POLITIQUE INTERNE DE PROTECTION DES DONNÉES

PREAMBULE

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, dite Loi Informatique et Libertés ainsi que le Règlement 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, dit Règlement Général sur la Protection des Données ou RGPD, , en vigueur depuis le 25 mai 2018, règlementent l'utilisation des informations relative à une personne physique en France.

Le règlement européen est venu renforcer la protection des données à caractère personnel et amène des changements structurants tant au niveau organisationnel, technique que juridique autour de la collecte et du traitement de ce type de données.

TOURS HABITAT, Office Public de l'Habitat, est directement impactée par cette législation.

Cette législation impose des obligations strictes pour le Dirigeant et les employés quant à la collecte et à l'utilisation qui pourra être fait des données relatives à une personne physique et donne des droits aux personnes concernées, personnes dont les données ont été collectées.

Soucieux du respect de la vie privée et de la protection des données personnelles, dans un souci de transparence, TOURS HABITAT a adopté une politique interne de protection des données à caractère personnel.

1. Définitions

Données à caractère personnel : toute information qui permet d'identifier une personne physique (ci-après dénommée « personne concernée »), directement ou indirectement.
Certaines données, dites sensibles, sont soumises à un principe d'interdiction de collecte (données relatives à la santé, à l'orientation sexuelle ou à la vie sexuelle, données génétiques ou biométriques, origines raciales ou ethniques, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, appréciation sur les difficultés sociales, données relatives à des infractions, condamnations et mesures de sûreté, numéro de sécurité sociale), lequel souffre d'exceptions.
Les données bancaires ne sont pas objectivement considérées comme « sensibles » au sens du RGPD mais doivent évidemment être manipulées avec précautions et conservées soigneusement.

Un traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre

forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Une finalité : objectif poursuivi par la mise en place du traitement.

Un fichier : tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

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.

Le Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte d'un responsable de traitement. Elle traite des données pour le compte d'un autre organisme et a, à ce titre, un devoir de conseil, d'assistance et de coopération avec l'organisme pour le compte duquel elle traite les données. A son égard, le sous-traitant a une obligation de transparence et de traçabilité ainsi qu'une obligation de garantir la sécurité des données traitées.

La Personne concernée : la personne concernée par un traitement de données est celle à laquelle se rapportent les données qui font l'objet du traitement. Il s'agit d'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.
Les personnes dites vulnérables sont celles qui sont dans l'incapacité de donner leur consentement et/ou s'opposer aisément au traitement de leurs données ou d'exercer leurs droits soit d'un point de vue légale, hiérarchique ou mental. Sont considérés comme vulnérables, les enfants (qui peuvent être vus comme incapables de s'opposer ou de consentir sciemment et de manière réfléchie au traitement de leurs données), les employés et les majeurs protégés.

Le Destinataire d'un traitement de données : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

Le Tiers autorisé : les organismes autorisés par une disposition législative ou réglementaire, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à obtenir d'un responsable de traitement la communication de données à caractère personnel.

Le Référent à la Protection des données ou « RPD », anciennement « RIL » : personne physique désignée comme interlocuteur privilégié auprès du Délégué à la Protection des données. Une personne désignée comme Référent dispose des compétences minimales requises dans la compréhension des principes Informatique et Libertés et RGPD.

Le Délégué à la Protection des Données ou « DPO » : personne physique désignée par lettre de mission et chargée de mettre en œuvre des traitements de données à caractère personnel et de veiller de manière indépendante au respect de la loi Informatique et Libertés et du RGPD.

La Commission Nationale de l'Informatique et des Libertés ou « CNIL » : autorité administrative indépendante chargée de l'application de la réglementation et du contrôle des organismes.

Le Registre de traitements *: document que doit tenir chaque responsable de traitement. Il s'agit d'un document de recensement et d'analyse qui doit refléter la réalité des traitements de données à caractère personnel et permettre d'avoir une vue d'ensemble des activités de traitement.*

Une durée de conservation : les données personnelles ne peuvent être conservées de façon indéfinie dans les fichiers informatiques ou papiers. Une durée de conservation doit donc être déterminée en fonction de l'objectif ayant mené à la collecte. Il est interdit de conserver ad vitam aeternam des données personnelles.

