis dans cette fonction aux dispositions de la loi cantonale du lieu sur la protection des données. En outre, les règles du droit pénal sur le secret de fonction (art. 320 du code pénal) obligent également les enseignants au respect de la personnalité des écolières et des écoliers.

Secret de fonction

Les règles du droit pénal concernant le secret de fonction obligent les collaborateurs d'établissements publics à ne pas communiquer des secrets de fonction. Un secret de fonction est un fait non communément connu dont un membre d'un service administratif a pris connaissance dans l'exercice de sa fonction. Les règles concernant le secret de fonction sont, d'une part, plus étendues que les règles sur la protec-

tion des données personnelles parce qu'en relèvent aussi des données non-personnelles (par ex. les questions budgétaires d'une école). D'autre part, leur champ d'application est plus limité du fait qu'elles règlent seulement la communication de secrets et non la collecte, la conservation, la destruction etc. de données.

Les enseignants sont donc tenus de ne pas communiquer les « secrets » dont ils ont eu connaissance en exerçant leur activité. Une autorisation ou une obligation légales peuvent toutefois en justifier la communication.

Secret professionnel

Conformément à l'art. 321 du code pénal, le secret de fonction est à distinguer du secret professionnel. Sans doute, il doit lui aussi protéger des « secrets », toutefois il ne concerne pas des membres de services administratifs mais certains genres de professions, en particulier les ecclésiastiques, les avocats, les notaires, les médecins, les dentistes, les pharmaciens, les sages-femmes. Certaines personnes sont concernées par les deux obligations au secret, les médecins scolaires par ex.

Lois cantonales sur la protection des données

Les lois cantonales sur la protection des données déterminent comment les administrations cantonales doivent traiter les données personnelles. Sont ainsi réglées la collecte, la conservation, la modification, l'association, la communication ou la destruction de données personnelles. Les données qui ne se réfèrent pas à des personnes ne tombent pas dans le domaine d'application des lois. Si des collaborateurs d'établissements publics enfreignent les dispositions légales, la personne concernée peut introduire une requête visant à ce que les données collectées, erronées ou illégales, soient corrigées ou effacées. La violation du droit relatif à la protection des données (par ex.

la communication illégale de données personnelles ou la perte de données personnelles à conserver) peut en outre conduire à des mesures disciplinaires internes (par ex. le blâme). Si la violation entraîne en plus un dommage, cela peut justifier des obligations à des dommages-intérêts pour l'école (en règle générale, c'est la commune qui en répond) ou pour l'enseignant (dans le cas de dommages provoqués de façon intentionnelle ou à la suite d'une faute lourde.)

Données à l'usage personnel de l'enseignant

Les données personnelles qu'un enseignant traite exclusivement pour son usage personnel ne tombent pas sous le coup de la loi sur la protection des données. Il s'agit dans ce cas d'aides pour le travail tels que des notes pour la préparation d'une réunion de parents ou des inscriptions sur un agenda. Le fait que ces données soient exclues de la loi sur la protection des données a pour conséquence que des personnes concernées n'ont aucun droit de regard sur ces données. Il n'en suit pour autant en aucune façon que ces données puissent être communiquées. En conséquence, ces aides personnelles doivent être elles aussi protégées contre l'accès de tiers et on ne peut les laisser traîner sans y faire attention. Si par exemple des notes d'entretien contiennent des informations délicates sur un écolier, il faut les conserver sous clé dans un bureau ou une armoire. Les contrôles d'apprentissage en particulier font partie également des données personnelles des écolières et des écoliers tant qu'ils peuvent leur être attribués. Si l'on enlève le nom et tous les autres éléments permettant qu'ils soient reliés à une écolière ou à un écolier identifiés, il ne s'agit plus alors de données personnelles.

Principes du droit de protection des données

Les dispositions contenues dans les lois cantonales sur la protection des données s'adressent à toutes les administrations du canton. Elle ne ciblent donc

pas spécialement le traitement de données personnelles à l'école. C'est pourquoi il est important de connaître les principes de la loi sur la protection des données. Il faut en déduire des solutions concrètes pour l'école au quotidien.

Légitimité du traitement des données personnelles
Le traitement de données personnelles doit toujours être légitime. À cet égard, la loi sur la protection des données fait la distinction entre données personnelles « normales » et « sensibles » (voir ci-dessus). En simplifiant, cela revient à dire que la distinction implique que l'on observe des règles plus sévères lors du traitement de données personnelles « sensibles » que lors du traitement de données personnelles « normales ».

