EIFR

Séminaire du 9 février 2016

La protection des données à caractère personnel dans le secteur financier

Paul-Olivier Gibert, président, Association française des correspondants à la protection des données à caractère personnel

Stéphane Grégoire, chef du service des Affaires économiques, Commission nationale de l'informatique et des libertés

Fabrice Naftalski, avocat, EY

François Rosier, directeur adjoint des Affaires juridiques, direction des Affaires juridiques, fiscales et de la concurrence, Fédération française des sociétés d'assurance

Dominique Calmes, juriste IT/IP/data, direction des affaires juridiques, BNP Paribas

Florence Bonnet, associée, CIL Consulting

Marie-Noëlle Gibon, *data protection officer*, La Banque postale

Philippe Salaun, correspondant informatique et libertés, CNP Assurances

Paul-Olivier Gibert

Des ruptures

Une évolution technique majeure : la sortie des données des systèmes d'information.

Emergence du *big data*, du *smart data*, des lacs de données.

Le règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ou règlement général sur la protection des données).

Le texte de compromis a été approuvé en décembre 2015. Le règlement devrait entrer en vigueur au printemps 2016 et en application au printemps 2018.

Le devoir de rendre compte se substitue aux déclarations.

Obligation de documenter.
Notion d'impact préalable sur la vie privée.
Notion de droit à l'oubli numérique.
Notion de droit à la portabilité (pouvoir récupérer ses données dans un format réutilisable).
Des sanctions pouvant représenter jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise.

Les enjeux sont significatifs, y compris d'un point de vue économique (une nouvelle source de création de valeur).

Stéphane Grégoire

Règlement général sur la protection des données

Ce texte a notamment pour objectif d'harmoniser les règles à l'intérieur de l'Union européenne et de mieux contrôler les grands groupes situés hors de l'Union européenne.

Un texte de 200 pages, mais tous les concepts ne sont pas explicités.

Il prévoit la création d'un organisme européen ad hoc.

Champ d'application :
Champ d'application matériel très large.
Une révolution s'agissant du champ d'application territorial :
. Les dispositions s'appliquent aussi aux responsables des données ou à leurs sous-traitants établis en dehors de l'Union européenne qui mettent en œuvre des traitements visant à fournir des biens ou des services à des résidents européens ou à les surveiller.

Des principes précisés, mais pas d'évolutions notables.

Un renforcement global des droits existants.
Le droit d'accès est précisé.
Le droit à l'effacement et à l'oubli numérique confirmé.
De nouveaux droits comme la portabilité des données.

Introduction du principe d'*accountability* (principe de responsabilité, obligation de rendre compte).

. Prendre des mesures appropriées ; être en mesure de prouver la conformité du dispositif à tout moment.

. Selon une approche dynamique : évolution en fonction des risques encourus.

Compétences étendues des autorités nationales (*Data Protection Authorithies*).

Coopération entre autorités nationales.

. Principe du guichet unique (*one-stop-shop*).

Création du Conseil européen des autorités nationales de protection des données.

. Le juge de paix en cas de désaccord entre autorités nationales.

Fabrice Naftalski

Principes fondateurs de la loi informatique et libertés :

Déclarer les traitements de données à caractère personnel, après avoir vérifié la faisabilité du traitement.

Informer les personnes concernées.

Protéger les données.

Effacer régulièrement les données.

Permettre aux personnes concernées d'exercer leur droit d'accès, de correction, d'opposition.

Sécuriser les transferts hors de l'Union européenne.

Transferts internationaux des données personnelles :

. On peut transférer des données hors de l'Union européenne si le pays est reconnu par la Commission européenne comme offrant un niveau de protection des données suffisant.

. Ou, si des clauses contractuelles types approuvées par la Commission européenne sont signées entre les entreprises concernées.

. Ou, si des règles internes d'entreprise (*Binding Corporate Rules*) sont adoptées à l'échelle du groupe.

. Depuis l'invalidation de l'accord entre les Etats-Unis et l'Union européenne, dit Safe Harbor (Cour de justice de l'Union européenne, 6 octobre 2015), il faut se tourner soit vers les clauses types, soit vers les règles internes d'entreprise.

. Des outils d'encadrement des transferts dans le nouveau règlement européen.