2. Les principes de la Protection des données

Il faut que trois conditions soient remplies pour que les règles relatives à la protection des données s'appliquent :

- *Présence d'informations concernant une personne telle que Nom, Adresse, Date de naissance, Matricule, Numéro de téléphone, Identifiant, etc.*
- *Traitement de ces informations tel que la collecte, l'utilisation, l'enregistrement, etc.*
- *Traitement figurant dans des fichiers informatiques (Base de données, Tableau Excel, etc.) ou classeurs papiers.*

Les principes de la Protection des données sont les suivants :

- *Finalité déterminée : les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage défini avant la collecte. La collecte de données à caractère personnel ne peut jamais être une fin en soi ; la collecte et le traitement doivent se faire dans un but précis. On ne peut plus se livrer à une collecte de données « au cas où » ; cela répond au principe de prévisibilité ;*

- *Finalité explicitée : les finalités sont compréhensibles par tous et portées à la connaissance des personnes concernées ; le libellé de la finalité doit être clair et précis ; cela répond au principe de transparence ;*
- *Finalité légitime : l'intérêt du responsable de traitement ne doit pas aller à l'encontre de celui de la personne concernée. Les finalités du traitement ne doivent pas aller à l'encontre de la loi ni des droits et libertés fondamentales des personnes. La finalité de traitement doit reposer sur l'une des cinq bases légales : intérêt légitime, consentement, obligation légale, intérêt vital ou intérêt public ; cela répond au principe de sécurité juridique ;*
- *Minimisation des données : les données collectées doivent être nécessaires à la bonne marche du traitement. De manière générale, elles doivent être proportionnelles à la finalité que poursuit le traitement. Seules les données nécessaires, utiles, adéquates et pertinentes peuvent être collectées et traitées. Lorsqu'on collecte des données personnelles, il est important de se poser la question suivante : ces données sont-elles utiles et nécessaires pour le traitement que je souhaite mettre en place ? Pourquoi je collecte ces données ? Les réponses : « on a toujours fait comme ça » ne suffisent plus !*
- *Durée de conservation limitée : les informations ne peuvent être conservées au-delà de la réalisation de la finalité ou au-delà de la durée légale ; dans tous les cas, si on conserve les données au-delà, il faut pouvoir être en mesure de justifier les raisons qui nous poussent à conserver plus longtemps ; des réponses comme « on ne sait jamais » ou « au cas où » ne suffiront pas devant la CNIL ;*
- *Accès restreint aux données : les données doivent être traitées d'une manière confidentielle et doivent uniquement être divulguées aux personnes habilitées à en prendre connaissance dans le cadre de leurs missions ;*
- *Sécurité physique et logique : le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ;*
- *Obligation d'information : les personnes doivent être informées de l'existence d'une collecte de données les concernant ;*
- *Droit des personnes : les personnes disposent de droits sur leurs données dont elles doivent être informés et qu'elles peuvent exercer quand bon leur semble, à la seule condition de pouvoir justifier de leur identité à l'appui de leur demande ;*
- *Transfert de données hors Union Européenne : par principe, tout transfert de données en dehors de l'Union Européenne est interdit.*

I. OBJET DE LA PRÉSENTE POLITIQUE

La présente procédure a pour objet de définir et garantir les rôles et responsabilités de chacun des acteurs impliqués dans la mise en œuvre de traitements ainsi que les grands principes de protection des données applicables.

Cette procédure a pour objectif d'assurer le développement de TOURS HABITAT dans le respect de la réglementation relative à la protection des données à caractère personnel.

II. PÉRIMÈTRE

Cette procédure s'applique à tout collaborateur de TOURS HABITAT (salarié, intérimaire, stagiaire, apprenti, CDD, collaborateur externe et occasionnel, prestataire, etc.) ainsi qu'à toute personne, physique ou morale, qui serait amenée à traiter des données à caractère personnel pour le compte de TOURS HABITAT.

La procédure a été validée en Comité de Direction exceptionnel le 3 avril 2019 et a fait l'objet d'une information lors de la séance du Comité Social et Economique du 23 avril 2019. La procédure sera annexée au Règlement Intérieur du personnel de TOURS HABITAT. La procédure a été diffusée auprès de tous les collaborateurs de TOURS HABITAT, après validation par le Délégué à la Protection des Données (DPO). Elle est transmise de manière dématérialisée au personnel disposant de l'outil informatique et sous format papier pour le personnel de proximité (agents de maintenance et surveillants d'immeubles notamment).

