« Toulouse Capitole Publications » est l'archive institutionnelle de l'Université Toulouse 1 Capitole.

LES PROFESSIONNELS DE L'IMMOBILIER CONFRONTÉS À LA NOUVELLE RÉGLEMENTATION DE LA PROTECTION DES DONNÉES PERSONNELLES

ALEXANDRA MENDOZA-CAMINADE

Référence de publication : Dictionnaire permanent Gestion immobilière p1 2018-07-27

Pour toute question sur Toulouse Capitole Publications, contacter portail-publi@ut-capitole.fr

LES PROFESSIONNELS DE L'IMMOBILIER CONFRONTÉS À LA NOUVELLE RÉGLEMENTATION DE LA PROTECTION DES DONNÉES PERSONNELLES

Les administrateurs de biens, syndics et agents immobiliers par leurs activités sont détenteurs de données qui touchent à la vie privée, en conséquence ils doivent désormais se conformer au règlement général européen sur la protection des données personnelles (RGPD) applicable depuis le 25 mai 2018.

Le règlement général sur la protection des données du 27 mai 2016, visé sous l'acronyme RGPD, issu du Parlement européen, vient d'entrer en vigueur 2 ans plus tard, le 25 mai 2018. Le délai de 2 ans devait permettre à tous les acteurs de se préparer à l'application de la nouvelle réglementation (Règl. (UE) 2016/679 du Parlement européen et du Conseil, 27 avril 2016, art. 99 : JOUE n° L 119, 4 mai). Pour permettre la mise en œuvre du règlement, la loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a été modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles (L. n° 2018-493, 20 juin 2018 : JO, 21 juin). Les professionnels de l'immobilier qui détiennent de multiples données à caractère personnel notamment sur les locataires, propriétaires, copropriétaires, acquéreurs mais aussi sur leurs collaborateurs ou sous-traitants sont tous concernés par ces textes et doivent intégrer la gouvernance des données personnelles au sein de leur politique générale et de leur fonctionnement au quotidien.
La loi du 20 juin précise que le gouvernement est autorisé à prendre dans un délai de 6 mois suivant la promulgation de la loi, une ordonnance pour procéder à la réécriture de l'ensemble de la loi Informatique et libertés dans un souci de clarté et d'intelligibilité (L. n° 2018-493, 20 juin 2018, art. 32). Le chantier législatif n'est donc pas encore totalement achevé.

Données personnelles à protéger : une nouvelle logique de responsabilisation

Si la protection des données personnelles vise à protéger la vie privée du citoyen, il s'agit par ce texte européen de mieux protéger les données au regard de l'évolution des usages numériques tout en facilitant leur libre circulation au sein du marché intérieur. Le texte veut susciter la confiance qui permettra à l'économie numérique de se développer (RGPD, art. 7). Le droit français était, jusque-là, régi sur cette question par la loi Informatique et libertés n° 78-17 du 6 janvier 1978 qui avait été modifiée à l'occasion de la transposition de la directive 95/46/CE du 24 octobre 1995. Largement pionnier en la matière, le droit interne n'avait été influencé qu'à la marge par la directive. Avec le RGPD, le cadre juridique en matière de protection des données personnelles est totalement réformé pour les 28 États membres.

Même si les professionnels de l'immobilier n'exercent pas à titre principal une activité de traitement des données, ils collectent et traitent cependant de nombreuses données personnelles. Quelle que soit leur qualité, agent immobilier, syndic (professionnel ou bénévole) de copropriété, administrateur de biens, promoteur immobilier ou encore notaire, tous sont conduits dans le cadre de leurs activités à traiter des données personnelles. Ces dernières concernent leurs propres collaborateurs et salariés, mais également des données des prestataires intervenant dans l'immeuble et autres mandataires ou clients selon les activités exercées. Ainsi, la gestion d'un immeuble implique la tenue de fichiers relatifs à la copropriété et aux copropriétaires, et des traitements de données personnelles concernant les salariés du syndicat. Plus largement, divers aspects de leur activité impliquent nécessairement le traitement de données à caractère personnel (relations avec les clients, les notaires, leurs salariés, voire leur communication publicitaire, etc.). A ce titre, les professionnels de l'immobilier confrontés à un nombre croissant de données à traiter doivent veiller à ce que les données personnelles soient utilisées en toute légalité au regard du nouveau dispositif du RGPD.

