Le nouveau règlement sur la protection des données personnelles : Quel impact pour la sécurité ?

Jean-Marc Suchier
Samuel Vinson

23 janvier 2013

SAFRAN
Morpho

AGENDA

- **Principales nouveautés du Règlement et de la Directive**

- **Retour d'expérience d'une approche « Privacy-by-Design »**
  - Autorisation pluriannuelle pour la constitution de bases de données biométriques
  - Finger VP

SAFRAN Morpho

/01/

Principales nouveautés du Règlement et de la Directive

Jean-Marc Suchier

SAFRAN Morpho

HISTORIQUE

➔ Régime actuel : la Directive 95/46

- Protection des données personnelles (DP)
- Garantie libre circulation des DP au sein de l'Union Européenne (UE)

➔ Problèmes

- Manque d'harmonisation au niveau européen (transpositions)
- Bouleversements technologiques depuis 1995
  - Internet
  - Réseaux sociaux
  - Explosion des transferts de données
- Traité de Lisbonne
  - La protection des données personnelles est un droit
  - Cette protection doit être homogène au sein de l'UE

➔ le Conseil mandate la Commission Européenne de revoir la Directive 95/46

LES NOUVEAUX TEXTES

➔ 1/2012 Publication d'une proposition (DG Justice)

- Un Règlement pour le cas général
- Une Directive pour
  - Les investigations / enquêtes criminelles
  - L'application des décisions de justice

➔ Ces textes ne concernent pas

- Les institutions européennes
- La sécurité nationale

➔ Principale cible: les applications sur internet

- ➔ mais les textes **s'appliquent à tous les secteurs industriels**

➔ Remarques

- le Règlement s'applique au traitement des données des employés
  - Non couvert dans la présentation

ETAT D'AVANCEMENT

➔ 1/2013 Rapports du PE (Commission LIBE) sur les 2 textes

- Renforcement de la protection des individus
- Renforcement des pouvoirs des autorités de contrôle (AC), les « CNILs »
- Demande à la CE de préparer des textes similaires couvrant les activités des institutions européennes

➔ Vote du PE attendu en 4/2013

➔ Approbation finale du texte

- Normalement courant 2013

SAFRAN Morpho

QUELQUES DÉFINITIONS

➔ Personne concernée

- Une personne physique **identifiée** ou une personne physique **qui peut être identifiée**, directement ou indirectement, par des **moyens raisonnablement susceptibles d'être utilisés** par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un **numéro d'identification**, à des données de **localisation**, à un **identifiant en ligne** ou à un ou plusieurs éléments spécifiques, propres à son **identité physique**, **physiologique**, **génétique**, **psychique, économique, culturelle** ou **sociale**;

➔ Données à caractère personnel

- Toute information se rapportant à une personne concernée

QUI EST CONCERNÉ PAR LE RÈGLEMENT? 1/2

➔ Le responsable du traitement (RT)

- « Celui qui détermine les finalités, les conditions et les moyens du traitement des données à caractère personnel »

➔ Le sous-traitant

- « Celui qui traite les données à caractère personnel pour le compte du responsable du traitement »

➔ Quid du développeur d'application?

- A priori, pas concerné directement (maintenance ?)
- Opinion juridique: le RT et les personnes peuvent se retourner contre le développeur
- Rapport PE: introduit formellement a notion d'« éditeur »
  - Responsable du respect des grands principes de protection des données personnelles
  - Doit respecter les règles de « Privacy-by-Design (PbD) » et « Privacy-by-Default (PbDf) »

QUI EST CONCERNÉ PAR LE RÈGLEMENT? 2/2

➔ Quid des PME ?

- Elles sont soumises au Règlement
- Texte prévoit quelques allègements spécifiques
  - Délégué à la protection des données
  - Documentation
  - …
- Rapport PE supprime ces allègements
  - Ce qui importe c'est l'activité principale du RT
  - Règle du traitement des données personnelles de plus de 500 personnes par an

➔ Quid des laboratoires de recherche ?

- Ils sont également soumis au Règlement
  - Protection des données personnelles
  - Constitution des fichiers
  - Règle des 500 personnes par an ?
  - Cas de collaboration avec industrie en vue de développement produits ?
    - Respect de l'ensemble des règles de protection
    - Respect des règles de PbD

LES PÉNALITÉS, LES PLAINTES

➔ Principe

- Tout non respect d'une clause du Règlement peut donner lieu à des sanctions déterminées par les autorités de contrôle
  - « *Dans chaque cas, la sanction administrative doit être* ***effective****,* ***proportionnée*** *et* ***dissuasive*** ».
- Sanctions graduées et progressives pouvant aller, pour les entreprises, jusqu'à 2% du chiffre d'affaire mondial……

➔ Les plaintes

- Plaintes auprès des autorités de contrôle
  - Toute personne concernée
  - Toute association ou organisation qui vise à protéger les droits des individus
- Plaintes en justice
  - Toute personne concernée
  - Toute association ou organisation qui vise à protéger les droits des individus
  - Les autorités de contrôle

LES PRINCIPALES RÈGLES À SUIVRE

➔ Principe: le traitement des données personnelles est interdit, sauf

- Consentement explicite de la personne concernée
- Quelques exceptions spécifiques (obligation légale, intérêts vitaux de la personne,..)
- Recherche historique, statistique, scientifique (avec certaines restrictions)

