PFPD

Préposé Fédéral à la Protection des Données
Eidgenössischer DatenSchutzBeauftragter
Incaricato Federale per la Protezione dei Dati
Incumbensà Federal per la Protecziun da Datas
Swiss federal Data Protection Commissioner

EDSB

Respect de la loi sur la protection des données (LPD) au quotidien

GRIFES: Groupe Informatique et Sécurité
Genève, le mardi 28.01.2003

PFPD

Votre serviteur…

EDSB

- Pierre-Yves.Baumann@edsb.admin.ch
- « Informéthicien » chez le PFPD
- Qualified BS 7799-2:2002 Lead Auditor (ISMS)
- Ex prof. de math et informatique HES-BE/St-Imier
- Ex resp. Informatique chez Cabloptic SA
- Formation de mathématicien (Univ. Neuchâtel)

Thèmes abordés

PFPD EDSB

1. Organisation et tâches du PFPD
2. Loi fédérale sur la protection des données
3. Protection et sécurité des données
4. Cryptographie moderne (PGP, EDSB-Office)
5. Anonymisation et pseudonymisation des données
6. Utilisation d'Internet/Email au lieu de travail
7. Questions

Organisation du PFPD

PFPD EDSB

- Direction: Hanspeter Thür
  (Suppléant: Dr. Jean-Philippe Walter)

- 3 équipes pour le conseil juridico-technique par secteur d'activités
- 1 équipe pour la diffusion de l'information (presse)
- 1 centre de compétence en nouvelles technologies
- 1 secrétariat permanent

Rattachement administratif à la Chancellerie fédérale!

Tâches du PFPD

PFPD EDSB

- Conseil technique et juridique
- Formation/Sensibilisation
- Information (www.edsb.ch, brochures…)
- Contrôle/Audit
- Tenue du registre des fichiers
- Collaboration avec les cantons et l'étranger (UE)

Secteurs public et privé!

Fondements de la protection des données

PFPD EDSB

- **CEDH Art. 8**:
  1. *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
  2. *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*

PFPD

Fondements (suite)

EDSB

- **CF Art. 13**: (RS 101; 18.04.1999)
  [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.
- **LPD Art. 1**: (RS 235.1; 19.06.1992)
  La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données.

PFPD

LPD: définitions

EDSB

- Art. 3a: Données personnelles
  Toutes les informations qui se rapportent à une personne identifiée ou identifiable
- Art. 3b: Personne concernée
  La personne physique ou morale au sujet de laquelle des données sont traitées
- Art. 3c: Données personnelles sensibles
  - opinions ou activités religieuses, philosophiques, politiques ou syndicales
  - santé, sphère intime, appartenance à une race
  - mesures d'aide sociale
  - poursuites ou sanctions pénales et administratives

PFPD

LPD: définitions…

EDSB

- Art. 3d: Profil de la personnalité
  Un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique
- Art. 3e: Traitement de données
  Toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données

PFPD

LPD: définitions……

EDSB

- Art. 3f: Communication de données
  Le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant
- Art. 3g: Fichier
  Tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée
- Art. 3i: Maître du fichier
  La personne privée ou l'organe fédéral qui décide du but et du contenu du fichier

PFPD

LPD: principes généraux

EDSB

- Art. 4.1 Collecte licite
- Art. 4.2 Traitement selon bonne foi et proportionnalité
- Art. 4.3 Traitement conforme au but indiqué
- Art. 5 Exactitude/Rectification des données
- Art. 6 Communication à l'étranger (déclaration)
- Art. 7 Sécurité des données (technico-organisationnel)
- Art. 8 Droit d'accès (demande au maître du fichier)
- Art. 11 Registre des fichiers (tenu par le PFPD)

PFPD

Sécurité des données

EDSB

- La sécurité des données couvre les domaines suivants:
  - Disponibilité
  - Intégrité
  - Confidentialité
  - Traçabilité
- En anglais, on fait en outre la distinction entre Safety et Security, soit resp. entre les mesures contre des défaillances non intentionnelles (pannes…) ou intentionnelles (sabotage…).

