Protection et sécurité des données

avec les nouvelles technologies de l'information et de la communication…

GRIFES: Groupe Informatique et Sécurité

Ecole d'ingénieurs de Genève, le mardi 28.03.2006

PFPD

Votre serviteur…

EDSB

- Pierre-Yves.Baumann@edsb.admin.ch
- « Coordinateur informéthique » chez le PFPD
- Qualified BS 7799-2:2002 (ISO 27001:2005) Lead Auditor
- Ex prof. de math et informatique à la HES/St-Imier
- Ex resp. Informatique chez Cabloptic SA/Cortaillod
- Formation de mathématicien (Univ. Neuchâtel)

PFPD

Thèmes abordés

EDSB

1. Fondements de la protection des données
2. **Loi fédérale** sur la protection des données
3. Organisation et tâches du PFPD
4. Protection et sécurité des données
5. **Cryptographie** et stéganographie
6. **Anonymisation/pseudonymisation** de données
7. **Internet/Email** au lieu de travail (à domicile)
8. Nouvelles technologies (RFID, biométrie, …)
9. Questions

PFPD

1. Fondements

EDSB

- « Individual's right to be left alone » du juge de la Cour Suprême *Lous Brandeis* dans son article "*The* ***Right to Privacy***" (1890)

Le droit de l'individu à être laissé en paix !

- Dimensions de la „privacité“:
  - **Informationnelle** (autodétermination, sphère privée/publique, …)
  - **Communicationnelle** (poste, téléphone, SMS, courriel, etc.)
  - **Corporelle** (biométrie! + tests ADN/urine/sang/SIDA, etc.)
  - **Territoriale** (domicile, place de travail, lieux publics, etc.)

PFPD

Privacy is a complex issue!

EDSB

- Privacy has legal, regulatory, social, economic, political, technological, historical, moral and ethical dimensions.
- Privacy changes with context and is driven by perplexing questions:
  - Convenience? Profitability? Security? Trust? Liberty? Identity? Efficiency? Accountability? Monitoring? Democracy?

PFPD

Droits de l'Homme

EDSB

- **DUDH (1948) Art. 12:**
  Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.
- **CEDH (1950) 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…*

PFPD

Fondements européens

EDSB

- Convention N. 108 du CE (1981): Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
- Traité sur l'UE (1992, Maastricht, Titre I Art. 6 Al. 2)
  L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et tels...
- Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications
- Directive 99/93/CE sur un cadre communautaire pour les signatures électroniques (art. 8 Protection des données...)

PFPD

Fondements européens

EDSB

- Charte des droits fondamentaux de l'UE 2000/C 364/01:
  (Article 8: Protection des données à caractère personnel)

1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

PFPD

Fondements européens

EDSB

- Règlement (CE) 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données
- Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques
- Constitution pour l'Europe (29.10.2004/Rome => 01.11.2006?):
  Art. I-51 Protection des données à caractère personnel
  1. Toute personne a droit à la protection des données à caractère personnel la concernant.
  2. La loi ou loi-cadre européenne fixe les règles relatives à la protection des personnes physiques s'agissant du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.

Constitution Fédérale et Loi féd. sur la Prot. des Données

PFPD

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

2. 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 (2/4)

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 (3/4)

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

LPD: principes généraux (4/4)

PFPD

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
- Art. 8 Droit d'accès (demande au maître du fichier)
- Art. 11 Registre des fichiers (tenu par le PFPD)

PFPD

LPD: sécurité des données

EDSB

- Article 7 *Sécurité des données*

1. Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées…
2. Le Conseil fédéral édicte des dispositions plus détaillées sur les exigences minimales en matière de sécurité des données.

PFPD

LPD: révision en cours…

EDSB

- Art. 11 (nouveau) **Procédure de certification**

1. Afin d'améliorer la protection et la sécurité des données, les fournisseurs de systèmes de traitement de données et de logiciels ainsi que les personnes privées ou les organes fédéraux qui traitent des données personnelles peuvent soumettre leurs systèmes, leurs procédures et leur organisation à une évaluation effectuée par des organismes de certification agréés et indépendants.
2. Le Conseil fédéral édicte des prescriptions sur la reconnaissance des procédures de certification et sur l'introduction d'un label de qualité de protection des données. Il tient compte du droit international et des normes techniques reconnues au niveau international.

