Impacts de la Réglementation RGPD sur la Banque de Détail et d'Investissement

« En 2019, le secteur bancaire poursuit sa mise en conformité vis-à-vis de la réglementation européenne RGPD. Les exigences semblent impacter plus les activités de Retail que les activités CIB »

Janvier 2019

DEVLHON CONSULTING

"La RGDP met sur le même pied d'égalité les entreprises établies au sein de l'Union européenne et celles basées hors d'Europe et met fin à une distorsion de concurrence"

Le Règlement Général sur la Protection des Données

Mise en conformité du secteur bancaire

Dans le cadre de la démarche de mise en conformité du secteur bancaire face à la RGPD (Règlement Général sur la Protection des Données), ce document s'appuie sur les éléments principalement publiés par la CNIL (Commission Nationale de l'Informatique et des Libertés) afin de clarifier les actions à mener par les **Banques de Financement & Investissement** ainsi que les **Banques de Détail**. A ce jour, le secteur bancaire poursuit sa mise en conformité vis-à-vis de la réglementation européenne RGPD. Les exigences semblent impacter plus les activités de la Banque du Detail que les activités CIB.

Que dit le règlement ?

La RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne et en dehors de celle-ci. Tout organisme quelle que soit sa taille, son pays d'implantation et son activité, peut être concerné. Or, la RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

- Qu'elle est établie sur le territoire de l'Union européenne
- Que son activité cible directement des résidents européens (toutes nationalités confondues)

La RGDP met sur le même pied d'égalité les entreprises établies au sein de l'Union européenne et celles basées hors d'Europe et met fin à une distorsion de concurrence.

Quelle donnée est concernée ?

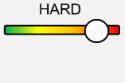
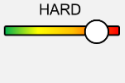
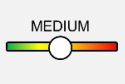
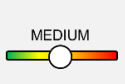
Le type de donnée qui est concernée par le RGPD est la donnée dite 'personnelle'. Une « donnée personnelle » corresponde à toute information se rapportant à une personne physique identifiée ou identifiable. Une personne peut être identifiée **directement**, par exemple, par son nom et prénom, ou **indirectement**, par un identifiant (n° client), un numéro de téléphone, une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image. L'identification d'une personne physique peut être réalisée à partir **d'une seule** donnée (exemple : numéro de sécurité sociale, ADN), ou à partir **du croisement de données** (par exemple, une femme vivant à telle adresse, née tel jour et militant dans telle association).

Les types de banques

Dans cet article, nous présentons les impacts de la réglementation RGPD sous 2 perimètres bancaires spécifiques: la **Banque de Détail** et la **Banque de Financement & Investissement** (**BFI** et aussi appellées **CIB**). Chacune possède une activité, une clientèle, une organisation et des métiers différents. Le tableau ci-dessous introduit plus en détail ces sujets :

SUJET	BANQUE DE DÉTAIL	BANQUE D'INVESTISSEMENT ET FINANCEMENT
Activités	La collecte de dépôts, la distribution de crédits et la gestion de moyens de paiement sont les principales activités de la banque de détail. Des services et produits d'une autre nature (assurance, téléphonie, services à la personne, immobilier...) sont de plus en plus souvent proposés.	Les opérations financières comme les introductions en Bourse, les fusions acquisitions des sociétés, les émissions de titres ou de produits financiers et les opérations de vente et de trading sur les marchés constituent les activités spécifiques à la BFI.
Clientèle	Les activités de la banque de détail sont orientées vers la clientèle de particuliers, de professions libérales et d'entreprises de petite taille (commerçants, artisans...).	Les principaux clients de la banque de financement et d'investissement sont les grandes entreprises, les investisseurs institutionnels, les gestionnaires de fonds, les États.
Organisation	Les banques de détail s'appuient sur des réseaux d'agences bancaires. Mais ces dernières sont complétées par les services de banque à distance : banque en ligne (centres de relation clients) et banque internet.	Les BFI font partie de grands groupes bancaires universels mais elles ont leur organisation et leurs personnels propres.
Métiers	On retrouve principalement les métiers suivants : - Chargé d'accueil et services à la clientèle - Chargé de clientèle particuliers - Chargé de clientèle professionnels - Conseiller en patrimoine - Chargé de clientèle entreprises - Responsable / animateur d'unité commerciale - Analyste risques - Gestionnaire de back office - Spécialiste des opérations bancaires - Responsable d'activités de traitement bancaire - Responsable informatique / organisation / qualité - Informaticien / chargé de qualité - Analyste risques	La BFI est principalement représentée par les métiers suivants : - Chargé de clientèle entreprises - Opérateurs de marché - Concepteur et conseiller en opérations et produits financiers - Autres métiers (les BFI ont leur propre état-major, DRH etc.…) - Gestionnaire de back office - Spécialiste des opérations bancaires - Responsable / animateur d'unité ou d'activités de traitement bancaire - Responsable informatique / organisation / qualité - Informaticien / chargé de qualité - Analyste risques

