Protection des Données Personnelles

COMMISSION NATIONALE
POUR LA PROTECTION
DES DONNÉES

Etablir une bonne gouvernance

au sein de l'entreprise

Enjeux et Avantages

Avantages d'une bonne gouvernance en la matière

- « It's all about TRUST »
- La confiance de la part des clients, utilisateurs et tiers impliqués
  des fournisseurs et partenaires,
  des salariés et collaborateurs,
  du régulateur et des pouvoirs publics,
  de l'opinion publique.
- Elle se gagne pas à pas, péniblement, se consolide et se mérite tous les jours, mais un seul jour suffit , une seule faille de sécurité, une indélicatesse, un abus, pour la perdre: ex. Playstation Network, Google Wifi
- « Accountability = organised compliance, transparency and fairness, lawfulness and security in data processing »
- Cette naturellement les acteurs de certains secteurs d'activité que le souci d'une image de marque fondée sur la confiance a d'abord conduit à investir dans la protection des données: e-commercce, IT et services sur Internet, Santé, Finance
- …

Identification des traitements de données personnelles effectués dans l'entreprise

- Faire l'inventaire des processus et des fichiers utilisés au sein de l'entreprise et comprenant des données à caractère personnel
- Identifier et déterminer précisément les finalités des traitements (art. 4)
- Vérifier la légitimité (identifier le critère légal « porte d'ouverture ») (art. 5)
- La nécessité: les données collectées doivent être indispensables pour les finalités définies (« Datensparsamkeit ») (article 4)
- Principe de proportionnalité (article 4):
  - catégories de données (ne doivent pas être excessives),
  - opérations de traitement,
  - destinataires,
  - durée de conservation

Les formalités de déclaration préalable des traitements

- Formalités à accomplir dépendent de la finalité et des catégories de données traitées

  cf. http://www.cnpd.public.lu/fr/declarer/index.html

- Exemptions (article 13 § 3)
  - Traitements « anodins » les plus courants (p.ex. calcul des salaires, gestion des contacts)
- Notification préalable (articles 12 et 13) Formulaire standard
  - Constitue la règle pour les traitements non exemptés
  - Applicable même aux données de santé (sauf données génétiques, ou utilisation secondaire)
  - Surveillance de personnes tierces sans enregistrement
- Notification unique (article 12 § 1 lettre (b))
  - Procédure simplifiée pour traitements standardisés (p.ex. élections sociales)
  - Délibération de la CNPD décrivant le traitement (conditions et restrictions)
  - Formulaire spécifique : engagement formel de conformité
  - N.B. Il existe une formalité similaire d'autorisation simplifiée: p.ex contrôle d'accès et des horaires de travail par badges)
- Autorisation préalable (article 14)
  - Traitements à caractère plus « intrusif » (p.ex. surveillance, données génétiques, biométrie, utilisation secondaire pour recherche scientifique)
  - Demande sous forme de lettre libre (sauf pour la vidéosurveillance → formulaire spécifique)

La mise en pratique de principe de l'«accountability»: (organiser sa responsabilité)

- Article 4 de la loi énonce que le responsable doit s'assurer que les données qu'il traite le sont loyalement et licitement et respectent notamment les:
  - a) principe de finalité;
  - b) principe de proportionnalité et de nécessité
  - c) principe d'exactitude, mise à jour;
  - d) durée limité de conservation, sinon anonymisation
- Mettre en place des structures et procédures efficaces pour assurer la conformité avec la protection des données et la prise en charge des problèmes
  - Elaboration d'une politique de protection des données écrite (charte) et contraignante (p.ex. pour la création de nouveaux fichiers)
  - Mappage/supervision des procédures
  - Mise en place d'un système de gestion des plaintes de personnes concernées
- Guidance pour les collaborateurs
  - Diffusion de guides d'utilisation / codes de bonnes pratiques
  - Organisation de formations
  - Transparences quant aux procédures internes / gestion des plaintes
  - Publication de rapports annuels d'incidents et améliorations

Identification des enjeux en fonction de l'activité de l'entreprise

- Vérifier les mesures de sécurité requises en fonction du risque d'atteinte à la vie privée (« sensibilité » des données), de l'état de l'art et des coûts liés à leur mise en œuvre (article 23)
  - Mesures au niveau technique et de l'organisation mise en place
  - Gestion scrupuleuse et « granulaire » des droits accès aux systèmes (restriction au minimum nécessaire selon les fonctions et compétences des employés)
- Traitement des données (pour compte du responsable) par un sous-traitant
  - Choix d'un sous-traitant apportant des garanties suffisantes
  - Obligation de conclure un contrat avec le sous-traitant précisant que
    - le sous traitant ne peut agir que sur la seule instruction du responsable du traitement
    - les obligations relative à la sécurité des traitements incombent également à ce dernier
- Garantir le respect des droits des personnes concernées (phase I)
  - Information de la personne concernée (articles 26 et 27)
    - Identité du responsable du traitement
    - Finalité(s) déterminées du traitement
    - Destinataire(s) au(x)quel(s) sont communiqués les données
    - Autres informations contribuant à la transparence vis-à-vis de la personne concernée