III. LES RÔLES ET MISSIONS DE CHACUN DES ACTEURS DE TOURS HABITAT

- **Collaborateur de TOURS HABITAT**

Tout collaborateur a pour mission de permettre et de faciliter le travail du DPO. Il tiendra à disposition de celui-ci, toute information nécessaire dans le cadre de ses missions.

Chaque collaborateur de TOURS HABITAT s'engage à faire son maximum au quotidien pour respecter les données personnelles qu'il pourrait être amené à collecter et traiter dans le cadre de ses missions. Il s'engage à préserver la sécurité de ces données, en veillant notamment à ranger sous clé tout document contenant des données personnelles ou tout document confidentiel. Il pourra pour cela se référer au **Référentiel « La protection des données personnelles au quotidien » (Annexe 1)**.

Pour rappel, lorsqu'une personne nous communique de son propre chef des données dites « sensibles » que ce soit par courrier ou à l'oral, cela ne signifie pas pour autant que nous sommes autorisés à les collecter et à les traiter, nous

devons préalablement obtenir de la personne son consentement écrit ; communiquer certaines données sensibles ne veut pas dire donner l'autorisation à TOURS HABITAT de collecter, traiter ou utiliser les données.

Chaque collaborateur assurera la confidentialité de toutes les informations personnelles concernant les clients de TOURS HABITAT qu'il serait amené à collecter et traiter dans le cadre de ses missions.

Afin de permettre à TOURS HABITAT de garantir la conformité de son activité, l'attention quotidienne et la rigueur de chaque collaborateur est exigée lors de la collecte et l'utilisation de données personnelles, que ces dernières soient informatisées ou manuelles (papier). Pour cela, les règles d'or suivantes sont à respecter :

1. *N'enregistrer que les informations pertinentes, objectives et en relation avec l'objet du traitement ;*
2. *Ne pas collecter d'informations faisant apparaître directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de la personne ;*
3. *Ne pas collecter le NIR ou Numéro de Sécurité Social ni des informations relatives à des infractions, condamnations, mesures de sûreté, subjectives, sauf autorisation légale ou intérêts légitimes ;*
4. *Ne pas collecter des informations qui du fait de leur nature, de leur portée ou de leurs finalités, excluent des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, en l'absence de toute disposition législative ou réglementaire ;*
5. *Bloquer votre poste en cas d'absence. Rangez les dossiers dans les meubles fermant à clé en fin de journée ; ne laisser aucun document contenant des données personnelles ou confidentielles sur votre bureau sans surveillance ;*
6. *Informer le service informatique en cas de constat d'une faille de sécurité et ce, au moindre doute ;*
7. *Informer le Référent de toute mise à jour ultérieure d'un traitement, ajout d'un traitement, arrêt ou suppression d'un traitement ou de tout nouveau projet. Ce dernier en informera le DPO. Le RGPD a rendu obligatoire la mise en œuvre d'une étude d'impacts en cas de nouveau projet et sous certaines conditions.*

En cas de question ou de doute, s'adresser au Référent désigné au sein de TOURS HABITAT

En cas de non-conformité relative à la loi Informatique et Libertés, la responsabilité d'un collaborateur ne pourra être engagée. Néanmoins, le collaborateur en cause pourra faire l'objet d'une sanction disciplinaire.

- **Référent à la Protection des Données**

Un Référent est désigné au sein de TOURS HABITAT. Le Référent doit avoir une bonne connaissance de la législation sur la protection des données personnelles et avoir reçu une formation sur cette thématique. Le DPO dispose de l'identité, de la fonction et des coordonnées du Référent en place au sein de TOURS HABITAT et les met à jour si nécessaire (départ du Référent, nouveau Référent désigné, etc.).