PFPD

Protection des données

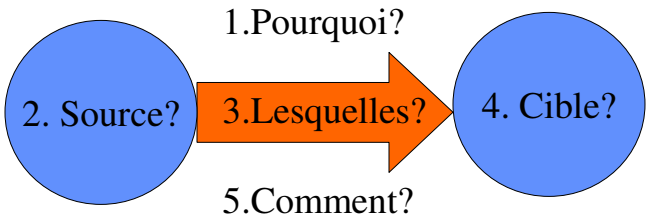
EDSB

- La protection des données vise plus particulièrement à atteindre les objectifs suivants:
  - lutte contre les détournements de finalité
  - économie/non-production de données
  - pseudonymisation/anonymisation des données
  - classification des données selon leur sensibilité (profils de personnalité)
  - chiffrement des données sensibles mémorisées!
  - analyse des flux de données internes et externes
  - journalisation des traitements (sensibles!) => Surveillance…
  - délai de conservation des données récoltées
  - exécution du droit d'accès

PFPD

5 questions de protection (en cas de communication)

EDSB

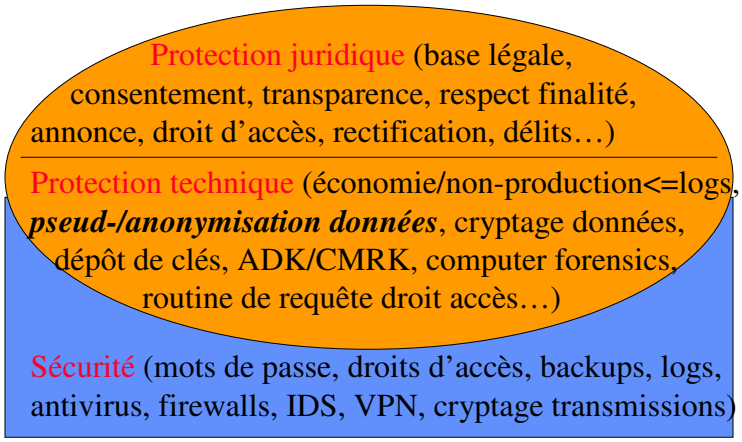


1. Licéité ? Finalité !
2. Authentification, Consentement ? Droit d'accès!
3. Proportionnalité ? Économie, Pseud-/Anonymisation !
4. Disponibilité, Confidentialité, Exactitude, Retransmission?
5. Inviolabilité, Intégrité ? Chiffrement !

PFPD

Sécurité + Protection

EDSB



PFPD

Sécurité ‡ Protection !

EDSB

- Une haute sécurité des données ne se traduit pas forcément par une bonne protection des données, tandis qu'une haute protection des données n'est guère possible sans une sécurité élevée des données! Ex: données personnelles sauvées sous forme chiffrée, mais superflues et/ou acquises à l'insu de l'intéressé!
- En d'autres termes, la sécurité des données est un des moyens essentiels pour atteindre une protection adéquate des données…

But(s) de la cryptographie

- Transformation réversible (chiffrement, cryptage, codage) des données visant à les protéger contre toute prise de connaissance (*confidentialité*) ou modification (*intégrité*) indue! Le procédé de transformation repose sur un secret (table, nombre, mot de passe) habituellement désigné comme une clé cryptographique.
- Cachetage ou signature numérique de données (méthodes d'authentification avec contrôle d'intégrité)

BY-17 28.01.2003

Cryptographie symétrique

- On utilise la même clé aussi bien pour le chiffrement/cachetage que pour le déchiffrement/décachetage!
- Si ces deux opérations ne sont accomplies par la même personne, il faut avoir/utiliser un canal sûr pour l'échange de la clé!
- Longueur de clé réputée sûre: 128/256 bits
- Algorithmes connus: 3DES, CAST, IDEA, AES; HMAC