Impacts concrets pour la Banque de Détail

CHANTIERS		EXIGENCES RGPD	BANQUE DE DÉTAIL
Consentement Client		La preuve du consentement indubitable de la personne concernée par le traitement de ses données personnelles doit être démontrée par l'établissement effectuant le traitement. Le consentement sera valide dans le seul cas où il est libre, clair et distinguable d'autres problématiques.	Le consentement est requis dans le cadre d'activités de la banque du détail. L'impact sur les activités est lourd du fait de l'utilisation de données strictement personnelles employées et clients, tels que les transactions bancaires de personnes physiques (donnant information sur ses habitudes d'achats, par exemple).
Gestion des Droits		Le Data Subject dispose de plusieurs droits sur ses données personnelles (traitées) qui doivent être garantis par l'établissement : Droit d'accès aux données, Droit de rectification des données, Droit à l'effacement lorsque qu'il retire son consentement à leur traitement et Droit d'opposition au traitement.	Le périmètre de données traitées par les activités de Détail concerne des personnes morales et physiques. L'impact est fort du fait qu'il faut définir une gouvernance afin de recevoir, gérer et stocker les droits sur toute donnée traitée dans le cadre d'activité de la banque de détail.
Privacy Impact Assessment		Le PIA (Privacy Impact Assessment) est un process selon lequel une organisation identifie et minimise les risques liés à la protection des données d'un nouveau projet. Il doit être implémenté dès qu'un projet représente un risque élevé pour les particuliers.	Les services d'une Banque de Détail (assurance, crédit, épargne, etc.) cible des personnes physique. Or, la RGPD a un impact moyen-fort puisque presque la totalité des projets doit se mettre en conformité en faisant les analyses d'impact sur la privacité. Néanmoins, par sa nature d'activité, la Banque effectue un certain nombre d'analyse autour des risques.
Information		Certaines informations doivent être communiquées au Data Subject lorsque des données personnelles sont collectées (contact du régulateur et du DPO, raison du traitement des données, informations par rapport aux droits du Data Subject…).	La charte de protection des données doit s'aligner avec les exigences du RGPD. Cela suppose également la mise à jour des procédures de collecte de données afin d'y inclure une notice d'information, et un processus de capture des évolutions du traitement de l'information.
Transfert de données		Le Transfert vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si certaines conditions sont respectées par le responsable du traitement et le sous-traitant.	Des nouvelles clauses d'adaptation à la RGPD doivent être mises en place entre la Banque et tout fournisseur basé à l'international. Il s'agit principalement d'une tache administrative qui se dérivera de la cartographie de données et leur localisation.
Privacy By Design		Le concept de la « Protection de la Vie Privée dès la Conception » permet d'intégrer les notions du RGPD dès la conception d'un nouveau produit, process ou système de manière proactive et préventive. Le Privacy-by-Design facilite le traitement de données personnels et limite les violations de la protection des données lors du lancement d'un nouveau projet.	L'impact est très important pour les activités de la Banque du Détail, avec comme mesure : • Cartographie des données personnelles avec traitements associés • Définition d'une gouvernance pour la mise à jour des process associés
Sécurité IT		L'obligation de notification des failles de sécurité est élargie sous la RGPD : celle-ci doivent être notifiées à la CNIL ainsi qu'aux *Data Subjects* concernés. Le contenu de la notification est également alourdi.	Mise à jour de processus tels que : management de failles de sécurité, procédure de notification en cas de faille et mise en œuvre de standard de chiffrement des données du SI.