➔ Règles

- Transparence
- Protection spécifique de donnée sensibles (croyances, opinions, origine, génétiques,..) ou des enfants (moins de 18 ans)
- Droit de rectification, droit à l'oubli
- Profilage interdit, sauf loi spécifique
- Notification, en cas de violation des données, sous 24H

➔ Analyse d'impact relative à la protection des données personnelles

- Obligatoire lorsque « les traitements présentent des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités »

LES AUTORITÉS DE CONTRÔLE

➔ Renforcement de leurs responsabilités et de leur pouvoir

- Elles vérifient que le règlement est appliqué correctement
  - Droit d'investigation, d'audit, de sanctions
  - Reçoivent et traitent les complaintes
  - Coordination avec les autres AC
  - Participation au Comité Européen de la Protection des Données (CEPD)

➔ Le CEPD (Remplace le Groupe de l'Article 29)

- Participants
  - Responsables de chaque autorité de contrôle
  - Le superviseur des données européen
- Rôle
  - Vérifie l'harmonisation de l'application du Règlement au sein de l'UE

➔ Le PE suggère d'augmenter les prérogatives des ACs et du CEPD

QUEL IMPACT POUR LES ENTREPRISES?

➔ Mettre en place un délégué à la protection des données

- Rattaché au management (peut être un sous-traitant)
- Responsable de l'application du règlement
- Rôle fondamental pour organiser formation et mise en place de procédures
- Point de contact avec les autorités de contrôle

➔ Mettre en place l'organisation et les procédures nécessaires

- Documentation
- Formation du personnel chargé de la R&D
- Audit interne

➔ Impact juridique

- Assurances
- Ajustement des clauses dans les contrats commerciaux

MISE EN ŒUVRE DU PbD ET DU PbDf

➔ Concepts simples

- Des grands principes définis dans les années 1990s (Ann Cavoukian)

➔ Mais aucune description claire de ce qui est à faire

- Quelques grandes entreprises ont défini leur approche « maison »
- La CE souhaite que les associations d'industriels définissent des « codes de conduite »

➔ Communication sur la politique de sécurité industrielles (07/2012)

- Action 8: mandater les organismes de certification pour préparer un standard pour les mise en œuvre du « Privacy-by-Design »

/02/

Retour d’expérience d’une approche « privacy by design »

Samuel Vinson

AUTORISATION PLURI-ANNUELLE (1/2)

➔ Objectifs de Morpho : Mise en place d'une procédure pour la constitution de bases de données biométrique à des fins de recherche scientifique

- Des garanties en termes de protection des données biométriques pour la société, ses employés et pour les volontaires
- Des garanties en termes de protection des données biométriques pour les projets de recherche collaboratifs

➔ Dans le cadre d'une approche résolument « Privacy by Design », collaboration avec l'autorité de protection des données

- Début collaboration : Mars 2009
- Réunions régulières de travail, de nombreux échanges par email et téléphone
- Fourniture de documents au service de l'expertise de la CNIL

➔ Réalisation Morpho

- Analyse de risque EBIOS version 2 (début 2010)
- Définition et mise en place d'une organisation interne de gouvernance
- Définition et mise en place de l'environnement et des processus de gestion des bases

AUTORISATION PLURI-ANNUELLE (2/2)

➔ Résultats

- Obtention de l'autorisation pluri-annuelle en Juillet 2010
- Certification ISO 27001 du processus de gestion des bases de données (Mai 2011)

➔ Remarques économiques

- 18 mois de définition d'un cadre conforme ISO 27001
  - 12 mois de travail avec la CNIL
- Processus sécurisant mais contraignant pour les utilisateurs et les responsables de campagnes d'acquisition
- Difficilement transposable à tous nos produits et à toute l'industrie

CAPTEUR FINGER VP (1/2)

- **Objectifs de Morpho : concevoir un produit innovant, haut de gamme, présentant :**
  - Les meilleures performances biométriques du marché
  - Des garanties représentant l'état de l'art en termes de protection des données biométriques
  - Des garanties représentant l'état de l'art en termes de protection contre l'usurpation d'identité

- **Dans le cadre d'une approche résolument « Privacy by Design », collaboration avec l'autorité de protection des données**
  - Début collaboration : Janvier 2010
  - 6 réunions de travail, de nombreux échanges par email et téléphone
  - Fourniture de 6 documents au service de l'expertise de la CNIL, dont certains ont nécessité l'autorisation de nos donneurs d'ordre
  - Prêt de matériel

CAPTEUR FINGER VP (2/2)

➔ Résultat un capteur conforme au respect de la privacy

- Capteur biométrique reposant sur une technologie SANS TRACE
- Capteur biométrique dont les données biométriques ne peuvent être extraites
- Niveau de risque identique à celui d'un support individuel

➔ Remarques économiques

- Dés délais supplémentaires et un surcout
  - Dont une partie conséquente liée aux éléments de sécurité
- Un développement de 24 mois au lieu des 18 mois habituels
- Un surcout de 25 %

CONCLUSION ET PROJECTION

➔ Conclusion

- Deux exemples de développement Privacy-by-Design positifs
- Démarches non transposables à l'ensemble des produits et de l'industrie

➔ Projection

- Le nouveau règlement impose le Privacy-by-Design
- Nécessité de définir une démarche de PbD clair sans délai et surcout excessif

SAFRAN Morpho