BY-18 28.01.2003

Cryptographie asymétrique

PFPD EDSB

- On recourt à une paire de clés formée d'une partie privée et d'une partie publique, chaque partie pouvant être utilisée isolément pour accomplir une fonction cryptographique duale.
- La relation mathématique entre les deux parties de la paire de clés est déterminante, sans qu'une partie ne soit déductible de l'autre!
- Longueur de clé réputée sûre: 1024/2048 bits
- Algorithmes connus: RSA, El-Gamal, DH; DSS

Anneaux de clés asymétriques

PFPD EDSB

- Toutes les clés utiles sont conservées dans un anneau privé et un anneau public.
- Chaque clé privée est mémorisée dans un format chiffré symétriquement et son accès est ainsi protégé par une expression de passe!
- Chaque clé publique est en outre exportée dans un format alphanumérique, afin de pouvoir être transmise aux intéressés par un canal quelconque.

Infrastructure à clés publiques

- Mise à disposition avec certification (numérique) de clés publiques.
- La certification de clés publiques appartenant à des personnes qui se rencontrent et/ou connaissent est pratiquement superflue…

Problèmes plus subtiles:
- révocation de clés
- dépôt central de clés (key escrow)
- clé additionnelle de déchiffrement (ADK/CMRK)
- certifications croisées (entre différentes autorités)

Pretty Good Privacy

- Développé et distribué par Phil Zimmerman dès 1991
- PRZ -> ViaCrypt -> PGP Inc. -> NAI -> PGP Corp. (2002)
- Code source publié (versions 2.x, 6.x et 8.x)
- Version freeware téléchargeable!
- Algorithmes cryptographiques standards
- Mode hybride: interne symétrique, externe asymétrique
- PKI informelle de type « Web of Trust » basée sur la signature numérique « mutuelle » des clés publiques
- Fournisseurs de services Web (gratuits): www.mailvault.com, www.hushtools.com/, lok.com ?

PGP: chiffrement d'emails

PFPD EDSB

- L'expéditeur chiffre les données avec les clés publiques du (des) destinataire(s) <- la sienne aussi!
  => Affichage sécurisé: TEMPEST
  => Fichiers joints peuvent aussi être chiffrés!
- Le destinataire déchiffre les données reçues au moyen de sa clé privée (protégée par expr. de passe)

Les courriels doivent pouvoir être conservés sous forme chiffrée, de façon à les tenir à l'abri de regards indiscrets (ex: administrateurs de la messagerie).

PGP: signature d'emails

PFPD EDSB

- L'expéditeur signe numériquement les données avec sa clé privée (protégée par expr. de passe)
  => il ne pourra pas répudier son envoi!
- Le destinataire vérifie la provenance et l'intégrité des données reçues au moyen de la clé publique de l'expéditeur!
- La signature a lieu avant le chiffrement optionnel des données, tandis que la vérification n'est possible qu'après leur déchiffrement…

Notre système EDSB-Office

PFPD EDSB

- Système sécurisé de gestion des affaires et dossiers (planif. temps et projets, stat, base de connaissances)
- Application Client/Server développée en Visual-Basic qui appelle MS-Office (passerelle Outlook!) et PGP
- Différents groupes de chiffrement assurent un cloisonnement des documents selon leur niveau de confidentialité (Direction: inaccessibles pour Admin!)
- Données mémorisées sous forme chiffrée dans une base de données traditionnelle (SQL-Server)
- Recherche en plein texte (indexation des contenus!)
- Haute disponibilité (serveurs clusterisés) en été 2003!