Politique d'information des personnes concernées

- Assurer une transparence loyale envers les personnes concernées
- Fournir des informations aux personnes concernées par des moyens appropriés
  - En facilitant l'accès aux renseignements:
    - Notice d'information dans un formulaire de collecte de données
    - intranet (employés)
    - internet (clients, fournisseurs,…)
  - Présentation des informations au moment propice par rapport à la collecte de données
  - Utilisation d'un langage et une présentation faciles à comprendre
  - Information de la personne en fonction de la « sensibilité » des données
- Multiplier les niveaux et supports d'information pour la personne concernée / format multistrates (concept de la « multi-layered information »)
  - Avis succinct (« short notice »)
  - Avis condensé (« condensed notice »)
  - Information compléte (« full notice ») p.ex. notice concernant la vie privée (« privacy notice ») décrivant les conditions juridiques et modalités pratiques exactes à l'intention des personnes souhaitant s'informer plus exhaustivement

Une équipe dédiée en matière de protection des données

Création d'une instance spéciale « privacy officer » ou « privacy team » au sein de l'entreprise: (p.ex le compliance officer, un juriste/informaticien spécialisé

- Consultation de cette personne/équipe lors de la mise en place d'une nouvelle procédure ou de la création d'un nouveau fichier
- Lui demander le cas échéant une évaluation de l'impact sur la vie privée droits des personnes concernées (« privacy impact assessment ») en fonction de la « sensibilité », des données traitées, de la divulgation qu'elle engendre potentiellement et de l'ampleur du cercle des personnes accédant aux données
- Lui confier un rôle de contrôle interne, d'alerte et de conseil en la matière
- D'organiser périodiquement un audit externe débouchant sur un plan d'action

L'instance : le chargé de la protection des données (I)

- Fonction facultative prévue à l'article 40 de la loi
  - Règlement grand-ducal d'exécution du 27 novembre 2004
  - Responsable du traitement exempté du devoir de notification
  - Niveau de formation universitaire requis (droit, économie, … ou profession réglementée)

- Procédure à suivre
  - Demande d'agrément préalable à présenter à la CNPD
  - Décision d'inscription sur la liste des chargés par la CNPD
  - Désignation du chargé de la protection des données par l'entreprise
  - Vérification de son indépendance par la CNPD (éviter conflits d'intérêts, p.ex. RSSI)

- Statut du chargé au sein de l'entreprise
  - « Correspondant » de la CNPD » en parallèle à sa fonction habituelle dans l'entreprise
  - Jouit d'une certaine indépendance vis-à-vis du responsable du traitement qui le désigne
  - Doit disposer d'un temps approprié pour s'acquitter de ses missions
  - Révocabilité

Le chargé de la protection des données (II)

- Missions pouvoirs et obligations du chargé de la protection des données définies à l'article 40 de la loi et dans le RGD du 27 novembre 2004

  –Etablir et tenir à jour un registre des traitements de données à caractère personnel mis en œuvre au sein de l'entreprise / communication à la CNPD tous les 4 mois

  –Contrôle de l'application des dispositions légales réglementaires applicables aux traitements opérés par l'entreprise

  –Pouvoir d'investigation auprès le responsable du traitement / droit à l'information

  –Fonction de médiateur: traitement des plaintes des personnes concernées

  –Conseiller avec rôle d'alerte et de recommandation: Information du responsable du traitement sur les formalités à accomplir afin de se conformer aux dispositions légales en la matière

  –Interface entre la CNPD et le responsable du traitement: consultation de la CNPD en cas de doute quant à la conformité d'un traitement avec la loi

  –Suivre une formation continue régulière (perfection et mise à jour des connaissances)