François Rosier

Pack de conformité assurance

La Commission nationale de l'informatique et des libertés (CNIL) a suscité ce pack en 2012 : deux ans de travaux et de discussions, qui ont débouché sur cinq délibérations (deux normes simplifiées et trois autorisations uniques).

Ce pack constitue un outil de pilotage de la conformité.

Ce pack constitue un élément de sécurité pour les membres de la Fédération française des sociétés d'assurance.

Refonte de la norme simplifiée 16 (gestion et passation des contrats d'assurance) :

Les types de données concernées.

Durée de conservation.

Information des personnes : utilisation faite des données, droit d'accès…

Norme simplifiée 56 (gestion commerciale).

Autorisation unique 31 :

Définit les conditions d'accès au répertoire national d'identification des personnes physiques.

Autorisation unique 32 :

Traite les données relatives aux infractions, condamnations, mesures de sûreté…

Autorisation unique 39 (lutte contre la fraude) :

Les points sensibles lors des discussions avec la CNIL : durée de conservation des données ; information aux personnes.

Dominique Calmes

Pour les banques, il existe un environnement réglementaire constitué notamment :

D'autorisations uniques : AU 045 – consultation du répertoire national d'identification des personnes physique dans le cadre de la loi Eckert du 13 juin 2014 ou encore AU 003 – blanchiment de capitaux ; financement du terrorisme et sanctions financières.

De normes simplifiées : NS 13 – gestion des crédits ou des prêts consentis à des personnes physiques ou NS 12 – tenue des comptes de la clientèle et traitement des informations s'y rattachant par les établissements bancaires et assimilés.

De contrôles effectués et de sanctions (rares) infligées par la Commission nationale de l'informatique et des libertés (CNIL).

En octobre 2014, la CNIL lance le pack de conformité pour les banques (après l'assurance, le logement social, l'énergie), avec l'objectif d'établir un ensemble de règles et de bonnes pratiques déclinées au moyen des vecteurs juridiques existants (normes simplifiées, autorisations uniques, recommandations…), de rédiger des fiches pratiques, de réfléchir à des processus organisationnels (code de bonne conduite, labels…).

Les attentes des banques à l'égard du pack : favoriser le discussion avec le régulateur, simplifier les formalités, renforcer la sécurité juridique, donner un cadre aux traitements sensibles (lutte contre la fraude, big data…), anticiper les nouvelles obligations du règlement général sur la protection des données…

Florence Bonnet

Avantages liés à la désignation d'un correspondant informatique et libertés (CIL) externe :

Accès facilité à la Commission nationale de l'informatique et des libertés.

Disposer d'une expertise dans un domaine en pleine évolution.

L'entreprise ne dispose pas toujours des ressources internes suffisantes.

Le CIL externe peut faire le lien entre les différentes parties prenantes à l'intérieur de l'entreprise (conduite de projets).

Des entreprises peuvent hésiter à explorer le potentiel de domaines comme le *big data*. Si elles ne le font pas, d'autres le feront.

Le règlement général sur le traitement des données va dans le bon sens, notamment avec les notions de certification, de label et de code de conduite.

Marie-Noëlle Gibon

Qu'est-ce qu'un correspondant informatique et libertés ?

Il cible les bons interlocuteurs, notamment dans les champs de la conformité, du juridique, de l'informatique, du marketing…

. Il anime un comité « privacy »

. Il dialogue avec l'extérieur : CNIL, Fédération bancaire française…

Il sensibilise les métiers : sensibilisation, formation, boite à outils (fiches, affiches, intranet, quizz, journal interne…).

Il accompagne les métiers dans leurs projets.

Pierre Salaun

Le quotidien d'un correspondant informatique et libertés :

Veiller à la conformité des traitements :

. lancement de produits

. traîtement par les ressources humaines

. intégration de clauses standards dans les contrats de délégation de gestion…

Répondre aux demandes des clients : rectifications, droit à l'oubli…

Sensibiliser, diffuser la culture « informatique et libertés » :

. intranet

. présentation au comité d'entreprise

. mooc…

Anticiper l’impact de la réglementation.

Assister la Commission nationale de l’informatique et des libertés (CNIL) lors des contrôles sur place.

Mobiliser les acteurs en cas de recommandation de la CNIL.

Parler aux autres correspondants informatique et libertés.