BY-25 28.01.2003

Alternative à PGP

PFPD EDSB

- GNU Privacy Guard V1.2.x (www.gnupg.org)
- Standard OpenPGP (IETF)
- Outils additionnels:
  - Windows Privacy Tray (www.winpt.org)
  - WinPTEE (Explorer Extension)
  - GPGshell (Graphical interface)
  - G DATA GnuPG-Plugin (Outlook)
  - GPGOE (Outlook Express)
  - EudoraGPG (Eudora)
  - QDGnuPG (Pegasus)
  - BkGnuPG (Becky)
  - EnigMail (Mozilla/Netscape)
  - Gnuzza (CryptChat)

BY-26 28.01.2003

Stéganographie

PFPD EDSB

- La stéganographie ou "écriture recouverte" vise à dissimuler des informations, chiffrées ou non, dans une enveloppe ou conteneur d'apparence anodine. On appelle stéganogramme l'enveloppe de couverture incluant des données cachées extractibles par tout destinataire connaissant la méthode de dissimulation.
- Exemples: acrostiche (linguistique), encre sympathique ou microtrou (technique), stéganogiciel (numérique) => tatouage/filigranage (droits d'auteur!)
- Softwares: H4PGP, S-Tools4, HIP, Blindside, HideSeek, Contrab.And, InPlainView, Camouflage, MP3Stego…

BY-27 28.01.2003

Anonymisation de données

PFPD EDSB

- Définition:

  Modification de données personnelles de telle sorte que les informations relatives à la situation personnelle ou matérielle ne puissent plus (ou ? seulement au prix d'un effort disproportionné en temps, coût ou personnel) être mises en corrélation avec une personne physique déterminée ou déterminable.

- Toutes les données d'identification personnelle (directes ou indirectes) doivent être éliminées!

BY-28 28.01.2003

PFPD

Anonymat non traçable

EDSB

- La personne concernée fait partie d'un « grand » ensemble de données, au sein duquel elle ne peut pas être identifiée et plusieurs traces de sa part ne sont pas « corrélables/reliables ».
- La taille de l'ensemble de données est déterminante et peut de plus évoluer au cours du temps! La date de naissance peut ainsi devoir être remplacée par l'année de naissance ou l'âge.
- Exemples: paiement comptant, sondage stat.

PFPD

Anonymat traçable

EDSB

- La personne concernée reste parfaitement anonyme, bien qu'il soit possible de corréler plusieurs « actions » ou traces de sa part.
- Exemples:
  - cartes téléphoniques prépayées (Teleline, EASY)
  - code de liaison anonyme de l'OFS (stat. méd.)
- L'anonymat traçable est parfois désigné comme un « pseudonymat anonyme » ?!

Pseudonymisation de données

PFPD EDSB

- Définition:

  Modification de données personnelles par une règle de correspondance de telle sorte qu'il ne soit plus possible de mettre les informations relatives à la situation personnelle ou matérielle en corrélation avec une personne physique, sans avoir connaissance de cette règle ou sans y avoir recours.

- Les données d'identification sont par ex. converties en une désignation arbitraire (le pseudonyme!) au moyen d'une règle de correspondance.

BY-31 28.01.2003

Dépseudonymisation

PFPD EDSB

- Alors qu'une désanonymisation est théoriquement impossible, une dépseudonymisation / réidentification peut uniquement être accomplie si le pseudonyme de la personne concernée et la règle de correspondance sont connus.

- Des données pseudonymisées sont en fait anonymes pour toutes les personnes qui n'ont pas connaissance de la règle!

BY-32 28.01.2003

Pseudonymes à sens unique

PFPD EDSB

- La personne concernée est enregistrée sous une désignation dérivée de ses données d'identification par une fonction mathématique univoque.
- Une dépseudonymisation peut uniquement être accomplie à l'aide de la règle de correspondance, si l'identité de la personne concernée est connue ou si cette dernière fait partie d'un répertoire ou dictionnaire d'identités connues!

