Mieux vivre l'immobilier

Février 2018

PROTECTION DES DONNEES PERSONNELLES
Les principales nouveautés

En tant que professionnel de l'immobilier vous gérez des données personnelles.

Ce qui était jusqu'à présent soumis à la loi du 16 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, prend une nouvelle dimension avec le Règlement européen 2016/79 du 27 avril 2016 applicable dans tous les pays membres de l'Union européenne à compter du 25 mai 2018.

Il est d'usage d'employer les termes suivants : « Règlement Général sur la Protection des Données » (RGPD), ou en anglais « General Data Protection Régulation » (GDPR).

Un projet de loi, déclaré d'urgence, est en cours d'élaboration pour assurer l'adaptation de la législation nationale. Partant du principe selon lequel « *un règlement directement applicable ne se recopie pas* », le projet de loi renvoie implicitement aux dispositions essentielles du RGPD.
La CNIL regrette le retard pris dans la préparation de ce projet de loi. Elle appelle, de toute urgence, à l'adoption de l'ordonnance prévue pour la réécriture du droit français de la protection des données afin de rendre le nouveau cadre juridique plus lisible pour les professionnels et les citoyens (avis de la CNIL du 30 novembre 2017 publié 13 décembre 2017).

La présente circulaire a pour objet d'indiquer les principales nouveautés du RGPD.

Nous reviendrons vers vous lors de la publication de la loi réformant la loi de 1978.
Un article de fond relatif à l'impact de la réforme sur les métiers de l'immobilier par une avocate spécialiste en la matière sera prochainement publié dans la revue Administrer.

Entrée en vigueur du RGPD : 25 mai 2018

Objectifs et Objet du RGPD (art.1 et 2)

➢ Objectifs

- **Le choix d'un instrument juridique fort : le Règlement**

Alors qu'une directive impose une transposition dans les Etats européens pour être effective ; un règlement fait directement office de loi.

Cependant, le règlement n'impose pas aux Etats d'abroger leurs législations nationales (en cas de dispositions divergentes le RGDP primera).

Le RGPD répond à plusieurs objectifs :

- **Protéger les individus** contre les nouveaux risques en renforçant les droits des personnes (vie privée, cybersécurité…) ;
- **Responsabiliser davantage l'ensemble des acteurs** qui traitent des données personnelles. Le RGPD **en supprimant le contrôle a priori,** et en le **remplaçant par un contrôle a posteriori**, les entreprises doivent **pouvoir à chaque instant démontrer leur conformité**
- Mettre en place de **véritables sanctions dissuasives** ;
- Mettre en place d'une **coopération plus forte entre les « CNIL » européennes**.

➢ Objet

Le règlement établit des règles relatives à la **protection des personnes physiques à l'égard du traitement des données à caractère personnel** et des règles relatives à la libre circulation de ces données.

Le règlement s'applique au **traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.**

Définition d'une donnée à caractère personnel (art.4 RGPD)

L'article 4 définit ainsi les données à caractère personnel :

*« toute information se rapportant à une **personne physique identifiée ou identifiable** (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique **qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne,** ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale « .*

Tous les métiers de l'immobilier sont impactés.

Champ d'application territorial (art. 3 RGDP)

Toutes les organisations (quelle que soit leur forme sociale) **qui sont situées sur le territoire de l'Union européenne sont soumises au RGPD pour le traitement des données personnelles liées à leur activité** (que le traitement ait lieu ou non dans l'Union).

Entrée en vigueur le 25 mai 2018 et sanctions

Le RGDP entre en vigueur le **25 mai 2018.**

A compter de cette date, à défaut de pouvoir démontrer leur conformité, les organisations encourent une amende administrative pouvant atteindre jusqu'à **20 millions d'euros** ou **4 % du chiffre d'affaires mondial total de l'exercice précédent** (le plus élevé des deux plafonds étant retenu).

Les principales nouvelles obligations du RGPD

➢ 1) Limiter les finalités et Minimiser les données personnelles collectées : « ne collecter que les données strictement nécessaire » (article 5 RGDP)

Le règlement impose de **ne collecter que les données strictement nécessaires**.

L'article 5 précise que :

« Les données à caractère personnel doivent être (…)
*b) collectées pour des **finalités déterminées, explicites et légitimes,** et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (…)*
***c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées** (minimisation des données) (…)*

Il s'agit d'une évolution importante de la règlementation par rapport au texte ancien, qui prévoyait simplement que les données ne soient pas excessives.