Les traitements réalisés au sein des entreprises ne sont pas les seules visés par le règlement. Les contrats passés par l'entreprise doivent aussi être examinés, tant à l'égard des clients, des prestataires que des sous-traitants. En effet, le RGPD renforce considérablement les informations dues à la personne concernée, ce qui implique de revoir les clauses des contrats afin de respecter la très longue liste de mentions désormais prévues (RGPD, art. 13 et 14). Il est aussi indispensable de revoir les contrats passés avec les sous-traitants puisqu'un contrat écrit est nécessaire et qu'il doit indiquer les nouvelles obligations mises à la charge du sous-traitant (u RGPD, art. 28). De la même manière, les entreprises dotées d'un site internet doivent adapter les mentions légales et les conditions mises en ligne, et veiller également à ce que la politique de gestion des cookies soit conforme au nouveau dispositif.

Le RGPD conforte les principes fondamentaux déjà consacrés par le droit européen et par la loi française Informatique et libertés du 6 janvier 1978. Toutefois, la philosophie du système est entièrement réformée au profit d'une logique de responsabilisation des acteurs, les responsables et leurs sous-traitants, afin notamment de réduire les formalités administratives. Le système des déclarations et autorisations préalables auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) qui permettait un contrôle a priori n'est plus : la logique administrative se voit remplacée par un contrôle a posteriori des entreprises. Ce contrôle est exercé par le régulateur national, à savoir en France par la CNIL. Les entreprises doivent pouvoir établir le respect du RGPD à tout moment du cycle de vie des données. Ainsi, faut-il prendre toutes les mesures nécessaires afin d'être en conformité avec le RGPD et être en mesure de le prouver en

cas de contrôle, car les manquements aux obligations légales peuvent aboutir à des sanctions très lourdes (v. in fine « Sanctions renforcées de la CNIL »).
Par ce changement d'approche, la protection des données personnelles doit être intégrée dès la phase de conception de tout service ou de tout produit traitant de données personnelles : il faut prévoir la protection de la vie privée dès la conception (concept du « privacy by design »). Les acteurs ont des responsabilités plus lourdes et leurs obligations sont renforcées (v. ci-dessous « Renforcer l'obligation d'information et de transparence à l'égard des personnes concernées »). Parallèlement, la protection des personnes concernées est plus importante.

A quel titre les professionnels de l'immobilier sont-ils soumis au dispositif du RGPD ?

Les responsables de traitement, mais aussi désormais leurs sous-traitants, sont visés par le RGPD dans un souci de responsabiliser l'ensemble des acteurs impliqués dans le processus. La nouvelle réglementation s'impose à toute entreprise, quelle que soit sa forme, sa nature, son activité économique, lucrative ou non, exercée ou non sur internet (RGPD, art. 4, 18). En effet, est visée toute « personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique ». Par conséquent, l'ensemble des professionnels du secteur immobilier sont touchés par la réglementation, y compris le syndic de copropriété qui exerce à titre bénévole.

Mise en place d'un responsable du traitement des données personnelles

Dans le cadre de la gouvernance des données personnelles, le responsable de traitement est la personne qui détermine les finalités et les moyens du traitement (RGPD, art. 4, 7). Ce dernier doit alors mettre en œuvre les mesures appropriées pour garantir « un niveau de sécurité adapté au risque » (RGPD, art. 24 et s. et art. 27 et s.), et être en conformité avec les obligations nouvelles découlant du règlement. L'autonomie dont dispose l'entreprise dans la mise en œuvre des traitements, qu'il s'agisse de leur finalité ou de leurs modalités de mise en œuvre, suffit à conférer la qualité de responsable de traitement. Cela sera alors le cas du syndic qui bénéficie de cette autonomie en matière de traitements alors qu'il agit pour le compte du syndicat des copropriétaires.

L'entreprise qui agit sur instruction d'une autre personne, par exemple un prestataire agissant sur ordre d'un syndic ou encore une entreprise de gestion des salaires, aura la qualité de sous-traitant. La responsabilité du sous-traitant peut être engagée en cas de manquements dans les mêmes conditions que celle d'un responsable de traitement, s'il n'a pas respecté ses obligations ou s'il a agi « en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci » (RGPD, art. 82). En cas de contentieux, une « coresponsabilité » des deux acteurs

est possible. Il faudra donc que l'entreprise intègre dans son choix de sous-traitant la protection des données personnelles et s'assure que le sous-traitant choisi soit lui-même en conformité avec le RGPD.