PFPD

Loi féd. sur la Transparence (de l'administration)

EDSB

- Forme évoluée de la **politique d'information**…
- **Meilleurs rapports** entre l´État et ses administrés
- Instrument pour renforcer les **droits démocratiques**
- Accès à des sources d'**informations précieuses**
- Renforcer **l'efficacité** de l'admin. et de ses mesures
- Renforcer le secret quand il est jugé nécessaire…

Mais:

- Fragilisation de la sécurité intérieure et extérieure ?
- Surcharge de travail, coûts supplémentaires ?

PFPD

LTrans et LPD

EDSB

- Art. 9 Protection des données personnelles:

1. Les documents officiels contenant des données personnelles doivent être rendus si possible anonymes, avant qu'ils soient consultés.
2. Lorsque la demande d'accès porte sur des documents officiels qui ne peuvent pas être rendus anonymes, l'art. 19 de la LPD s'applique. La procédure d'accès est régie par la présente loi.

- Art. 13 Médiation:

1. Toute personne peut déposer une demande en médiation:
   a. lorsque sa demande… est limitée, différée ou refusée
   b. lorsque l'autorité n'a pas pris position … dans les délais (20 jours) ou
   c. lorsque l'autorité, après l'avoir entendue, entend accorder l'accès aux documents malgré son opposition.
2. La demande en médiation est déposée auprès du PFPDT dans un délai de 20 jours à compter de la date de réception de la prise de position de l'autorité ou à l'échéance des délais fixés à l'autorité pour prendre position
3. Lorsque la médiation aboutit, l'affaire est classée.

3. Organisation du PFPD

PFPD

EDSB

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

- 1 unité « **conseil et information** »
- 1 unité « **surveillance** » (contrôles et analyses)
- 1 centre de compétence « Privacy Enh. Technologies »
- 1 secrétariat permanent à Berne

Rattachement administratif à la Chancellerie fédérale!

PFPD

Tâches du PFPD (2/2)

EDSB

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

Dans les secteurs public et privé!

PFPD

Projets PET

EDSB

- Privacy risks of pervasive computing (**RFID**)
- Personnel log data policy (client/server/net)
- Web-bugs & Cookies
- EDSB-Office (encryption, PKI)
- **SMS encryption**

- "**Voice over IP**": yes, but privacy-friendly! (Skype...)
- Privacy risks/leaks of "Desktop search tools"…

Notre système EDSB-Office

PFPD

EDSB

- Système **haut. confidentiel** de gestion des affaires (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 dès 2003)

PFPD

4. Sécurité des données

EDSB

- La sécurité des données couvre traditionnellement les domaines suivants:

!

1.	**Confidentialité**	Confidentiality	Vertraulichkeit
2.	**Intégrité**	Integrity	Integrität
3.	**Disponibilité**	Availability	Verfügbarkeit
4.	(Traçabilité	Traceability	Nachvollziehbarkeit)