Le Référent assistera le DPO au quotidien et l'aidera à maintenir et mettre à jour la cartographie des traitements ainsi que le registre de manière générale. Il a une culture *« protection des données personnelles »* et est sensibilisé aux problématiques et principes Informatique et Libertés. Il assure un rôle d'alerte auprès du DPO en cas de constat d'un manquement à la loi Informatique et Libertés et au RGPD. Il est chargé de diffuser au sein de l'entreprise la culture *« protection des données personnelles »* et les bonnes pratiques en ce domaine. Il est le lien entre le DPO et les collaborateurs de TOURS HABITAT. Il est le relais du DPO au sein des différentes directions de l'organisme. Il doit maintenir de manière opérationnelle la conformité RGPD au sein de TOURS HABITAT et reporter au DPO les éventuelles évolutions et incidents. Il accompagne et conseille les collaborateurs dans les thématiques de protection des données.

Il a pour rôle de coordonner les acteurs et de susciter l'adhésion des différents collaborateurs. Il contribue à la conformité RGPD dans l'ensemble des directions.

En cas de non-conformité relative à la réglementation sur la protection des données personnelles, la responsabilité du Référent ne pourra être engagée.

- **Relais métiers par Direction ou Service**

Le Référent à la Protection des Données doit pouvoir s'appuyer sur un réseau de Référents opérationnels, sachant sur des domaines techniques.
Ainsi, dans chaque direction et, le cas échéant, dans certains services, un interlocuteur sera nommé pour assister le Référent ; étant précisé que le DPO n'aura qu'un seul et unique correspondant en interne : le Référent et son suppléant en cas d'absence de ce dernier.

- **Responsable de Traitement**

Le Responsable de traitement est le représentant légal de l'organisme, sauf cas de délégation de pouvoir.

Le Responsable de traitement ou son représentant s'engage à rencontrer le DPO dans le cadre de ses activités afin d'évaluer ses attentes et besoins, prendre connaissance des éventuelles difficultés rencontrées, analyser et anticiper les projets à venir.

Le Responsable de traitement s'engage à respecter les termes de la lettre de mission signée avec le DPO.

Notamment, il s'assure que les compétences du DPO sont régulièrement entretenues et que celui-ci bénéficie d'un budget annuel dédié et de moyens lui permettant d'assurer ses missions (temps consacré à la mission, moyens humains, outils dédiés, etc.).

Le responsable de traitement est juridiquement responsable de tout manquement à la réglementation sur la protection des données personnelles qui pourrait être constaté au sein de son organisme. La désignation d'un DPO n'entraîne aucune exonération de responsabilité civile, administrative ou pénale pour le responsable de traitement. Il ne peut sanctionner le DPO du fait de l'accomplissement de ses missions.

Le Responsable de traitement est le Directeur Général de TOURS HABITAT ou tout autre directeur ou responsable de service qui aurait reçu de lui délégation de compétence.

Pour mémoire, la CNIL dispose d'un pouvoir de sanction et de contrôle étendu.

- ✓ *Amendes administratives : jusqu'à 10 à 20 millions d'euros selon le niveau de gravité du manquement constaté (ou 2 à 4 % du Chiffres d'Affaires annuel).*
- ✓ *Sanctions pénales : jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amendes.*
- ✓ *Dommages-intérêts à verser aux personnes physiques victimes qui porteraient plainte.*
- ✓ *Atteinte à l'image et à la réputation en cas de publication des sanctions, perte de confiance des clients.*

➢ Délégué à la Protection des Données (dit DPO)

Le DPO est directement rattaché au Responsable de Traitement et ne reçoit aucune instruction pour l'exercice de ses missions de DPO. Il agit en toute indépendance.

Les missions du DPO sont précisées dans la lettre de missions signée entre le DPO et le Responsable de traitement.

Notamment, le DPO réalisera chaque année des actions d'information, de formation et de sensibilisation avec une forme et une fréquence adaptées au contexte (telles que la tenue de formations, la diffusion de bonnes pratiques, la réalisation de supports de communication, le rappel des consignes, la création d'outils pédagogiques et méthodologiques). Il appartient au DPO de définir la forme et la fréquence adaptée et d'en tenir informé le responsable de traitements.

Le DPO pourra participer à toute formation relative à la protection des données qu'il jugera nécessaire, notamment les formations dispensées par la CNIL ainsi qu'à toute action permettant l'entretien et l'amélioration de ses compétences.

