Maîtrise des données et RGPD

Jérôme Couzigou – EY

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable.
Les fichiers physiques sont aussi concernés par les règles régissant les données personnelles.
Le sujet devient européen, notamment au travers de la coordination des autorités de protection des données locales (en France, la Commission nationale de l'informatique et des libertés - CNIL).
Règles d'or : délivrer une information accessible, renforcée et tenue à jour ; recueillir et gérer des consentements éclairés parfois explicites ; respecter tous les droits des personnes.
Parmi les challenges à venir : i) il s'agit d'un sujet transversal ii) il revêt une dimension internationale iii) les principes qui régissent le droit sont sujets à interprétation iv) l'approche commerciale qui en découle reste à imaginer v) il faut intégrer l'approche par les risques vi) les enjeux financiers, dont le coût de mise en conformité, sont élevés vii) il y a des connexions avec d'autres règles.

Imad Abounasr - EY

L'application du règlement européen sur la protection des données est « pour demain » (mai 2018), surtout compte tenu de la dimension informatique des chantiers à mettre en œuvre.

Les différentes phases des missions (dans l'ordre chronologique) : cadrage général et portée générale du texte ; analyse des écarts avec le dispositif existant ; élaboration d'une feuille de route ; mise en œuvre de la feuille de route, avec sa dimension interdisciplinaire ; revue régulière du dispositif.

Pour l'instant (octobre 2017), en moyenne, les entreprises en sont au stade de la feuille de route.

Parmi les obstacles à la mise en conformité : manque de ressources internes ; manque de budget ; multiplicité des règles ; définition du périmètre territorial (quelles entités sont concernées ?) ; mise en place d'une organisation, avec, notamment, la question du rôle, des moyens et de la place dans l'organisation du délégué à la protection des données.

Cédric Pommot - EY Financial Services

Comment mettre en œuvre la mise en conformité et avec quels outils ? Il n'y a pas sur le marché de solutions « packagées », mais des initiatives se développent, en mode sofware as a service. L'offre est vaste et variée, tandis que les outils les plus appropriés sont à rechercher chez les éditeurs de premier plan.

Il est ainsi recommandé de se livrer à une veille technologique dans ce domaine, et de coordonner les efforts entre la direction des services informatiques, le responsable des données (chief data officer) et le délégué à la protection des données.

Cinq types d'outils : i) Data analytics (inventaire et scan) ii) gouvernance du délégué à la protection des données (partage des données, alertes, mise à jour des rôles et des responsabilités…) iii) registre des traitements iv) consentement v) vie privée et sécurité (privacy by default, gestion des accès aux données, anonymisation, cryptage, suppression en masse des données…)

Il est recommandé de bien cerner ses besoins et d'évaluer les logiciels existants (du potentiel à exploiter ; cela peut permettre de limiter le nombre de licences)

Tiana Ramanakasina - EY

On assiste à une montée en puissance de l'open data. Les données personnelles en masse permettent de saisir au plus près les besoins exprimés par les clients, de procéder à des ciblages, d'améliorer l'efficacité opérationnelle, d'évaluer le potentiel d'un marché, ou encore d'étudier la concurrence.

Il existe des techniques analytiques (pilotage du projet, text mining, process mapping, visualisation des données, sécurité des systèmes d'information…) qui permettent de se mettre en conformité avec le règlement européen sur la protection des données tout en améliorant la relation avec les clients, en enrichissant l'offre de services et en renforçant l'image de l'entreprise.

De nouvelles habitudes à intégrer : rendre les données anonymes (elles ne seront plus assujetties aux règles sur la protection) ; attribuer des pseudonymes (les données demeurent assujetties).

Pierre Bienvenu - ACPR

De façon générale, l'Autorité de contrôle prudentiel et de résolution (ACPR) applique de façon constante trois principes : la neutralité technique (pas d'à priori à l'égard des innovations) ; proportionnalité (approche par les risques) ; la sécurité ne doit pas être minorée par des avancées techniques.

Les données constituent le principal défi actuel des établissements financiers : on a affaire à une explosions de ces données (données de connexion, mais aussi satellitaires, météorologiques, maritimes…), qui constituent d'ailleurs la principale matière première des fintechs. Parallèlement, on assiste à une révolution réglementaire avec, par exemple, la deuxième directive européenne sur les services de paiement (DSP 2), qui fait obligation aux établissements financiers de partager certaines données personnelles et on constate une multiplication des cyberattaques (cibles récentes : Yahoo, Equifax).

Les enjeux sont donc très forts pour tous les acteurs de la finance, qui disposent pour y faire face de nouveaux outils puissants, dont l'intelligence artificielle. L'industrie financière peut retourner cette situation en sa faveur, car elle peut prétendre au statut de tiers de confiance dans le domaine des données personnelles (de nombreuses fintechs se sont engouffrées dans ce créneau).

Les acteurs de la finance doivent avoir conscience qu'en ce qui concerne la sécurité, les données bouleversent les frontières sectorielles (l'ACPR collabore d'ailleurs avec la CNIL) et que la « sécurité bunker » n'est plus concevable. Dans le domaine de la stratégie : il est indispensable de disposer des meilleures compétences humaines, au moment où la finance a perdu de son aura.