Traitement de données personnelles normales
Des données personnelles « normales » peuvent être traitées, quand
– une loi (le niveau de l'ordonnance est une base de référence suffisante) l'autorise ou
– le traitement est indispensable à l'exécution d'une mission légale (c'est-à-dire que l'exécution d'une mission légale serait considérablement entravée sans le traitement de données envisagé).

Traitement de données personnelles sensibles
Des données personnelles « sensibles » ne peuvent être traitées que si en plus
– une loi (le niveau de la loi est ici requis comme base de référence) le prévoit clairement ou
– l'exécution d'une mission légale rend le traitement de données impérativement nécessaire (c'est-à-dire que l'exécution d'une mission légale serait rendue impossible sans le traitement de données envisagé) ou
– la personne concernée a donné expressément son accord.

Principe de finalité
Les données issues du domaine scolaire rassemblées selon les règles expliquées ci-dessus ne peuvent en principe être traitées qu'en vue des buts pour lesquels elles ont été collectées ou auxquels les écolières et les écoliers ou les parents doivent s'attendre. Dans le cadre scolaire, ces buts résultent des missions de l'école maternelle et de l'école primaire citées plus haut. Pour cette raison il est par exemple absolument exclu de publier des listes de classes à des fins commerciales.

Principe de proportionnalité
De ce principe il découle d'une part que des données personnelles, comme on l'a indiqué plus haut, ne peuvent être traitées que dans la mesure où c'est nécessaire à l'accomplissement d'une tâche légale. Rassembler des données en vue de constituer des réserves (par ex. la collecte de données dont la destination n'est pas connue au moment de la collecte) est illégal. Le principe de proportionnalité exige d'autre part qu'entre diverses possibilités de traitement des données il faille toujours choisir celle qui représente l'intervention la moins lourde dans les droits de personnalité de la personne concernée.

Principe de bonne foi
Du principe de bonne foi il découle que le traitement de données doit être visible et transparent. Un traitement de données occulte est dès lors interdit. Il faut que les écolières et les écoliers ainsi que les parents puissent s'apercevoir sans effort particulier que l'on traite des données personnelles les concernant et savoir quelle données sont traitées. Aussi, en règle générale, les données personnelles sont elles à collecter auprès des écolières et des écoliers concernés ou auprès de personnes ayant la garde et non auprès d'une autre personne privée ou d'une administration.

Principe d'exactitude
Ce principe donne aux écolières et aux écoliers ainsi qu'aux parents le droit de faire corriger ou de détruire des données personnelles inexactes les concernant.

Sécurité des données
Celui qui traite des données personnelles est aussi responsable de leur protection.

Conditions requises
L'accord peut être une base de la légitimité du traitement des données. Toutefois, l'accord donné pour le traitement de données ne peut concerner qu'une situation très précise, strictement définie dans l'espace et dans le temps. Jamais il ne sera global ni ne permettra un traitement des données à durée indéterminée. La personne concernée est en règle générale l'écolière ou l'écolier. Puisqu'un accord ne peut être donné que par une personne capable de jugement, il faut élucider d'abord à quelles conditions des écolières et des écoliers sont capables de jugement. Une deuxième étape prévoit que l'on vérifie les exigences concernant la forme de l'accord. Est capable de jugement au sens du code civil celui qui n'est pas hors d'état d'agir raisonnablement en raison de son bas âge ou à la suite de « maladie mentale, faiblesse mentale, ivresse ou situations semblables ». Ceci signifie qu'un enfant ou un jeune est capable de jugement quand il peut former sa propre décision et agir selon cette décision. La loi ne connaît pas de limites d'âge fixes. L'horizon d'expérience d'un enfant qui grandit est variable selon son degré de développement. Les écolières et les écoliers de l'école maternelle et de l'école primaire ont en règle générale entre 4 et 16 ans. Lors de ce laps de temps, la capacité de former sa propre décision et d'agir selon cette décision varie considérablement. Même parmi des enfants du même âge, cette faculté peut être développée de façon très variable.

En principe, on peut toutefois dire ce qui suit :
Comme il est souvent difficile même pour des adultes d'évaluer les conséquences d'un traitement de données, ceci est d'autant plus difficile pour des enfants. C'est pourquoi, concernant le traitement de données personnelles « sensibles » ainsi que de données personnelles « normales » pouvant compromettre leurs droits de personnalité et entraîner des suites qu'il est difficile d'évaluer, la capacité de juger ne peut leur être reconnue au plus tôt que vers la fin du temps de l'école obligatoire. Il est recommandé avant cela de demander l'accord des responsables légaux. Ce n'est que dans des cas très clairs et très simples qu'un enfant peut évaluer les conséquences d'un traitement de données et se former à cet égard une décision propre.

