Octobre 2018

Note de conjoncture

Où en sont les acteurs du secteur financier dans la mise en œuvre du droit à l'information des clients au regard des obligations RGPD ?

Cinq mois après l'entrée en application du RGPD, Siltéa propose un point d'étape des pratiques des acteurs du secteur financier en matière de transparence des traitements. Les banquiers et assureurs informent-ils leurs clients sur les traitements auxquels leurs données personnelles sont assujetties ? Au-delà des traitements, les personnes sont-elles informées de leurs droits ? Quelles sont les pratiques du marché ? Cette note apporte des éléments de réponse, sur la base d'une étude réalisée en octobre 2018[1] et du retour d'expérience Siltéa auprès d'acteurs de la place.

Le droit des personnes à être informées, un corollaire du principe fondamental de transparence

Le RGPD prévoit que toute personne dont les données à caractère personnel font l'objet d'un traitement automatisé dispose d'un droit à être informée. Tous les traitements sont concernés, tout au long de leur cycle de vie, quelle que soit leur finalité ou leur base légale. Le responsable du traitement doit transmettre les informations au moment de la collecte des données, mais également à des moments spécifiques du cycle de vie du traitement : violation des données, modification significative du traitement initial.

Les articles 12, 13, 14 et 34 RGPD comportent les dispositions précises liées au droit à l'information.

Des informations précises à communiquer aux personnes concernées

Trois catégories d'informations doivent être transmises pour permettre à la personne concernée d'appréhender le traitement dans sa globalité :

1 Qui sont les acteurs du traitement ?

- Identité et coordonnées du responsable du traitement
- Coordonnées du délégué à la protection des données
- Sources des données
- Destinataires des données
- Existence d'un transfert international ainsi que les garanties qui l'entourent

[1] Etude réalisée à partir de la documentation client de 30 acteurs représentatifs de la banque et de l'assurance. Les supports suivants ont été étudiés : formulaires de contact, formulaires de devis en ligne, documents de souscription, contrats, bandeaux cookies, espaces cookies, espaces données personnelles.

2 Quelles sont les caractéristiques du traitement ?

- Finalités du traitement
- Base juridique du traitement
- Durée de conservation des données
- Caractère obligatoire ou facultatif du traitement
- Existence d'une décision automatique ainsi que ses modalités

3 Quels sont les droits des personnes ?

- Droit d'accès, rectification, limitation, suppression, opposition, portabilité
- Droit de retirer le consentement
- Droit de déposer une réclamation auprès de la CNIL

Compte tenu de la quantité de renseignements à transmettre, la répartition optimale des informations sur la documentation constitue un enjeu important pour les établissements.

La bonne pratique : structurer l'information en plusieurs niveaux afin de garantir la cohérence globale de la communication

La plupart des acteurs reprend la préconisation de la CNIL de structurer les informations sur deux niveaux afin de la rendre plus accessible :

- **Niveau 1** : informations de synthèse à transmettre immédiatement au moment de la collecte
- **Niveau 2** : exhaustivité des informations liées au traitement, que le client peut consulter à sa guise sur le site internet ou sur un document papier

En ligne, les supports suivants contiennent les informations de niveau 1 à transmettre immédiatement au moment de la collecte :

- Formulaires de prise de contact
- Formulaires de devis en ligne ou de simulation de crédit
- Documents de souscription
- Conditions générales, conventions de compte, règlements mutualistes et autres documents contractuels
- Bandeaux cookies

L'information de niveau 2 figure au sein d'un espace dédié aux données personnelles sur le site internet. Cet espace contient un document exhaustif dont l'intitulé varie selon les acteurs : Politique de la vie privée, Notice de protection des données… Les personnes concernées ont le droit de demander une version papier du document si elles n'ont pas accès à internet.

Une maturité variable dans la mise en œuvre de la transparence au niveau 1

L'étude Siltéa révèle que peu d'acteurs proposent une documentation de niveau 1 à jour des obligations de transparence RGPD. A nos yeux, les éléments suivants permettent d'expliquer ce constat :

- La mise à jour des contrats relève de processus encadrés. La périodicité de mise à jour est annuelle, voire pluriannuelle. La mise aux normes RGPD aura lieu progressivement, au fil des échéances consacrées à la revue des documents.
- La mise à jour des formulaires et des documents de souscription exige un degré d'avancement élevé dans la démarche projet de mise en conformité. Les prérequis sont une

cartographie finalisée des documents de collecte ainsi que la mise en œuvre d'un plan d'action opérationnel de mise à jour de la documentation.

Des obligations globalement respectées au niveau 2, avec la généralisation d'un espace « Données personnelles » sur les sites internet

L'étude des sites internet révèle que 90% des acteurs proposent un espace en ligne dédié aux données personnelles. Cet espace comporte systématiquement un document d'information exhaustif de niveau 2 dont le niveau de complétude est plutôt élevé. Ce résultat s'explique par le caractère *quick win* de l'espace données personnelles en ligne. En effet, l'aménagement de cet espace n'exige pas une cartographie préalable de la totalité de la documentation client existante, comme c'est le cas pour la mise à jour de la documentation de niveau 1.

Conclusion : une approche résolument pragmatique ?

Les résultats de notre étude suggèrent le pragmatisme des banques et des assureurs dans l'application des évolutions réglementaires relatives à la transparence. Ce pragmatisme est reflété dans la mise en œuvre de *quick wins* par la quasi-totalité des acteurs et l'absence de surtransposition par rapport à la lettre de la règlementation.

Les acteurs du secteur financier montrent ainsi rapidement des gages de confiance au régulateur et aux consommateurs. Toutefois, l'inscription dans la continuité de cette relation de confiance dépendra de la capacité à atteindre la cible en matière de documentation de niveau 1. Celle-ci reste la source d'information de référence pour le client au moment critique de la collecte des données. Rappelons que la période de tolérance de la CNIL quant à la mise en œuvre des nouvelles obligations RGPD expire à la fin de l'année 2018.

Marko Sankovic, Consultant Senior

Siltéa & Talan Consulting

Siltéa a développé des compétences fortes dans le domaine de la mise en conformité réglementaire. Forte de ses références RGPD et de ses connaissances des pratiques du marché, Siltéa peut vous accompagner dans vos projets de mise en conformité.

Contacts pour en savoir plus sur l'étude *Droit à l'information RGPD* :

Franck COUAILLIER
Senior Manager
franck.couaillier@siltea.com

Marko SANKOVIC
Consultant Senior
marko.sankovic@siltea.com