Le DPO actuellement désigné de manière étendue pour le compte de la TOURS HABITAT est la société d'avocats GRANT THORNTON, immatriculée au RCS de NANTERRE sous le numéro 632 013 843, dont le siège social se situe 29 rue du Pont

92200 NEUILLY SUR SEINE et représenté par Madame Anne FREDE. La personne chargée de la désignation étant Monsieur Nicolas RÉMY-NÉRIS.

Il s'agit d'un DPO mutualisé et externe. Il est chargé d'accompagner la mise en œuvre de la conformité vis-à-vis du RGPD au sein de TOURS HABITAT.

La désignation d'un DPO n'entraîne aucun transfert de responsabilité. Pour autant, il existe des situations dans lesquelles le DPO peut, malgré tout, voir sa responsabilité pénale engagée. Ainsi, la responsabilité pénale du DPO devrait pouvoir être retenue s'il enfreint intentionnellement la réglementation relative à la protection des données personnelles ou s'il aide le responsable des traitements à violer la loi.

IV. LA CARTOGRAPHIE DES TRAITEMENTS

Le DPO accompagné du Référent réalisent notamment une cartographie de l'ensemble des traitements mis en œuvre par TOURS HABITAT et la mettent à jour pour tout nouveau traitement.

Les collaborateurs, le Référent, les interlocuteurs ainsi que le responsable de traitement devront mettre le DPO en mesure d'assurer cette cartographie, notamment en remontant par l'intermédiaire du Référent, toute information concernant ce traitement dont ils auraient connaissance.

La cartographie attendue comprend notamment pour chaque traitement :

- le nom (dénomination) et l'adresse du responsable du traitement ;
- la ou les finalités de traitement ;
- le ou les services chargés de sa mise en œuvre ;
- la fonction de la personne ou le service auprès duquel s'exercent les droits des personnes ainsi que leurs coordonnées ;
- les modalités d'information et d'exercice des droits des personnes ;
- une description des catégories de données traitées et de l'origine de leur collecte ;
- les catégories et une estimation du nombre de personnes concernées par le traitement ;
- les destinataires ou catégories de destinataires habilités à recevoir communication des données ;
- la ou les durées de conservation des données traitées ;
- le régime juridique applicable et, le cas échéant, la date de dépôt des formalités ainsi que la décision datée de la CNIL (pour les traitements relevant des demandes d'autorisation ou d'avis, le DPO procède à l'accomplissement des formalités nécessaires auprès de la CNIL) ;
- les dispositions prises pour assurer la sécurité des données ;
- l'existence ou non d'un transfert hors Union Européenne et le cas échéant : la finalité du transfert, les catégories de personnes concernées, la nature des données transférées, les catégories de destinataires du transfert (filiale, prestataire, etc.), la nature des traitements opérés chez le destinataire, le pays d'établissement et la garantie permettant d'encadrer le transfert (telle que les BCR, clauses contractuelles types et Safe Harbor) ;

- l'existence ou non de la sous-traitance d'une activité (avec mention de l'existence et de la date de signature du contrat de sous-traitance comportant une clause Informatique et Libertés) ;
- un niveau de vraisemblance et de gravité pour l'ensemble des risques liés au traitement ;
- la date et l'objet des mises à jour ;
- les modalités de recueil du consentement lorsque nécessaire ;
- l'utilisation de cookies le cas échéant.

V. LE PILOTAGE DE LA MISE EN CONFORMITÉ

On entend le terme *« projet »* comme n'importe quelle tâche ou opportunité impliquant un traitement de données personnelles. Chaque Relais du Référent devra compléter le tableau dénommé « Fiche Projet » **(Annexe 2)** afin que le Référent soit informé des différents projets en cours au sein de TOURS HABITAT ; ceci permettra d'actualiser le registre de traitement ou de procéder à une analyse d'impacts.