Flux internationaux de données : Art. 18 et 19

- Niveau de protection adéquat
  - « Sphère de sécurité »: directive 95/46/CE du 24 octobre 1995 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 transposée en droit national dans les 27 pays de l'Union européenne
  - Pays de l'Espace Economique Européen (EEE) : *Islande, Liechtenstein, Norvège)*
  - Pays (tiers) dont le niveau de protection adéquat a été reconnu par la Commission européenne: Suisse, Argentine, Canada, îles de la Manche, Etats-Unis d'Amérique (sociétés « safe harbor »)
- Autres pays:
  - Interdiction de transfert vers des pays tiers n'offrant pas un niveau de protection adéquat

Transferts de données à caractère personnel vers des pays tiers n'offrant pas un niveau de protection adéquat

- Dérogations prévues à l'article 19 § 1 de la loi du 2 août 2002
  - consentement de la personne concernée
  - contrat conclu avec ou dans l'intérêt de la personne concernée
  - intérêt public important
  - …

- Autorisation par la CNPD sur base de l'article 19 § 3 de la loi
  - demande dûment motivée
  - garanties suffisantes au regard de la protection de la vie privée, des libertés et droits fondamentaux des personnes concernées ainsi qu'à l'exercice des droits correspondants (information, accès, rectification, opposition)

Garanties appropriées

- Clauses contractuelles appropriées, telles que les clauses contractuelles types élaborées par la Commission européenne (téléchargeables à partir du site Internet http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm)

  - Identifier le rôle du destinataire (importateur) des données selon les finalités du transfert
    - Responsable du traitement réalisant ses propres finalités
    - Sous-traitant n'agissant que sur instruction du responsable du traitement

  - Modèle de contrat à conclure entre l'exportateur et l'importateur des données:
    - décision 2001/497/CE du 15 juin 2001 (vers un responsable du traitement) ou
    - décision 2004/915/CE du 27 décembre 2004 (vers responsable,set alternatif) ou
    - Décision 2010/87/EU du 5 février 2010 (vers un sous-traitant) → sous-traitance « en cascade » désormais possible, ce qui n'était pas le cas pour les clauses du 27 décembre 2001 (décision 2002/16/CE abrogée)

      (N.B.: ne pas confondre avec le contrat de sous-traitance prévu à l'article 22 de la loi !)

  - Autres mode d'établissement de garanties appropriées
    - règles contraignantes d'entreprises / « binding corporate rules » (BCRs)
    - …

Garanties appropriées (II): Binding corporate rules

- Caractéristiques et avantages
  - Charte reprenant les principes de la protection des données contraignante et applicable à toutes les filiales d'un groupe international d'entreprises
  - Solution intéressante à des groupes d'entreprises disposant de filiales dans le monde entier et confrontés à des flux de données réguliers
  - Système plus flexible et plus adapté à la culture d'entreprise que les clauses contractuelles types
  - Evite de devoir recourir à d'innombrables contrats à passer pour chaque type de flux de données
  - Procédure d'approbation définie: coopération des autorités nationales de la protection des données européennes concernées

- Site internet du Groupe Article 29 dédié aux règles contraignantes d'entreprises http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm

- Documents de travail (« working papers ») élaborés par le Groupe Article 29 (WP 74, WP107, WP108, WP153, WP154, WP155) disponibles sous http://ec.europa.eu/justice/policies/privacy/binding_rules/tools_en.htm

Structure des règles contraignantes d'entreprise WP154)

- Champ d'application; --Définitions
- Limitation des finalités
- Qualité des données et proportionnalité
- Condition(s) de légitimité
- Traitements de données « sensibles »
- Transparence et droit à l'information
- Droits d'accès, de rectification, d'effacement et de verrouillage des données
- Décisions individuelles automatisées
- Sécurité et confidentialité
- Relations avec les sous-traitants
- Restrictions relatives aux transferts ultérieurs (« onward transfers) »
- Programme de formation
- Programme d'audit
- Respect des règles et contrôle de leur application
- Relation entre les différentes législations et les BCRs
- Système interne de la gestion des plaintes (« complaint handling process »)
- Droits de tiers bénéficiaires (« third party beneficiary rights »)
- Responsabilité (« liability »)
- Entraide et coopération avec les autorités de protection des données
- Mise à jour des BCRs

Questions & réponses

Vos questions ?

Commission Nationale pour la Protection des Données

MM. Gérard LOMMEL (président)
Thierry LALLEMANG & Pierre WEIMERSKIRCH (membres effectifs)

Mme Josiane Pauly et
MM. Marc Hemmerling et Tom Wirion
(membres suppléants)

Adresse postale: L-4100 Esch-sur-Alzette
Bureaux : 41, avenue de la Gare
L-1611 Luxembourg
Tél.: 26 10 60 - 1
Fax.: 26 10 60 - 29
E-Mail: info@cnpd.lu
www.cnpd.lu