Accords
Pour ce qui est des accords, on distingue ceux qui sont oraux et ceux qui sont écrits, les accords formels et les accords tacites. Quand on traite des données personnelles « normales », qui ne constituent pas une menace considérable pour les personnes concernées, un accord tacite peut suffire. Un accord tacite est supposé quand aucune objection n'est élevée contre un traitement de données prévu réglementairement ou communiqué sans restriction. Afin de pouvoir en produire la preuve, des accords devraient toutefois être autant que possible demandés par écrit.

Données transmises au fournisseur d'accès

En principe, une transmission de données n'est autorisée que dans la mesure où la commune concernée le permet expressément dans son règlement sur la protection des données. Les règlements cantonaux modèles pour la protection des données prévoient en règle générale une interdiction de la communication de données à des fins commerciales. Il existe toutefois des communes dans lesquelles des décrets communaux permettent de telles communications de données.

Au cas où un tel décret communal existe, la communication est permise (par ex. règlement pour la protection des données de la commune de Thun, art. 3 al. 1).

Renseignements sous forme de listes

Les renseignements sous forme de listes sont des données classées systématiquement, par ex. une liste de noms, d'adresses ou d'adresses électroniques de toutes les écolières et tous les écoliers d'une école ou de tous les responsables légaux des écolières et des écoliers d'une école. On ne peut en principe les transmettre que si la commune compétente le permet expressément dans un règlement concernant la protection des données. Les personnes concernées doivent toutefois être informées avant la première communication dans le but de leur permettre de faire valoir des intérêts majeurs. Cette manière de faire est particulièrement recommandée si l'on soupçonne que l'on puisse faire un usage abusif des données personnelles (par ex. pour du marketing). S'il vous faut l'accord des responsables légaux ou des écolières et des écoliers pour une transmission de données, sollicitez dans ce cas de façon active un assentiment écrit, formel. N'utilisez pas de formules comme « sauf avis contraire de votre part jusqu'au … nous supposons que vous êtes d'accord ». [Bâle-Campagne : notice sur la protection des données]

Demandes de renseignements à des fins commerciales

Les demandes de renseignements – en particulier, celles qui proviennent de fournisseurs de services web – sont à traiter avec la plus grande réserve. Les conditions générales des fournisseurs de services web sont à lire de façon très attentive (par ex. de fournisseurs de logiciels du type Software-as-a-Service), car ce que le dépliant publicitaire présente comme une offre séduisante pour l'école peut être lié à des conditions qui créent des dépendances indésirables ou sont douteuses au niveau du droit de la protection des données.

Sites web scolaires

Celui qui rend accessibles sur l'internet des données concernant des écolières et des écoliers ou des enseignants, traite ce faisant des données personnelles. Il faut donc respecter aussi dans ce contexte les principes déjà cités. Les données publiées sur l'internet sont consultables dans le monde entier et l'on peut s'en servir aux fins les plus variées. C'est pourquoi il faudrait procéder avec beaucoup de prudence, pour les images en particulier. Les exigences en matière de sécurité sur internet sont en outre à respecter.

Directives pour les sites web scolaires
En principe, les données suivantes peuvent être publiées sans problèmes :
Informations sans liens avec des personnes :
– Agenda scolaire
– Organisation de l'école
– Modèles
– Adresses d'institutions proches de l'école
– Règlements internes
Reportages sans liens avec des personnes :
– Événements scolaires ou de classe,
– Représentations théâtrales
– Fêtes scolaires
– Semaines thématiques
– Excursions
Travaux d'écolières et d'écoliers publiés de façon anonyme.

Données personnelles
Si des personnes concernées ne sont pas d'accord avec la publication de quelque donnée personnelle que ce soit – même celles que l'on dit non problématiques – ou s'ils retirent par après leur accord, il faut donner suite à leur droit de suppression dans les plus brefs délais et retirer sans tarder le contenu en question du site web.

Données non problématiques
En règle générale, les données suivantes ne posent pas de problèmes :
– Nom de famille
– Prénom
– Fonctions

Accord préalable, exprès et de plein gré nécessaire
Les données personnelles sensibles qui suivent ne peuvent en principe être publiées sans un accord préalable, exprès et de plein gré :
– Adresses privées
– Adresse électronique
– Photos de personnes, si on peut identifier les personnes
– Informations sur les hobbys et les matières préférées
– Travaux scolaires avec référence de personnes

Données sensibles
Malgré un accord préalable, exprès et de plein gré, il faudrait renoncer à publier les données suivantes sur un site web scolaire :
– Adresses privées
– Numéros de téléphone
– Adresse électronique
– Photos sur lesquelles on peut identifier des personnes.