Tenue d'un registre des traitements de données personnelles

Seules les entreprises de plus de 250 salariés ont l'obligation de tenir un registre des traitements de données personnelles (RGPD, art. 30). Cependant, celles de moins de 250 salariés sont aussi visées si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données, à savoir les données sensibles et les données relatives à des condamnations pénales. Pour les entreprises non visées par cette obligation, il faut préconiser la tenue d'un tel registre car il facilitera la mise en œuvre de la conformité et sa démonstration en cas de contrôle de la CNIL.
La tenue à jour d'un registre des traitements s'effectue sous la responsabilité du responsable de traitement, mais aussi du sous-traitant (v. ci-dessus). Le registre est tenu à disposition de la CNIL.
En cas de risques spéciaux pour les droits et libertés des personnes, une analyse d'impact des traitements envisagés est nécessaire afin de faire apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Cela concernera notamment les traitements portant sur des données sensibles (RGPD, art. 35).

Nomination d'un délégué à la protection des données

Le délégué à la protection des données [DPD ou DPO (data protection officer)] remplace le correspondant Informatique et Libertés (CIL) jusqu'alors facultatif. Les entreprises sont encouragées à en désigner un, car il représente le point de contact avec l'autorité de contrôle (RGPD, art. 39) et les personnes concernées. Il est toutefois obligatoire dans plusieurs cas : notamment lorsque les activités de base consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou lorsque les activités de base consistent en un traitement à grande échelle de catégories particulières de données (RGPD, art. 37, 1). Ses missions élargies visent l'information, le conseil ainsi que le contrôle des obligations en vigueur. Pour les assurer, il doit « disposer des moyens matériels et organisationnels ». Le DPD peut être un salarié de l'entreprise, ou une personne extérieure, et une mutualisation du DPD est permise (ex : à l'échelle d'un syndic), ce qui peut constituer une solution pertinente à un moindre coût.

Remarque : en cas de manquement aux obligations par le responsable de traitement ou le sous-traitant, l'action de groupe peut être « exercée en vue soit de faire cesser le manquement », « soit d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis, soit de ces deux fins » (L. n° 78-17, 6 janv. 1978, art. 43 ter, mod. par L. n° 2018-493, 20 juin 2018, art. 25).

Inventorier les données à caractère personnel

Les données à caractère personnel sont définies comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Une personne physique identifiable est 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 (RGPD, art. 4, 1). Notamment les professionnels de l'immobilier disposent de multiples données personnelles à protéger (par exemple : noms, date de naissance, numéros de sécurité sociale, adresses, mails, numéros de téléphone, coordonnées bancaires, éventuellement vidéos de surveillance des parties communes, codes d'accès).

Recensement du traitement des données personnelles

Dans le cadre de la responsabilisation prônée par la réforme, chaque acteur de l'immobilier doit procéder au recensement des fichiers de données qu'il détient et de la manière dont les données ont été collectées. Quelles personnes, quels services utilisent des données personnelles ? Après avoir déterminé qui les traite, il faut déterminer à quoi elles servent. S'agit-il de répondre à une obligation légale ? De permettre un suivi administratif, contractuel ? De manière concrète, un état des lieux doit permettre au responsable de dresser une cartographie des traitements qu'il détient car il lui faudra à l'avenir être en capacité de réaliser un inventaire permanent des traitements. Cette cartographie permettra d'établir un registre des fichiers (RGPD, art. 30, v. " Tenue d'un registre des traitements des données ") et de s'interroger ensuite sur la conformité de ces fichiers au dispositif légal. En cas de points défaillants, des actions doivent être engagées afin d'y remédier et de limiter tout risque pour la vie privée. En conséquence, l'entreprise devra mettre en place des outils techniques et organisationnels pour protéger et prévenir toute atteinte aux données personnelles et pour prouver sa conformité au RGPD. Ce nouveau système de contrôle a posteriori de la CNIL se substitue à l'ancien contrôle a priori des formalités déclaratives auprès de la CNIL.
Les principaux points de vigilance : parmi les exigences concernant le traitement figurent la licéité, la loyauté et la transparence (RGPD, art. 5) ; ces principes étaient déjà requis par le

dispositif antérieur. Aussi, les entreprises qui étaient en conformité n'auront pas un travail d'adaptation considérable à fournir afin de satisfaire le respect de ces principes. L'utilisation de données personnelles implique pour l'entreprise de pouvoir établir la licéité du traitement par le recueil du consentement de la personne concernée, ou par d'autres justifications que sont l'exécution d'un contrat auquel est partie la personne, le respect d'une obligation légale, la sauvegarde d'intérêts vitaux de la personne concernée, l'exécution d'une mission de service public et les intérêts légitimes poursuivis par le responsable du traitement (RGPD, art. 6).