Impacts concrets pour la Banque de Financemenet & Investissement

CHANTIERS		EXIGENCES RGPD	BANQUE DE FINANCEMENT ET INVESTISSEMENT
Consentement Client		La preuve du consentement indubitable de la personne concernée par le traitement de ses données personnelles doit être démontrée par l'établissement effectuant le traitement. Le consentement sera valide dans le seul cas où il est libre, clair et distinguable d'autres problématiques.	Le consentement n'est pas requis dans le cadre d'activités dites d'intérêt légitime. Celui-ci peut néanmoins être demandé quand des données personnelles sensibles sont en jeu. L'impact sur les activités CIB est faible du fait de l'utilisation de données corporate et non personnelles.
Gestion des Droits		Le Data Subject dispose de plusieurs droits sur ses données personnelles (traitées) qui doivent être garantis par l'établissement : Droit d'accès aux données, Droit de rectification des données, Droit à l'effacement lorsque qu'il retire son consentement à leur traitement et Droit d'opposition au traitement.	Le périmètre de données traitées par les activités CIB se limite à celles de ses fournisseurs, clients au statut de personne morale et employés. La principale mesure consiste à adopter une gouvernance afin de recevoir, gérer et stocker les droits des employés sur leurs données personnelles afin de se conformer aux exigences du RGPD.
Privacy Impact Assessment		Le PIA (Privacy Impact Assessment) est un process selon lequel une organisation identifie et minimise les risques liés à la protection des données d'un nouveau projet. Il doit être implémenté dès qu'un projet représente un risque élevé pour les particuliers.	Du fait du périmètre d'activités CIB, l'impact opérationnel du PIA n'est pas conséquent pour ce département, contrairement aux activités Retail.
Information		Certaines informations doivent être communiquées au Data Subject lorsque des données personnelles sont collectées (contact du régulateur et du DPO, raison du traitement des données, informations par rapport aux droits du Data Subject…).	La charte de protection des données doit s'aligner avec les exigences du RGPD. Cela suppose également la mise à jour des procédures de collecte de données afin d'y inclure une notice d'information, et un processus de capture des évolutions du traitement de l'information pour la mise à jour de cette notice.
Transfert de données		Le Transfert vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si certaines conditions sont respectées par le responsable du traitement et le sous-traitant.	L'alignement des contrats fournisseurs de l'UE vers les pays membres de l'UE est requis, notamment à travers la priorisation et l'adaptation des contrats avec les clauses du RGPD.
Privacy By Design		Le concept de la « Protection de la Vie Privée dès la Conception » permet d'intégrer les notions du RGPD dès la conception d'un nouveau produit, process ou système de manière proactive et préventive. Le Privacy-by-Design facilite le traitement de données personnelles et limite les violations de la protection des données lors du lancement d'un nouveau projet.	L'impact est conséquent pour les activités CIB. Les mesures sont les suivantes : • Cartographie des données personnelles avec traitements associés • Définition d'une gouvernance pour la mise à jour des process associés
Sécurité IT		L'obligation de notification des failles de sécurité est élargie sous la RGPD : celle-ci doivent être notifiées à la CNIL ainsi qu'aux *Data Subjects* concernés. Le contenu de la notification est également alourdi.	Mise à jour de processus : management de failles de sécurité, procédure de notification des faille et mise en œuvre de standards de chiffrement.