- 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

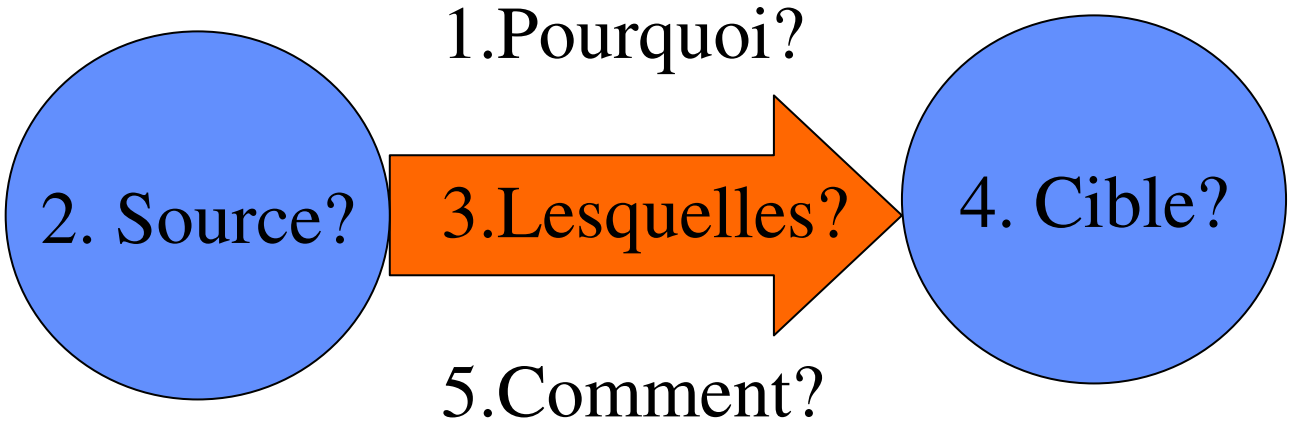
EDSB

- 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**

Cinq questions de protection (en cas de communication)