➢ 2) S'assurer du consentement des personnes à l'égard du traitement de leurs données (art. 7 RGDP)

Une personne doit matériellement consentir à ce que ses données puissent être traitées pour être dans la légalité.

Le consentement est défini par le règlement de la manière suivante (art. 4) :

« «Consentement» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une ***déclaration*** *ou par un* ***acte positif clair****,* ***que des données à caractère personnel la concernant fassent l'objet d'un traitement; (…)*** *»*

L'article 7 définit les **modalités du consentement :**

1. *« Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.*
2. *Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.*
3. *La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.*
4. *Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat. »*

➢ 3) Mettre en œuvre la portabilité des données (art. 20 RGDP)

Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle.

➢ 4) Assurer la sécurité des données personnelles (art. 32 RGDP)

La sécurité des données est un principe essentiel énoncé par l'article 5 f du RGPD :
« Les données à caractère personnel doivent être (…)
f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité); (..) »

L'obligation est définie par l'article 32 qui prévoit que :

1. « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.
3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.
4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre. »

Une étude de risque doit être entreprise, de laquelle doivent ressortir les mesures appropriées aux besoins. Le texte n'entre pas dans le détail technique des mesures devant être mises en œuvre.

➢ 5) Notifier à la CNIL la survenance d'une violation des données engendrant « *un risque pour les droits et libertés des personnes physiques* » (art. 33 et 34 du RGDP)

La notion de violation de données personnelles est définie à l'article 4 :

1. Une obligation de notification à la CNIL dans un délai de 72 heures

En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à la CNIL, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Contenu de la notification à la CNIL

La notification doit, à tout le moins:

a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

1. Obligation de notification à la personne concernée

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. Tenir un registre à cet effet

Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier.

La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

➢ 6) Une gestion spécifique des données sensibles (art. 35 RGDP)

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, **une analyse de l'impact** des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

➢ 7) Délégué à la Protection des Données (DPO), dans certains cas (Chapitre IV – article 27 à 43 du RGPD) art.37 RGPD)

1. Le DPO est obligatoire dans certains cas :

Le RGDP instaure la nomination obligatoire d'un délégué à la protection des données :

- Pour les entreprises du secteur public,

- Pour les entreprises dont l'activité principale conduit à assurer un suivi systématique et à grande échelle des personnes,

- Pour les entreprises dont l'activité principale est attenante à des traitements à grande échelle de données sensibles (politiques, religieuses, ethniques, biométriques, sanitaires, judiciaires, etc.) ou relative à des condamnations pénales et certaines infractions.

Le règlement ne donne pas de définition précise de la notion de « *grande échelle* », il faut tenir compte du nombre de personnes concernées, du volume de données traitées, de la durée du traitement et de son étendue géographique.

Le DPO aura notamment comme prérogatives :
De superviser la mise en œuvre et le suivi des initiatives de mise en conformité GDPR
D'informer l'organisation et le personnel de leurs obligations en matière de gestion des données personnelles
D'être le point de contact et de centralisation de toutes les demandes d'application des droits des personnes (droit à l'oubli, droit d'accès, droit à la portabilité, demande de modification, etc.)
De coopérer avec l'autorité de contrôle
De participer à l'élaboration des analyses d'impacts, obligatoires pour certains types de traitements (profiling, données sensibles, etc.)

2. A défaut, un ou des responsables du traitement des données pourront être désignés.

En dehors des hypothèses où la création d'un poste de DPO est obligatoire, il conviendra simplement et pragmatiquement de désigner un ou plusieurs responsables du traitement.

L'article 4 du RGPD définit ainsi le responsable du traitement : *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. »*

➢ 8) Constituer et tenir à jour un registre de conformité (art.30 RGDP)

3. Un outil obligatoire pour l'entreprise de plus de 250 salariés

Le registre est obligatoire pour les entreprises comptant plus de 250 salariés, ou bien lorsqu'elles réalisent des traitements réguliers susceptibles de comporter un risque pour les droits et libertés des personnes concernées (art. 30.5).

Le registre est un outil qui permet de démontrer le respect du RGPD, et pour le responsable du traitement de justifier qu'il « met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement », comme l'y oblige l'article 24.

Dans ces conditions, cet outil est conseillé y compris pour les entreprises comptant moins de 250 salariés. Dans tous les cas, il convient de lister les traitements mis en œuvre et d'assurer le suivi de l'évolution de leur conformité à minima.

4. Contenu du registre

Le registre comporte toutes les informations suivantes :

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 (voir paraphe 6 ci-dessus).