Juin 2017

Note de conjoncture

Banques et Assureurs à l'épreuve du RGPD : Impacts multiples et opportunités à saisir

Le Règlement Général sur la Protection des Données à Caractère Personnel RGPD sera applicable à partir du 25 mai 2018. Compte tenu de l'imminence de l'entrée en force du règlement, les opérateurs économiques entament les préparatifs à la mise en conformité. Consciente de la complexité du RGPD et de son champ d'application vaste, la CNIL a publié en mars une méthodologie à suivre en 6 étapes.

Cette note de conjoncture propose la lecture de Siltéa sur les impacts d'un règlement qui affecte les acteurs de la banque et de l'assurance.

Une protection renforcée des personnes physiques via de nouveaux droits, l'extension de droits existants et un encadrement renforcé du consentement

Nouveaux droits pour les personnes physiques

Toute personne située sur le territoire de l'UE dispose de droits nouveaux liés au traitement des données à caractère personnel la concernant :

- Droit à la portabilité des données
- Droit à la limitation du traitement
- Droit à une information complète sur ses droits dans un langage clair
- Droit à une action collective en responsabilité

Extension de droits existants

Le RGPD a également étendu certains droits existants des personnes physiques :

- Droit à l'accès aux données détenues par l'opérateur économique
- Droit à la suppression des données, notamment en cas de retrait du consentement
- Droit au déréférencement sur les moteurs de recherche, inscrit désormais dans la loi
- Droit d'opposition au traitement
  - Charge de la preuve reposant désormais sur le responsable du traitement
  - Droit d'opposition spécifique au profilage

A noter : le droit à la rectification évolue peu.

Encadrement renforcé du consentement

Les finalités de traitement qui donnent lieu au recueil du consentement sont davantage encadrées.

Finalités requérant un consentement	Finalités ne requérant pas un consentement
• Prospection au moyen d'un mode de communication électronique (Email, SMS, MMS) hors produits ou services analogues • Prospection au moyen d'automates d'appel ou télécopieurs • Cession à des partenaires d'adresses électroniques ou de numéros de téléphone à des fins de prospection par automate, télécopie, Email, SMS, MMS • Collecte ou cession de données sensibles • Collecte de la photographie ou de l'image de la personne	• Données nécessaires à l'exécution du contrat • Exécution de services connexes au service rendu • Prospection commerciale pour des produits ou services analogues • Lutte contre la fraude • Lutte contre le blanchiment des capitaux et le financement du terrorisme • Poursuite d'une mission d'intérêt général • Respect d'une obligation légale

Désormais, le consentement devra être donné par un acte positif clair de la personne concernée. En cas de silence, de cases cochées par défaut ou d'inactivité, le consentement sera vicié.

De nouvelles obligations pour l'ensemble des opérateurs économiques qui se traduisent par des impacts opérationnels forts

Champ d'application vaste

Tous les acteurs qui manipulent des données à caractère personnel à l'aide de procédés automatisés sont concernés par les nouvelles obligations, qu'il soit question des responsables du traitement ou des sous-traitants.

1) Responsable du traitement : clé de voûte du dispositif

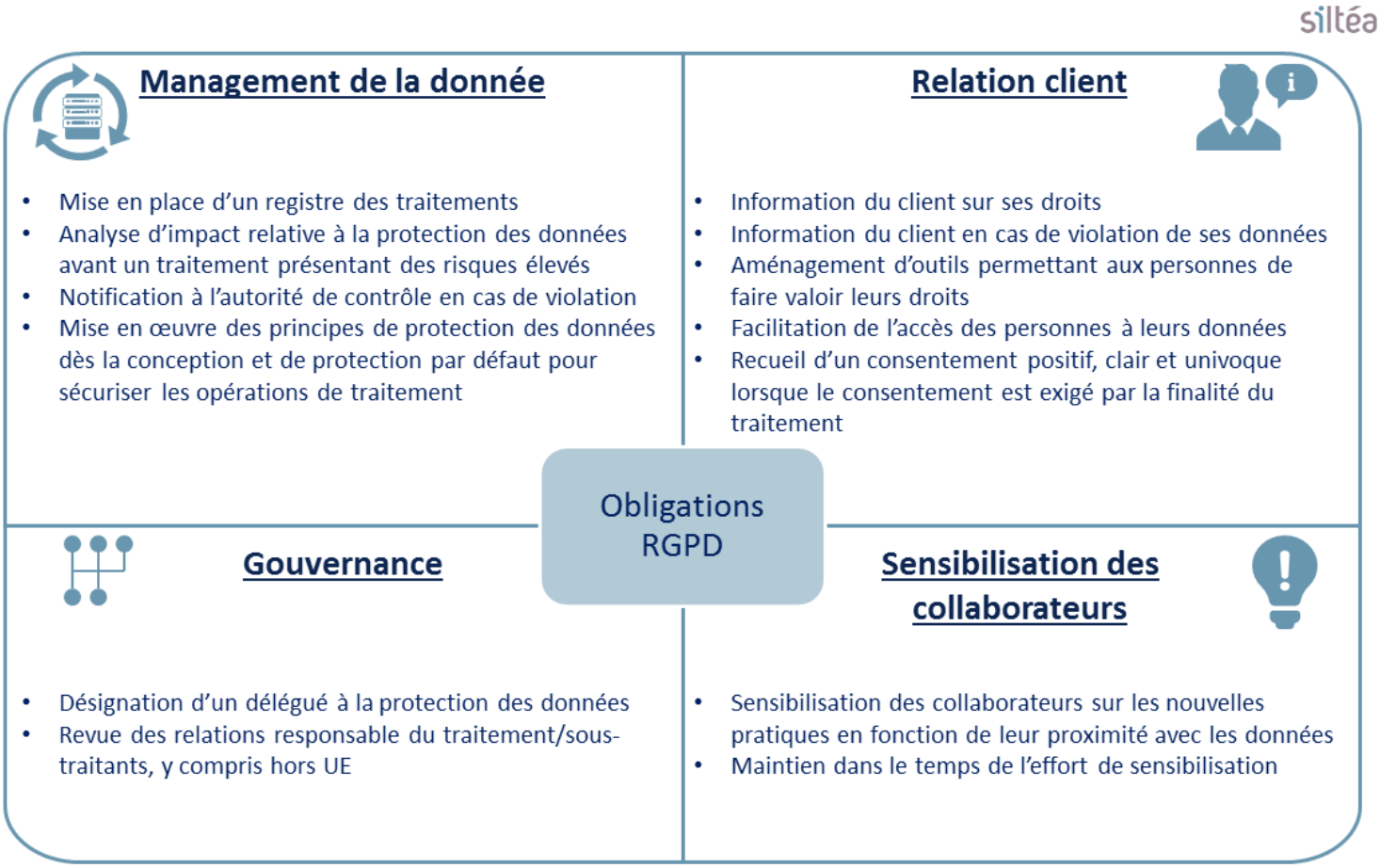
Il s'agit de la personne physique ou morale qui détermine les moyens et les finalités du traitement. Le responsable du traitement se situe au centre du dispositif de protection des données personnelles. S'il n'est plus soumis à l'obligation de déclaration préalable à l'autorité de contrôle pour les traitements communs (déclaration CNIL), le responsable du traitement est désormais pleinement responsable de tout manquement au cadre juridique en vigueur.