PFPD

EDSB

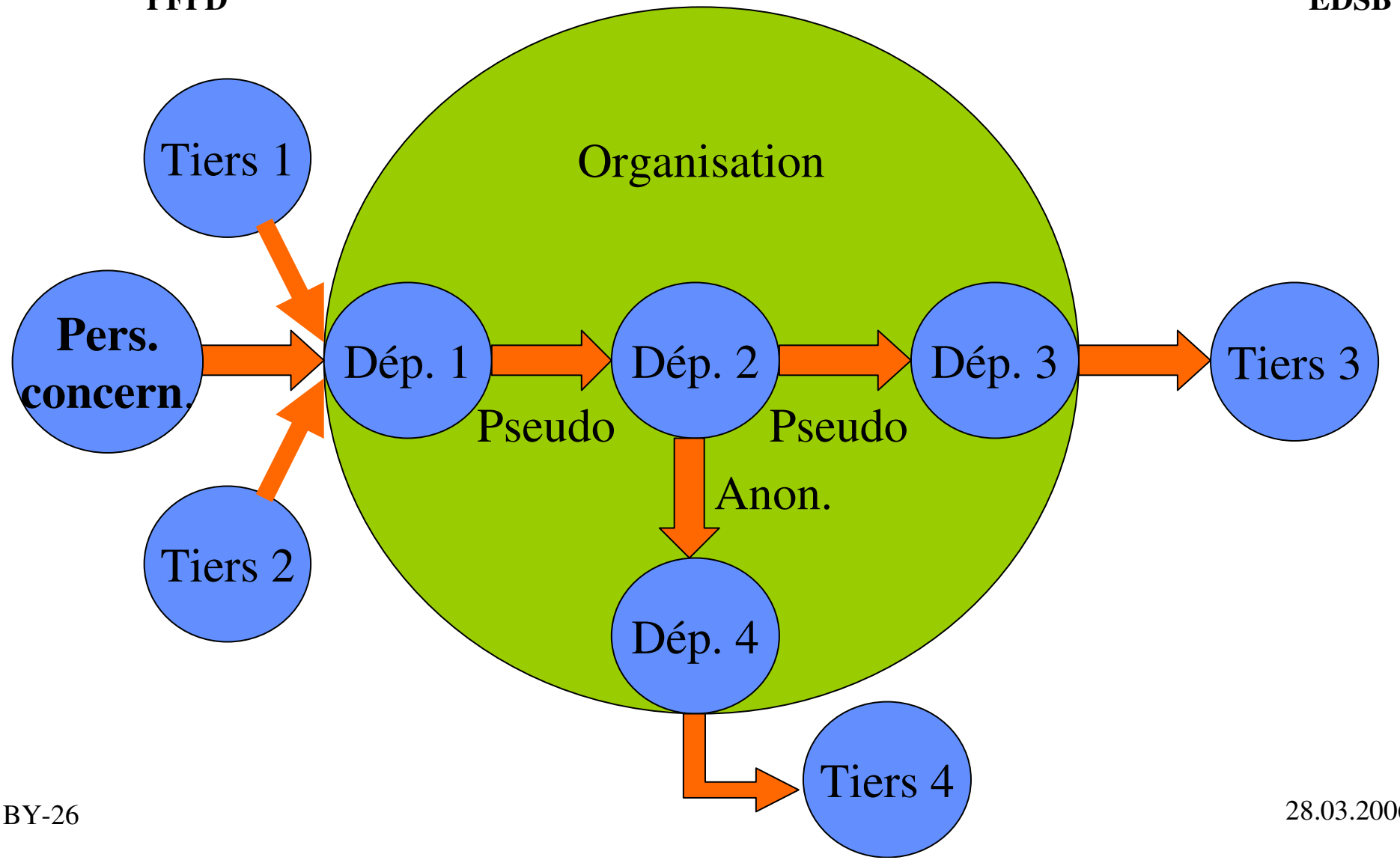


1. Licéité ? Finalité !
2. Authentification, Consentement ? Droit d'accès!
3. Proportionnalité ? Économie, Pseud-/Anonymisation !
4. Disponibilité, Confidentialité, Exactitude, Retransmission?
5. Inviolabilité, Intégrité ? Chiffrement !

Cascade de communications!