Renforcer l'obligation d'information et de transparence à l'égard des personnes concernées

On assiste à la fois à un renforcement des droits des personnes concernées par les traitements de leurs données personnelles et à la consécration de nouveaux droits. Le responsable du traitement doit pouvoir établir que les données collectées sont nécessaires au regard des finalités pour lesquelles elles sont traitées. S'il était jusque-là exigé que les données collectées ne soient pas excessives par rapport à la finalité du traitement, il faut désormais que les professionnels ne collectent et ne traitent que de données nécessaires à leur activité, ce qui implique une étroite adéquation des données à la finalité recherchée.

Droit d'accès et de rectification des données personnelles par les personnes concernées

Chaque fois que des données personnelles sont collectées, le support utilisé doit comporter des mentions d'informations. Le recueil du consentement « explicite et positif » (RGPD, art. 4, 11) doit pouvoir être prouvé par le responsable de traitement (RGPD, art. 7). Il faut rappeler que la personne physique dispose d'un droit d'information, de consentement mais aussi d'opposition et qu'elle doit pouvoir accéder sans frais à ses données, en demander la rectification ou l'effacement. Le droit à l'effacement des données est consacré par le RGPD (art. 5).

Remarque : la Cour de justice de l'Union européenne (CJUE) avait dégagé le principe du droit à l'effacement des données à partir de la directive 95/46/CE du 24 octobre 1995 dans l'affaire Google Spain en reconnaissant un droit au déréférencement d'un citoyen espagnol auprès du moteur de recherche (CJUE 13 mai 2014, aff. C-131/12). Ce droit à l'oubli fait partie des nouveaux droits des personnes physiques sur leurs données personnelles dont la conservation est possible « (…) pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Il faut donc veiller à mettre en œuvre une politique de conservation des données respectueuse de ce droit. Pour cela, les normes simplifiées édictées par la CNIL fournissent aux responsables de traitement des informations sur les durées.

Droit à la portabilité des données personnelles

Parmi les importantes nouveautés figure, par ailleurs, le droit à la portabilité des données. Cela implique le droit pour toute personne de réclamer ses données « dans un format structuré, couramment utilisé et lisible par machine » (RGPD, art. 20). Les professionnels de l'immobilier doivent être prêts pour mettre en œuvre cette portabilité des données personnelles de leurs clients, par exemple en cas de changement de syndic.

Sécurité et confidentialité des données personnelles

La sécurité des traitements doit être assurée par le responsable au nom du principe de « privacy by default » obligeant le responsable à garantir un niveau élevé de protection des traitements par défaut. Il doit mettre en place des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Il est pour cela possible d'utiliser des modalités pratiques pour garantir la sécurité informatique. En cas de violation des données, il faut alerter la CNIL dans les 72 heures (RGPD, art. 33 et 34). Il s'agit de réagir rapidement à une faille de sécurité présentant un risque pour les droits et libertés des personnes physiques qui doivent également être averties dans le meilleur délai.

Sécuriser les données dans un document de conformité

Les professionnels de l'immobilier doivent désormais se plier au principe de l'accountability, c'est-à-dire pouvoir établir leur conformité au RGPD, et être en capacité de produire une documentation attestant de cette démarche, des mesures prises et des actions mises en œuvre auprès de la CNIL. Pour les aider, la CNIL a publié un guide pratique pour l'application du RGPD disponible sur son site internet (www.cnil.fr/fr/un-nouveau-guide-de-la-sécurité-données-personnelles). A long terme, une fois les nouvelles contraintes intégrées, la réglementation profitera aux acteurs économiques : le RGPD est présenté comme une opportunité pour les entreprises qui doivent intégrer la gouvernance des données personnelles au sein de leur politique générale.

Sanctions renforcées de la CNIL

Les sanctions administratives ont été considérablement augmentées. Selon la catégorie de l'infraction au RGPD, il pourra s'agir d'une amende de 10 à 20 millions d'euros ou 2 % à 4 % du chiffre d'affaires annuel mondial (L. n° 78-17, 6 janv. 1978, art. 7, mod. par L. n° 2018-493, 20 juin 2018, art. 19). La CNIL se veut rassurante et elle a annoncé sa volonté d'accompagner les entreprises dans la mise en œuvre des nouvelles obligations du RGPD lors

des contrôles (droit à la portabilité, analyse d'impact sur la protection des données, tenue d'un registre de traitement, etc.). Elle maintiendra des vérifications rigoureuses pour les principes fondamentaux déjà inscrits dans la loi informatique et libertés.