Réglement Général sur la Protection des Données

Pierre-Yves Bonnetain
py.bonnetain@ba-consultants.fr

B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

17 octobre 2017

B&A Consultants

- Cabinet de conseil en sécurité informatique créé en 1996.
- Conseils, suivi et assistance en sécurité informatique.
- Audits de sécurité, de configurations, de code...
- Tests d'intrusion, tests d'applications.
- Réponse à incidents, analyses *post-mortem*.
- Analyses de risques, gestion des risques sur l'information.
- Ingéniérie de la sécurité informatique, recherche de solutions.
- Formations à la sécurité informatique.
- Expertise judiciaire (civile ou pénale) et expertises privées.
- Animateur de ReSIST, groupe de travail régional de l'OSSIR (`www.ossir.org/resist`)

Plan

Plan

Nous revenons de loin

Entre 2007 et 2011...

- Changements réguliers politique de vie privée de Facebook, fiasco dénoncé « the next Facebook privacy scandal »
- Eric Schmidt (PDG Google, 2009) : « Only miscreants worry about privacy » et « If you don't want it known, don't do it »
- 22 infractions majeures de Facebook à la législation irlandaise sur la protection des données personnelles (2011)
- Directive européenne et 28 pays $\rightarrow$ 28 lois avec variations

Conséquences

Nécessité de changement significatif de la législation en place pour apparition « véritables sanctions » et « une même règle pour tous »

Cibles principales

- Pas forcément les GAFA
  - bien meilleure gestion des risques juridiques
  - certaines déjà condamnées sous régime actuel (3 M€ max)
  - nette avance protection données personnelles
- plutôt les entreprises européennes
  - faible culture gestion risques juridiques
  - ne comprennent pas besoin protection données personnelles
  - peu de compétences en la matière

Principales évolutions

- réglement et non directive européenne
- homogénéisation probable (décisions, sanctions) niveau européen
- sanctions dissuasives (2 à 4% CA mondial, 10/20 M€ pour administrations)
- conservation majorité obligations antérieures
- suppression déclaration CNIL au profit responsabilisation et autocontrôle
- nouvelles obligations de sécurité
- étude d'impact obligatoire, avant mise en œuvre, pour certains traitements (données sensibles, profilage)
- renforcement droits personnes notamment sur preuve consentement

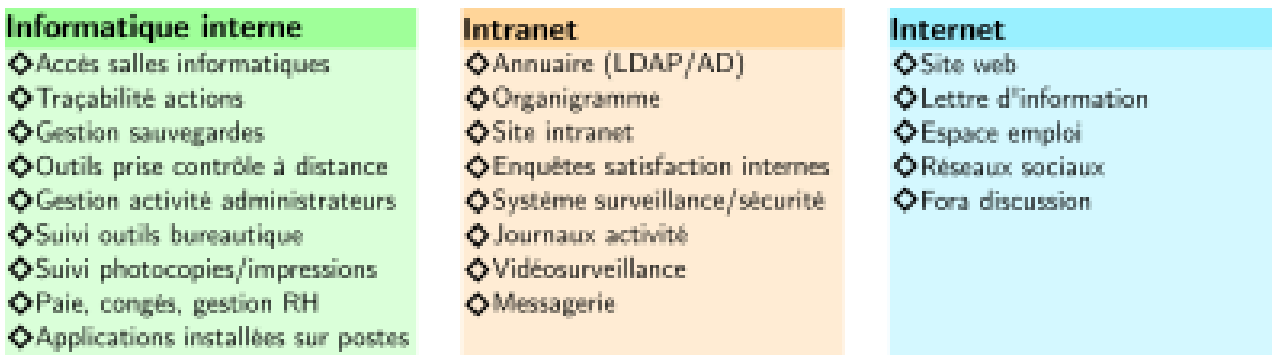
Et aussi...

