Fiche pratique

CONCILIER EXIGENCES LBC/FT ET RGPD

GARY CYWIE
AVOCAT À LA COUR

Alors que les règles internationales, européennes et nationales de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) exigent que des données à caractère personnel soient collectées, le Règlement Général sur la Protection des Données (RGPD)[1] encadre strictement le traitement de ces données, de la collecte à la destruction. Sous réserve d'une certaine discipline juridique, les deux régimes ne sont pas incomptables. Voici quelques clés essentielles de ce dispositif antagoniste mais néanmoins conciliable.

I. LES EXIGENCES LBC/FT

Les entités réglementées de plusieurs secteurs d'activité, en particulier le secteur financier, doivent collecter un certain nombre de données concernant leurs prospects et clients (procédures connues sous les noms de *customer due diligence* ou *know your customer*) et les transactions effectuées par ceux-ci. Outre l'identité des personnes physiques, il faut savoir si elles sont politiquement exposées et quelle est la source des fonds qu'elles utilisent ou de leur patrimoine selon les cas.

Les textes actuellement applicables sont essentiellement la directive modifiée *anti-money laundering* (*AMLD*)[2] et sa transposition en droit national par la loi modifiée du 12 novembre 2004 (la *Loi de 2004*)[3] (les *Règles LBC/FT*).

II. LE RGPD

Plusieurs exigences s'appliquent au *responsable du traitement*[4] des données dont la collecte est imposée par les Règles LBC/FT. De façon générale, chaque entité soumise aux exigences LBC/FT est un responsable du traitement. Ainsi, un prestataire lui-même soumis aux exigences LBC/FT qui effectue également des prestations LBC/FT pour ses clients peut être à la fois un responsable du traitement (vérifications effectuées pour remplir ses propres obligations) et **sous-traitant**[5] (prestations pour le compte d'un autre responsable du traitement) de données à caractère personnel. Les sous-traitants sont eux aussi directement soumis à certaines obligations en vertu du RGPD.

A. Exigence primordiale : satisfaire au moins une des bases légales limitativement énumérées par le RGPD[6]

L'article 43 de l'AMLD précise que « *le traitement de données à caractère personnel sur la base de la présente directive aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme visées à l'article 1er est considéré comme une question d'intérêt public au titre du [RGDP]* ». Cette disposition trouve écho dans l'article 3(6*bis*) de la Loi de 2004 selon lequel *« le traitement de données à caractère personnel sur base de la présente loi aux fins de la prévention du blanchiment et du financement du terrorisme est considéré comme une question d'intérêt public au titre du [RGPD]* » (nous soulignons).

Ainsi, en l'espèce, plusieurs bases légales peuvent s'appliquer, à savoir selon les cas, la nécessité du traitement pour le *respect d'une obligation légale*, l'exécution d'une *mission d'intérêt public* dont est investi le responsable du traitement ou encore aux fins des *intérêts légitimes* poursuivis par le responsable du traitement ou par un tiers (à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel). Cela s'applique également aux traitements portant sur des catégories particulières de données à caractère personnel (dites « *sensibles* »)[7] comme celles qui révèlent les opinions politiques d'une personne (dans le cadre de l'identification des personnes politiquement exposées) et, sous certaines réserves, celles relatives aux condamnations pénales et aux infractions[8].

1. Règlement 2016/679 du 27 avril 2016 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.
2. Directive modifiée (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme.
3. Loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme.
4. Art. 4.7 du RGPD : « La personne physique ou morale (...) qui, seul[e] ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (...) ».
5. Art. 4.8 du RGPD : « La personne physique ou morale (...) qui traite des données à caractère personnel pour le compte du responsable du traitement ».
6. Art. 6 du RGPD.
7. Art. 9 du RGPD. Pour ces données, d'autres bases légales comme l'intérêt public important s'appliquent (Art. 9.2(g) du RGPD).
8. Art. 10 du RGPD.

B. Principes spécifiques clés à respecter pour la collecte de données personnelles dans un contexte LBC/FT

Plusieurs principes doivent être respectés. Si les principes semblent relativement clairs, certaines difficultés peuvent apparaître lors de leur application pratique. Il faut essayer d'anticiper au maximum (*privacy by design*).

Principes de limitation des finalités et de minimisation des données

- Les données ne peuvent être collectées que pour des finalités explicites déterminées[9]. Il ne faut pas collecter plus de données que nécessaire au regard des finalités exprimées de façon transparente[10].
- Les données collectées dans le contexte LBC/FT ne peuvent en principe être utilisées à d'autres fins[11]. Certains types de données peuvent servir plusieurs finalités concomitamment (p. ex. les nom et prénom peuvent aussi servir à établir une fiche signalétique du client). Il faut alors explicitement en informer les personnes concernées.

Principe de transparence

- Il faut informer les personnes concernées de manière générale et spécifique, y compris quant aux finalités poursuivies et sur les modalités de l'exercice de leurs droits[12].
- L'information doit être communiquée avant le début de la relation (sans délai lorsque les données sont collectées auprès de la personne concernée elle-même, sinon maximum dans le mois qui suit)[13].

Principe de limitation de la conservation - droit à l'effacement ou «droit à l'oubli»

- Les données ne peuvent être conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées[14]. La durée de conservation (ou les critères utilisés pour la déterminer) doit être communiquée aux personnes concernées.
- Ainsi, les données collectées exclusivement pour se conformer à la Loi de 2004 doivent être détruites 5 ans après la fin de la relation d'affaire avec le client ou après la date de la transaction conclue à titre occasionnel[15]. Si elles ont été collectées de façon transparente pour d'autres finalités concomitantes (p. ex. signalétique client) elles peuvent parfois être conservées plus longtemps, mais pas indéfiniment.

Sous-traitants de données personnelles[16]

- Un responsable du traitement ne peut faire appel qu'à des sous-traitants qui présentent des garanties suffisantes quant au respect du RGPD et la protection des droits des personnes.
- La relation entre un responsable du traitement et chacun de ses sous-traitants doit être régie par un contrat contenant un certain nombre de stipulations relatives à la protection des données.

Mesures de sécurité techniques et organisationnelles[17]

- Les responsables du traitement et les sous-traitants doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.
- Les mesures doivent prendre en compte l'état des connaissances, les coûts de mise en œuvre et la nature, la portée, le contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques.

Droits des personnes concernées[18]

- Dans certaines conditions, les personnes concernées disposent de certains droits (droit d'information, droit d'accès, droit de rectification, droit à l'effacement, droit d'opposition, etc.).
- Exceptionnellement, en matière LBC/FT, le responsable du traitement doit limiter ou différer le droit d'accès si cela est nécessaire et proportionné pour les besoins de la LBC/FT ou pour éviter de faire obstacle aux mesures prises en application de la Loi de 2004[19].

9. Art. 5.1(b) du RGPD.
10. Art. 5.1(c) du RGPD.
11. Art. 3(*6bis*) de la Loi de 2004.
12. Art. 12 et 13 du RGPD et 3(*6bis*) de la Loi de 2004.
13. Art. 3(*6bis*) de la Loi de 2004 et 13 et 14 du RGPD.
14. Art. 5.1(e) du RGPD.
15. Art. 3(*6bis*) de la Loi de 2004 et 17 du RGPD.
16. Art. 28 du RGPD.
17. Art. 32 du RGPD.
18. Art. 12 à 22 du RGPD.
19. Art. 3(*6bis*) de la Loi de 2004.