PFPD

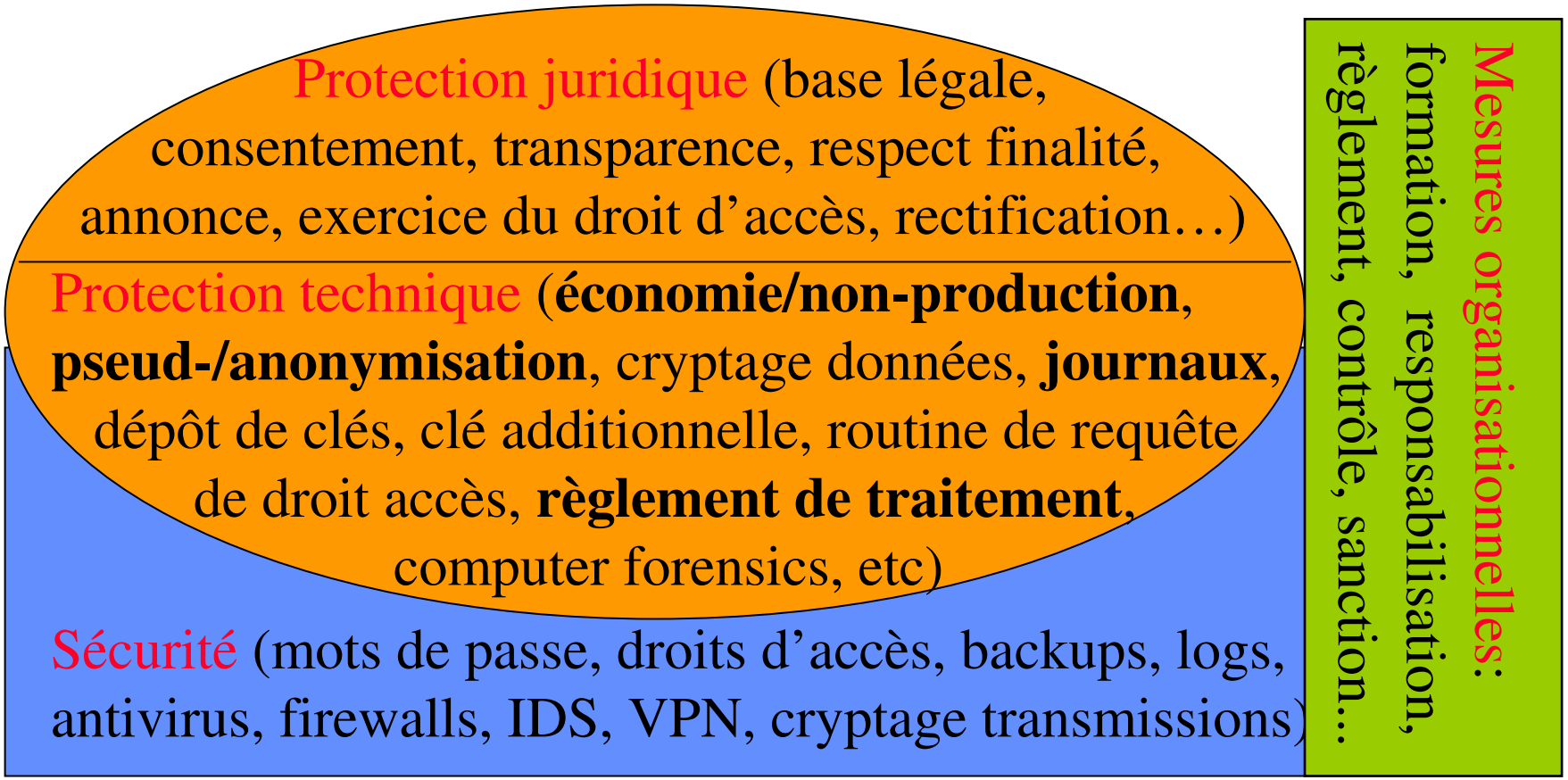
EDSB



Protection+Sécurité données

PFPD

EDSB



PFPD

Sécurité ‡ Protection !

EDSB

- Une haute protection des données n'est guère possible sans une sécurité élevée des données, tandis qu'une haute sécurité des données ne signifie pas forcément par une bonne protection 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…

5. Cryptographie: buts

- 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)

PFPD

Cryptographie symétrique

EDSB

- On utilise la même clé aussi bien pour le chiffrement/cachetage que pour le déchiffrement/décachetage!
- Si ces deux opérations ne sont pas accomplies par la même personne, il faut avoir/utiliser un canal sûr pour l'échange de la clé! => Question…

- Algorithmes connus: 3DES, CAST, IDEA, AES; HMAC
- Longueur de clé réputée sûre: 128/256 bits

- Exemple pratique: **ClipSecure** (Andrew Ferguson)

Cryptographie asymétrique

PFPD EDSB

- On recourt à une paire de clés formée d'une partie privée secrète et d'une partie publique (**PKI**), chaque partie pouvant être utilisée isolément pour accomplir une fonction cryptographique duale:
  Alice: $Enc(M,PK_B)=C$ ➔ $Dec(C,SK_B)=$**M** :Bob
  $Sig(M,SK_A)=\sigma$ ➔ $Ver(M,\sigma,PK_A)=$☺ **or** ☹
- La relation mathématique entre les deux parties de la paire de clés (SK/PK) est déterminante, et surtout SK ne doit pas être déductible de PK!

- Algorithmes connus: RSA, El-Gamal, DH, **ECC**; DSS
- Longueur de clé réputée sûre: 2048 bits **(~192 bits)**

Anneaux de clés asymétriques

PFPD EDSB

- Toutes les clés utiles sont conservées dans un anneau privé (SKR) et un anneau public (PKR).
- Chaque clé privée est mémorisée dans un format chiffré symétriquement, de manière à ce que son accès soit 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.

PFPD

Pretty Good Privacy

EDSB

- Développé et distribué par Phil Zimmerman dès 1991
- PRZ -> ViaCrypt -> PGP Inc. -> NAI -> PGP Corp. (2002)
- **Code source** publié (versions 2.x, 6.x, 8.x et 9.x)
- Version **freeware** téléchargeable (www.pgp.com) !
- 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/

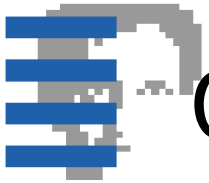
Alternative à PGP

- **GNU Privacy Guard** V1.4.x (www.gnupg.org)
- Standard OpenPGP (IETF)
- Outils additionnels: (cf. GNU Privacy Projekt – BMWA)
  - Windows Privacy Tray (www.winpt.org)
  - GNU Privacy Assistant (standard? graphical frontend)
  - 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)