Xavier Leclerc - DPMS

En France, la législation est ancienne (loi informatique et libertés de 1978) et se fondait sur des principes repris dans le règlement européen sur la protection des données. Une nouveauté cependant, la notion de privacy by design (protection de la vie privée prise en compte dès la création d'un produit), qui introduit la coresponsabilité (responsabilité d'un éditeur de logiciels par exemple).

Environ 70 % des correspondants informatique et libertés (CIL) ne deviendront pas délégués à la protection des données : les CIL n'ont la plupart du temps ni les moyens, ni la formation nécessaire. La fonction de délégué à la protection des données nécessite des connaissances, de l'expérience et de la formation continue.

Attention : on assiste à une prolifération de délégués à la protection des données externes.
Un projet en cours de certification des délégués à la protection des données (avec Bureau Veritas).
A propos de la mise en conformité avec le règlement européen :
On n'est jamais conforme à 100 %, aussi faut-il être capable de montrer au superviseur que l'on déploie des moyens pour se mettre en conformité.
Il est judicieux de partir de l'historique des sanctions de la CNIL : cela peut donner une liste des priorités.
La nouvelle approche est d'inspiration anglo-saxonne : la notion de traçage est fondamentale.
C'est une culture qu'il convient de mettre en place, car le maillon faible du dispositif est l'humain.
En ce qui concerne l'élaboration du registre des traitements, la cartographie à l'aide d'outils informatiques ad hoc est insuffisante, car toutes les données personnelles ne sont pas digitalisées.

Hermann Kamdem - Datanaos

La cartographie des traitements est très difficile à réaliser, en raison de l'hétérogénéité des systèmes d'information et de la présence de données non structurées.

Etapes lors d'une intervention dans l'entreprise : i) identification des traitements ii) quelles sont les types de données ? qui est concerné (fournisseurs, clients…) iii) évaluation des risques (conformité ou pas ?) iv) actions à mener (anonymisation, chiffrement, archivage, cloisonnement, suppression des données inutiles…).

Frédéric Germain – Société Générale

A la Société générale, la protection des données personnelles est directement rattachée à l'un des trois directeurs généraux délégués. Le dispositif comprend vingt-sept unités. L'objectif prioritaire est de renforcer la confiance des clients à l'égard de la banque.

La protection des données personnelles s'y inscrit dans un cadre plus global, ce qui nécessite, entre autres, des relations entre les équipes chargées de la protection des données et celles de la sécurité des services informatiques, ainsi que des échanges entre le délégué à la protection des données et le responsable de la sécurité (chief security officer).

La banque faisait appel aux services de Varonis (lire plus bas) avant même l'élaboration du règlement européen sur la protection des données, principalement pour traiter les données non structurées.

Julien Chamonal - Varonis

Varonis (cent salariés en France) est spécialisé dans la protection des données et dans la sécurité des systèmes d'information.

On assiste à une montée en puissance des attaques, qui visent le plus souvent des données personnelles, plus solvables, et en particulier les données non structurées (qui se situent hors du champ des logiciels de gestion intégrés ou des logiciels de paie).

Contrairement à l'idée que l'on s'en fait, les données non structurées constituent le sous-ensemble le plus important en volume.

Dans une entreprise cliente de 5000 salariés comptant 265 000 fichiers et 1,2 million de permissions d'accès, Varonis a dénombré 1250 fichiers sensibles, dont un tiers n'avait jamais été utilisé depuis trois ans.

Deux règles de bonne hygiène dans la gestion des données personnelles : se débarrasser des données devenues inutiles et limiter les accès.

Amine Talbi – Tessi Groupe

Tessi est une entreprise spécialisée dans les flux d'informations et dans la relation avec les clients qui compte 7000 salariés.

Plusieurs niveaux dans l'organisation de la protection des données :

DPO (data protection officer) : directement rattaché à la direction générale, c'est l'acteur central, qui construit, tient à jour et anime le programme de protection des données. Il est assisté de deux juristes. Une revue de direction semestrielle, avec le directeur général, le directeur des systèmes informatiques, le directeur de la sécurité des systèmes informatiques.

Les relais DPO, qui assurent l'interface avec les unités opérationnelles. Un comité de pilotage conformité par trimestre, qui réunit le relais DPO, le directeur de l'unité/filiale, le DPO, le directeur de la sécurité des systèmes informatique…

Les interlocuteurs projet. Un comité « unité opérationnelle » par mois où figure, notamment, le relais DPO.

Les facteurs de succès : des objectifs et un calendrier clair ; rôle des acteurs bien défini ; soutien de la direction générale ; une communication adéquate ; des priorités en fonction des enjeux et des risques.

Martina Duchonova - BNP Paribas Securities Services

BNP Paribas Securities Services est présent dans trente-quatre pays, dispose de plusieurs entrepôts de données en dehors de l'Union européenne et externalise de nombreuses prestations : autant de difficultés dans le champ de la protection des données.

Les grandes étapes du projet :

Définition de la « gouvernance » : personnes compétentes, prestataires de services compétents ; mise en place de l'organisation (ateliers, comités, compte rendus…).
Recensement de l'existant : de multiples points de non-conformité à identifier ; difficulté d'évaluer le risque de non-conformité.
Définition de l'organisation cible.
Analyse budgétaire
Planning
Plan de remédiation
Communication et sensibilisation : un facteur essentiel de réussite du projet