Pseudonymes de référence

PFPD EDSB

- Le lien avec la personne concernée peut être établi à l'aide d'une table de correspondance/référence, auquel l'accès est plus ou moins restreint…
- Protection efficace de la table de correspondance:
  - gérée exclusivement par des personnes authentifiées et accréditées
  - conservée uniquement sous une forme inviolable (par ex. sous forme chiffrée!)
  - réidentification d'un seul pseudonyme à la fois, avec journalisation/justification exhaustive des opérations

Pseudonymes de référence…

PFPD EDSB

- Table de correspondance privée/personnelle:
  Le pseudonyme est choisi librement (en évitant la collision avec des valeurs existantes) par la personne concernée. Ces pseudonymes sont communément baptisés noms de plume, de guerre, de scène, etc.
  Ex: San Antonio pour Frédéric Dard,
  Jean-Philippe Smet, alias Johnny Halliday!

- La communication de la correspondance affaiblit l'anonymat, alors que la réutilisation du pseudonyme augmente sa traçabilité. De ce fait, ce type de pseudonymes peut couvrir toutes les formes entre anonymat non traçable et pseudonymat public…

Pseudonymes de référence…

PFPD EDSB

- Table de correspondance semi-publique:
  La sécurité se base sur le maintien du secret de la correspondance entre pseudonyme et identité par tous les partenaires concernés.
  Ex: numéro (+ date exp.) de cartes de crédit

- Table de correspondance publique:
  Cette forme de pseudonymat correspond en fait à une identification indirecte des personnes.
  Ex: annuaire téléphonique (listes blanche/verte) permettant la recherche inversée!

Pseudonymat / Anonymat ?

PFPD EDSB

- Ne pas utiliser le même pseudonyme pour des buts différents, mais bien plutôt un pseudonyme différent pour chaque application distincte.
- Donner la préférence à l'anonymat, puis à un pseudonymat préservant au mieux la sphère privée de la personne concernée
  (PET: Privacy Enhancing Technologies…)
- Chiffrer les données personnelles sensibles qui ne sont ni anonymisées, ni pseudonymisées!

BY-37 28.01.2003

Internet/Email au travail

PFPD EDSB

- Nouvel outil de travail visant à une amélioration de la productivité, mais conduisant en pratique parfois à sa détérioration…
- La relation de confiance entre employeur et employés est en outre mise à mal (devoir de loyauté, sphère privée…) par l'introduction de ces nouvelles technologies!
- Première question fondamentale (à l'employeur): si la mise à disposition du courriel va aujourd'hui presque de soi, l'accès à Internet est-il utile et judicieux pour chaque employé?

BY-38 28.01.2003

PFPD

Intérêts de l'employeur

EDSB

- Préservation de la capacité de stockage de données
- Disponibilité et rapidité du réseau (bande passante)
- Sécurité des données et des applications (virus…)
- Maîtrise de l'information
- Productivité, Economicité
- Secrets d'entreprise
- Réputation, Image
- Confiance mutuelle avec les employés!
- Etc…

PFPD

Intérêts de l'employé

EDSB

- Être assuré du respect de sa sphère privée (LPD)
- Ne pas être victime de surveillance abusive (LT)
- Jouir de conditions de travail motivantes
- Bénéficier d'outils de travail efficaces pour atteindre ses objectifs
- Travailler dans une relation de confiance avec ses subordonnés, ses pairs et ses supérieurs.
- Etc…

PFPD

Solution proposée

EDSB

- Prévenir les abus par des mesures techniques et organisationnelles appropriées, plutôt que chercher à découvrir les auteurs d'abus déjà commis!
  (les délits pénaux devant bien sûr être poursuivis)
- Favoriser la transparence absolue des règles du jeu: communiquer les mesures (même intrusives) prises en expliquant pourquoi elles sont nécessaires, comment elles sont appliquées et à quoi les contrevenants s'exposent!