2) Sous-traitant : nouvel entrant dans le périmètre des obligations

Il s'agit de la personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable du traitement. La notion de sous-traitant est entendue de manière large et comprend les personnes qui effectuent des traitements de faible importance et/ou à titre gracieux. Absent du périmètre de la directive de 1995, le sous-traitant entre dans le champ d'application du RGPD afin de protéger les personnes dans le cadre de traitements sous-traités hors de l'UE.

Obligations nombreuses classables en quatre catégories

Les obligations prévues au chef des opérateurs économiques par le RGPD recouvrent plusieurs thèmes :



A noter : ces obligations s'appliquent également aux traitements existants.

Par ailleurs, les acteurs concernés devront croiser les contraintes introduites par le RGPD avec les obligations en matière de découverte et de connaissance client issues des réglementations MIF 2 et DDA.

Impacts opérationnels forts sur les organisations
Ces obligations auront des impacts multiples sur les acteurs de la banque et de l'assurance :

- Adaptation des dispositifs de gouvernance pour déterminer et délimiter les responsabilités de tous les acteurs de la chaîne du traitement
- Revue et refonte des processus métier faisant intervenir le traitement des données
- Adaptation des procédures de contrôle interne aux nouvelles contraintes issues du règlement
- Evaluation de la robustesse et de la résilience des dispositifs techniques en place et revue des processus techniques en cas de besoin
- Documentation des dispositifs mis en œuvre en application du RGPD en cas de contrôle de la CNIL

Une opportunité à saisir pour les assureurs

Les assureurs sont doublement impactés par le RGPD :

1. En tant que responsables du traitement
2. En tant qu'offreurs de produits Responsabilité civile professionnelle (RCP).

A ce titre, les assureurs RCP pourraient être incités à :

- Restructurer leur offre pour proposer des produits mieux adaptés à la couverture du cyber-risque
- Accompagner leurs clients sur la voie de la mise en conformité
- Moduler les primes en fonction du degré d'exposition au risque de leurs clients
- Appliquer des exclusions aux garanties offertes en cas de prise de risque excessive de la part des clients
- Prendre en charge les indemnités pécuniaires à la charge des responsables du traitement à l'issue d'actions civiles en justice

A propos de Siltéa

Siltéa a développé des compétences fortes sur les évolutions réglementaires et leurs impacts sur les organisations, que ce soit dans le domaine de la banque ou de l'assurance, en s'appuyant sur un centre de compétence interne qui organise une veille continue sur ces sujets. Forts de notre expérience dans la mise en conformité des organisations avec Solvabilité 2, MIF 2 et la DDA, ainsi que de notre connaissance approfondie des problématiques liées à la gestion des données personnelles, nous sommes en mesure de vous accompagner pour la mise en œuvre des chantiers relatifs au RGPD, avec une démarche adaptée à vos besoins :

- Diagnostic des traductions opérationnelles de vos obligations en matière traitement de données à caractère personnel
- Analyses d'impacts sur vos systèmes d'information et vos processus
- Pilotage des travaux visant à mener à bien l'adaptation de votre organisation face à ces défis souvent structurants et contraints dans le temps
- Intégration des travaux de conformité avec le RGPD au sein de vos chantiers réglementaires qui présentent un volet traitement des données (DDA, MIF2) dans le but de réaliser des synergies

Nous pouvons également partager avec vous les résultats de nos études internes et travaux de fond sur les sujets qui vous animent au quotidien.
Marko SANKOVIC, *Consultant Siltéa*