Liens
Les liens ne peuvent pas renvoyer à des pages illégales. Ce sont des pages qui présentent par ex. des contenus pornographiques, racistes ou déshonorants. Tous les liens doivent être contrôlés périodiquement sur ce point.

Webcams
Il faut renoncer au recours à des webcams pour la transmission d'images de personnes identifiables.

Formulaires de contact
Au cas où un site web mettrait à disposition une possibilité de contact par courriel ou par formulaire web, il faut attirer l'attention sur le fait que la liaison n'est pas sécurisée et que des informations confidentielles ne peuvent être transmises en ligne.

Enregistrement de visites, cookies
Un enregistrement des visiteurs de pages est interdit. Si la page installe des cookies, il faut expliquer dans quel but.

Livres d'hôtes, forums
Des livres d'hôtes et des forums ne doivent pas être utilisés, si des tiers peuvent entrer directement leurs contributions sur la page sans examen préalable par l'école. L'école doit empêcher de possibles diffamations par des tiers.

Précisions concernant la sécurité avec WLAN

WLAN signifie wireless local area network, en français réseau local sans fil. Les WLANs servent en particulier à permettre l'accès à Internet avec des appareils mobiles dans les hôtels, les restaurants, les gares, le domicile ou dans des firmes. Les WLANs relient ordinateurs, imprimantes, scanners et autres appareils et permettent aussi la plupart du temps une connexion internet. Ces appareils sont reliés entre eux par ce qu'on appelle des access points. WLAN est standardisé par l'IEEE (→ Wikipedia : IEEE), dans la famille de normes 802.

Que ce soit dans les firmes ou dans les ménages privés, les WLANs jouissent aujourd'hui d'une grande popularité, car ils permettent beaucoup de flexibilité sans enchevêtrement de câbles en assurant des débits de transfert très élevés. Les portées entre le point d'accès et les appareils vont de quelques mètres à plusieurs douzaines de mètres, selon la puissance d'émission et la texture des murs.

Les avantages indiscutables des WLANs obligent par ailleurs à des mesures techniques et organisationnelles particulières. Car les signaux radio sont en principe accessibles dans tout le secteur couvert par un WLAN, c.-à-d. donc aussi pour des tiers non autorisés. Il s'agit dès lors en premier lieu de protéger l'accès à des données confidentielles contre de telles personnes tierces. Par ailleurs, il ne faut pas non plus que des personnes non autorisées puissent réduire la bande passante du WLAN pour l'accès à l'internet en se comportant comme des profiteurs ou faire de celle-ci un usage absolument abusif en vue d'actions illégales.

Mesures de sécurité

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI de la Confédération propose concrètement les mesures suivantes de sécurisation des données et de protection des données :

- Changer le mot de passe standard pour la gestion du point d'accès.
- Utiliser si possible du câble, par ex. ethernet, pour la gestion du point d'accès et couper la fonction pour la gestion par radio.
- Couper des fonctions possibles pour la gestion à distance du point d'accès via l'Internet.
- Changer l'identification du réseau (SSID) et couper l'émission de l'identification du réseau (SSID Broadcast), afin que le point d'accès demeure caché à des personnes extérieures.
- Mettre en œuvre le codage le plus puissant qui soit pris en charge par le point d'accès et par les terminaux (de préférence WPA 2 ou WPA). Utiliser la longueur de clé la plus longue ou un mot de passe puissant. Le standard antérieur Wired Equivalent Privacy (WEP) (= confidentialité équivalente au filaire) offre une sécurité insuffisante et ne devrait plus être utilisé.
- Si c'est praticable dans le réseau et si l'on dispose du savoir nécessaire, utiliser des adresses IP plutôt que le protocole de configuration DHCP (Dynamic Host Configuration Protocol).
- Utiliser le filtre MAC, en vue de limiter l'accès à WLAN aux terminaux identifiés dans le réseau.
- Quand la fonction est présente dans le point d'accès et si l'activité du réseau n'en est pas restreinte, limiter la puissance d'émission pour diminuer la portée du WLAN.
- N'allumer le WLAN qu'en cas d'emploi.

Liens utiles à propos de WLAN

→ MELANI : Réseaux radio (WLAN)
→ OFSP : WLAN
→ Wikipedia : Wi-Fi Protected Access

educa.ch
Institut suisse des médias pour la formation et la culture
Erlachstrasse 21 | Case postale 612 | CH-3000 Berne 9

Téléphone : +41 (0)31 300 55 00
info@educa.ch | www.educa.ch