PFPD

Mesures techniques

EDSB

- Logiciel de base: options de sécurité, correctifs (SP)!
- Mots de passe personnels d'authentification:
  - complexité/longévité (PWD Mgr.) + économ. d'écran
- Droits d'accès (RWED) aux informations:
  - matrice de droits pour chaque groupe d'utilisateurs
  - chiffrement des documents sensibles!
- Limitation d'espace personnel de stockage (diskquota)
- Antivirus (mise à jour hebdomadaire, si pas journalière!)
- Firewalls personnels (gestion centralisée)
- Firewall-réseau contre les attaques et certains abus
- Système de détection d'intrusions (IDS)
- Sauvegardes régulières des données

Traces laissées par l'utilisateur

PFPD EDSB

- Historique des sites visités (N jours!)
- Fichiers temporaires (vidage automatique en quittant)
- Témoins (cookies) => Onglet « Confidentialité » (IE6)
- Saisie semi-automatique (adresses, formulaires, MDP)

- Courriels dans le dossier des éléments supprimés ou dans des dossiers d'archivage…

- Date et heure de connexion/déconnexion
- Documents imprimés (voire ouverts)
- Sites internes et externes consultés (URL)
- Données accessoires des courriels envoyés et reçus

Bases de la surveillance

PFPD EDSB

- Surveillance permanente du comportement au lieu de travail interdite par la loi sur le travail (Art. 26. Al. 1 O3LT; RS 822.113)
  => Spywares (espiogiciels) prohibés!
  => Détection: Lavasoft/Ad-aware ou SpyBot-S&D
- Surveillance globale et anonyme autorisée!
- Surveillance ponctuelle du travail accompli par les employés également autorisée à condition que:
  - but légitime et proportionnel
  - information préalable (ex: opérateurs télécom)
  - communication des sanctions en cas d'abus
  - délit pénal commis!

Surveillance du courriel

PFPD EDSB

- La réception de courriels privés à l'adresse prof. n'est pas entièrement maîtrisable par l'employé…
- Le critère de diffusion « Privé » indique par contre clairement la nature non professionnelle du courriel, qui ne doit alors pas être ouvert par l'employeur! (Loi sur les télécommunications; ATF 126|50 ext. 6a) => aussi valable pour le filtrage de contenu!
- Sans mention particulière et en l'absence d'indices concrets sur l'éventuelle nature privée d'un courriel, l'employeur peut supposer qu'il est professionnel.
- En cas de doute, l'employé devrait être consulté…

Courriels en cas d'absence

PFPD EDSB

- En cas d'absence planifiée d'un collaborateur, les mesures suivantes peuvent être prévues:
  - réponse automatique envoyée à chaque expéditeur (avec coordonnées de contact en cas d'urgence!)
  - règle de transfert automatique vers un remplaçant (exclusion des messages privés?; expéditeur averti?)
  - désignation d'un délégué avec autorisations de lecture et/ou écriture pour la boîte aux lettres (éléments privés en principe invisibles!)
- En cas d'absence imprévue, cela se complique:
  - administrateur introduit une réponse automatique ou bloque (longue durée) la boîte aux lettres…
  - existence d'un délégué permanent?

Courriels en cas d'absence…

PFPD EDSB

- En complément à l'adresse professionnelle nominative (jean.dupont@firme.ch), pourquoi ne pas recourir à une *adresse fonctionnelle impersonnelle*? (RespVente@firme.ch; Emp13@firme.ch; …)
- Un tel adressage offre les avantages suivants:
  1. Nature professionnelle apparente
  2. Délégué permanent défini (mesure organis. utile!)
  3. Peu sensible aux mutations internes
  4. Insensible aux renouvellements de personnel

BY-47 28.01.2003

Courriels en cas de départ

PFPD EDSB

- Donner la possibilité d'emporter ses courriels (comme les autres données) privés avant le départ!
- Transfert des messages professionnels (comme les autres dossiers) utiles/ouverts au remplaçant désigné ou au supérieur hiérarchique
- Blocage de la boîte aux lettres (comme les autres acomptes) au soir du dernier jour, ponctué par la destruction de tous les éléments contenus dans cette boîte (comme les autres conteneurs d'information).

BY-48 28.01.2003

PFPD

Questions ?

EDSB

Merci de votre attention,

Plein succès avec la
protection des données et surtout,

Bonne soirée à tous!