Infrastructure à clés publiques

PFPD EDSB

- **Service** de mise à disposition en ligne de certificats (numériques) des clés publiques d'utilisateur
  [ou de clés publiques signées par un/des garant/s…]
- La certification de clés publiques appartenant à des personnes qui se rencontrent et/ou connaissent est pratiquement superflue (=> chiffrement symétrique;-)
- Problèmes plus subtiles dans les PKI:
  - révocation de clés (corrompues, volées, etc.)
  - dépôt central de clés (key escrow)
  - clé additionnelle de déchiffrement (ADK/CMRK)
  - certifications croisées (entre différentes autorités)



Crypto basée sur l'identité (IBE)

PFPD EDSB

- Idée proposée en 1984 par Shamir et implémentée efficacement seulement en 2001 par Boneh-Franklin
- But: éviter la contrainte d'obtenir un certificat avant…
- Astuce: - utiliser un élément de **l'identité comme PK** (adr. courriel, num. téléphone, etc.)
  - destinataire obtient sa SK de la part d'un KDC pouvant être sollicité même après réception!
- 4 modules: Setup (KDC), Keygen, Encrypt, Decrypt
- Exemples: **Voltage/SecureMail**, Secude/HaloCore…
- Remarque: Identity-based signature!, identification?

Stéganographie

- La stéganographie ou "écriture recouverte" vise à dissimuler des informations (chiffrées ou non!) dans un conteneur d'apparence banale et d'accès souvent public, afin d'assurer la **non-observabilité** de leur transmission. On appelle stéganogramme l'enveloppe de couverture incluant des données extractibles par tout lecteur 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…

6. 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!

Anonymat non traçable

PFPD

EDSB

- La personne concernée fait partie d'un « grand » ensemble de données, au sein duquel elle **ne peut pas être identifiée** et plusieurs actions ou 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 (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.

PFPD

Dépseudonymisation

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.

- **<u>Remarque décisive</u>:**
  Des données pseudonymisées sont anonymes pour toutes les personnes qui n'ont pas connaissance de la règle de correspondance !

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 (identité ⇔ pseudonyme), auquel l'accès doit être restreint…

- Protection efficace de la table de correspondance:
  1. gérée exclusivement par des personnes authentifiées et accréditées
  2. conservée uniquement sous une forme inviolable (par ex. sous forme chiffrée!)
  3. 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…

PFPD

Pseudonymes de référence…

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's…), au lieu de traiter «inutilement» les données d'une personne identifiée!
- Chiffrer les données sensibles d'une personne identifiée, de même que la table de correspondance! de données pseudonymisées (personne identifiable)
  Rem: données anonymisées « échappent » à la LPD!

7. 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?

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 (LTr)
- 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! <= **Privacy policies!**

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 journalière!) et **Antispyware**
- Firewalls personnels (gestion centralisée des règles)
- Firewall-réseau contre les attaques et certains abus
- Système de détection d'intrusions (IDS)
- Sauvegardes (et destructions) 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

PFPD

Bases de la surveillance

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!

PFPD

Surveillance du courriel

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) => valable pour les backups et 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

- 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 organisationnelle utile!)
  3. Peu sensible aux mutations internes (hormis promotions ;-)
  4. Insensible aux renouvellements de personnel

Courriels en cas de départ

PFPD

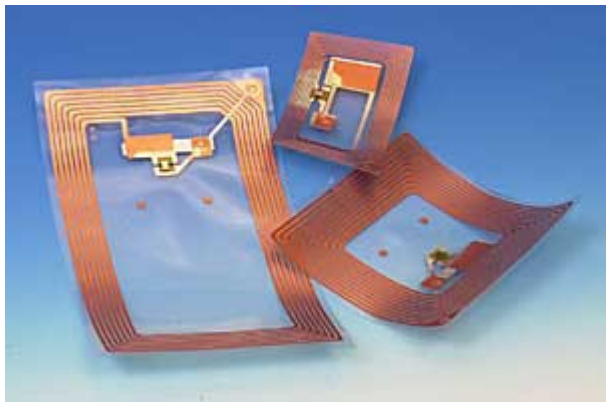
EDSB

- 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).