- co-responsabilité **automatique** sous-traitants (y compris GAFAM...) $\rightarrow$ contractualisation impérative
- obligations « sécurité et confidentialité par conception » (pour les données nominatives)
- portabilité données personnelles
- obligation notification violations

Plan

Registre des traitements – 1

- Tracer tous traitements de données personnelles
- Théoriquement selon taille entreprise ($\geq$ 250 personnes)
- Obligatoire prouver conformité tous traitements
- Difficile sans liste exhaustive
- Registre doit être tenu à jour



Évolution poste

Désigner un délégué à la protection des données (*data privacy officer*). Obligatoire dans secteur public, ou si traitements à grande échelle

Registre traitements – 2

Registre doit indiquer, pour chaque traitement

- nom et coordonnées responsable(s) traitement et délégué à la protection des données
- finalités traitement
- catégories personnes concernées et catégories données personnelles
- catégories destinataires données, y compris tiers, hors pays collecte ou entité internationale
- existence transferts hors pays collecte ou vers entité internationale
- délais effacement selon catégories des données (quand donnée devient-elle inutile ?)
- description générales mesures de sécurité techniques et organisationnelles

Minimisation des données

- Uniquement données personnelles *strictement nécessaires* pour chaque traitement
- Purger/nettoyer données existantes (volume collecté et durée conservation)
- Réflexion de fond sur *tous* traitements existants
- Avec contraintes légales de conservation de certaines données

Exemple minimisation

Liste de diffusion : adresse électronique (et rien d'autre)
Départ collaborateur : garder informations légales (contrat, versements, etc.), éliminer l'inutile (dates congés pris, photo pour badges, etc.).

Licéité traitement et consentement

Traitement licite si au moins une condition remplie :

1. Consentement explicite, éclairé et univoque
2. Traitement nécessaire pour exécution contrat (ou mesures précontractuelles) auquel la personne est partie
3. Traitement nécessaire pour respect obligations règlementaires du responsable du traitement
4. Traitement nécessaire pour sauvegarde intérêts vitaux personne ou tiers
5. Traitement nécessaire pour exécution service intérêt public par responsable du traitement

Consentement

- Consentement explicite, éclairé et univoque
- Fournir toutes informations nécessaires pour prise décision
- Pouvoir apporter preuve consentement utilisateur

Exemples

- lettre information : consentement explicite
- cafétéria : consentement explicite
- paye : obligation légale (noter celle-ci)

Questions en suspens

Que faire pour traitements anciens, non conformes (pas trace consentement explicite) ?
Fournisseur peut-il dire « faute d'acceptation de tous ces traitements, pas de service » ?

Mentions légales – 1

- identité et coordonnées responsable du traitement
- coordonnées *délégué à la protection des données* s'il existe
- finalité et base juridique traitement
- destinataires données
- transfert éventuel vers pays tiers/organisation internationale

Mentions légales – 2

- durée ou critères conservation
- droit d'accès, de rectification, d'effacement
- droit de limitation ou d'opposition au traitement
- droit de retrait du consentement
- droit réclamation auprès autorité de contrôle
- indication si fourniture données est à caractère règlementaire, contractuel ou conditionne conclusion contrat
- informations sur données obligatoires ou non et conséquences non fourniture données

Portabilité données

- Pouvoir fournir à l'intéressé *toutes les données* le concernant
- Dans délais raisonnables
- Dans format structuré, couramment utilisé, lisible par une machine

Attention !

Impératif vérifier demandeur a pleine légitimité à faire la demande. Héritier/époux/maîtresse ne sont pas légitimes sans accord explicite du propriétaire (si décédé... compliqué).

Obligation notification

- Dans les meilleurs délais, de préférence sous 72 heures après détection incident
- violation (accidentelle ou intentionnelle) sécurité avec perte, destruction, altération, divulgation ou accès non autorisé(s)
- notification CNIL (prioritaire) et personnes concernées (un peu moins, mais doivent être prévenues)
- notification doit indiquer
  - description nature violation, catégories et nombre victimes, volume données concernées
  - nom et coordonnées DPD
  - conséquences probables pour victimes
  - mesures remédiation ou atténuation mises en place
  - mesures pour prise en charge préjudice