8.1 Radio-Freq. IDentification

PFPD EDSB

- « The risk RFID technology poses to humanity is on a par with nuclear weapons » *Kath. Albrecht (2003)*
- « Used improperly, RFID has the potential to **jeopardize consumer privacy**, reduce or eliminate purchasing anonymity, and **threaten civil liberties** »
- Threats to privacy and civil liberties:
  1. **Hidden** placement of **tags**.
  2. **Unique identifiers** for all objects worldwide.
  3. Massive **data aggregation**.
  4. **Hidden readers**.
  5. Individual **tracking and profiling**.



RFID: perspectives…

- Pourquoi diable… les humains font-ils partie de cette liste ?

BITS	UNIQUE NUMBER	OBJECTS
23	6.0×10^{6} per annum	Automobiles
29	5.6×10^{8} in use	Computers
33	6.0×10^{9} total	Humans
34	2.0×10^{10} per annum	Razor blades
54	1.3×10^{16} per annum	Grains of rice

PFPD

8.2 Biometrics: Definitions

EDSB

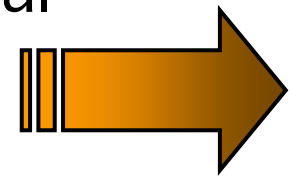
- Biometrics: automated methods of recognizing a person based on one (or many => multimodal…) of its ***behavioral* or *physiological* characteristics**
- Verification/Authentication: Matching a biometrical sample against a **single recorded reference (1-1)** "Is the person really who she claims to be ?"
- Identification: Matching a biometric sample against a list/database of identifiers (**1-N** comparison/search!)
- Templates: distinguishing characteristics **extracted from the raw** biometrics sample and converted into a processed **biometric identifier record**

Biometrics: Technologies

PFPD

EDSB

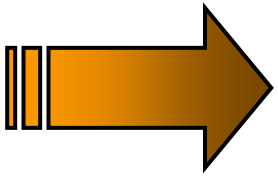
- Behavioral



Voice
Signature
Keystroke

Unique but variable

- Physiological



Finger
Hand
Eye
Face
Vein
DNA ?

Unique and permanent

Human authentication

- Types of human authentication
  - What you ***know*** (secret)
    - Password, PIN, mother's maiden name
  - What you ***have*** (token)
    - ATM card, smart card
  - What you ***are*** (biometric)
    - Stable: fingerprint, face, iris…
    - Alterable: voice, keystroke…

PFPD

Biometrics: Applications…

EDSB

- Season-cards for a public indoor **swimming pool** (CH)
- Access and payment in a **school canteen** (FR)
- Presence registration in an **elementary school** (UK)
- Personal authentication at **public concerts** (CH)
- Passenger verification at **airport** (CH)
- User verification for **cars, computers, premises**, etc.
- Biometrics in **E-Passports** and ID-Cards (worldwide)
- Etc…

Biometrics: Risks & Questions

PFPD EDSB

- **Human body as a data carrier !**
- **Uniqueness**, Universality, Permanence, Collectability
- **Traces** left unwillingly and unconsciously
- **Discrimination** of certain categories of individual (rejected or declined enrolment)
- **Reliability** (**FAR**/FRR), Traceability, Sensitivity
- **Linkage** of biometric databases

➢ How to minimise risks for privacy ?
➢ Expectations and benefits ?
➢ **Reasonable use ?**

Biometrics: Open questions

PFPD

EDSB

- Residual **sensibility of templates** ?
- **Linkability** of “independent” templates extracted from the same personal characteristic?
- **Standardisation** of extraction/comparison algorithms?
- Possible anonymisation of biometric data ?
- **Biometrics combined with RFID-technology** ?!
- **Centralisation** of templates ?
- Biometric data as the universal identifier ?
- …

PFPD

Biometrics: Conclusions…

EDSB

- DP-Evaluation: **Decision in the individual case**!
- Potential **impacts on privacy not fully assessed** from today's perspective
- Biometrics as a **mere "fun factor/fashion trend" ?**
- Whenever possible, do prefer **decentralised storage** (match-on-card)
- Plan alternative (non biometric) verification systems to **prevent discrimination**

PFPD

9. Questions ?

EDSB

Merci de votre participation,

Plein succès avec la
protection des données!

Et bonne soirée à tous!