Le responsable de traitement s'assure que le pilotage de la mise en conformité est réalisé par le DPO grâce à :

- la définition des circuits de validation pour l'ensemble des activités liées à la protection des données et l'intégration du DPO dans ces circuits. Dès l'initialisation du projet, le DPO sera consulté par le porteur du projet (Responsable de traitement, Référent, collaborateur, etc.). Aucun nouveau traitement ou activité ne pourra être mis en place avant consultation préalable du DPO.
- la mise en place d'outils de pilotage (réalisation d'un bilan annuel d'activités, suivi des activités) ;
- la nomination d'un Référent comme interlocuteur du DPO pour chaque traitement et l'établissement d'un réseau d'interlocuteurs, a minima, par direction pour assister le Référent. Le Référent pourra demander à tout autre collaborateur d'intervenir lorsque celui-ci dispose d'une connaissance d'éléments supplémentaires concernant le traitement ;
- la consultation du DPO dès l'initialisation d'un projet impliquant un traitement de données personnelles et à chaque fois qu'il le juge utile, dans le but d'introduire le respect de la protection des données dès la conception du projet.

Le responsable des traitements est tenu d'assurer la confidentialité, la sécurité, l'intégrité et la disponibilité des données objet du traitement. Dans ce cadre, le DPO devra, pour tout nouveau traitement, procéder ou faire procéder à une analyse de risques et d'impacts permettant l'identification et l'analyse des principaux risques liés à la sécurité des données à caractère personnel que les traitements font peser sur les libertés et la vie privée des personnes concernées. Cette démarche permet notamment d'estimer chaque risque en termes de vraisemblance et de gravité. Ces études permettront également la détermination des mesures de sécurité mises en œuvre et l'évaluation de leur pertinence vis-à-vis des risques ainsi appréciés.

Le DPO devra toujours disposer d'une copie de l'analyse des risques lui permettant de faire part de ses observations au Responsable de traitement avant la mise en œuvre du projet.

VI. CONFORMITÉ DANS LE TEMPS

En tant que garant de la mise en conformité de l'ensemble des traitements effectués par TOURS HABITAT, le DPO s'engage à contrôler la bonne conformité des traitements mis en œuvre par l'organisme.

Le délégué est consulté pour toute analyse d'impact et en vérifie son exécution. Le délégué peut dispenser des conseils au responsable du traitement. Il présente ensuite ses conclusions au Responsable de traitement qui doit consigner tout refus de suivi des actions préconisées. L'analyse des impacts précitée servira de base au DPO pour identifier les traitements de données particulièrement sensibles au sens de la loi.

Le DPO sera particulièrement attentif aux traitements sensibles identifiés grâce aux études de risques : il appartient alors au DPO de procéder à des audits interne ou externe périodiques pour s'assurer de la bonne conformité de ces traitements à la loi ainsi qu'au RGPD. Le DPO, s'il ne réalise pas lui-même l'audit, est toujours destinataire des résultats d'audit.

De plus, si une faille de sécurité intervient et qu'une mise à jour des études d'impacts est nécessaire, le DPO devra y procéder dans les meilleurs délais et non attendre le délai triennal de révision.

Dans le cas où le DPO observe l'irrégularité d'un traitement de données par rapport aux principes de protection des données personnelles, il doit proposer au responsable de traitement ou au Référent désigné un plan d'actions correctives permettant de mettre le dit traitement en conformité à la loi et au RGPD.

Le Responsable de traitement est tenu d'assurer au DPO les moyens de réaliser sa mission et s'engage à l'entendre lorsqu'une action corrective sera jugée nécessaire.

VII. CONTRÔLE DE LA CNIL A POSTERIORI

Eu égard à ses missions, ses compétences et sa connaissance de la chaîne des traitements de données de TOURS HABITAT, le DPO constitue l'interlocuteur privilégié dans le cas d'un contrôle de la CNIL effectué a posteriori. Chaque collaborateur veillera donc à respecter la procédure intitulée « Comment réagir en en cas de contrôle de la CNIL ? », mise à disposition de tout collaborateur et annexée à la présente politique interne de protection des données **(Annexe 3)**.

Cette procédure prévoit :

- dans le cadre de la réalisation d'un contrôle par la CNIL, le DPO prend toutes les mesures utiles pour faciliter le déroulement de la mission de contrôle (définition des règles d'accueil de la délégation et assurance de la

transmission des informations demandées par exemple), le DPO reçoit du responsable de traitement la copie du procès-verbal de contrôle et est également informé des suites par le responsable de traitement ;
- dans le cadre d'une mise en demeure, le DPO s'assure de la cohérence des actions réalisées suite à la mise en demeure, et du respect des délais ;
- dans le cadre de poursuites devant la formation restreinte, le DPO reçoit du responsable de traitement la copie du rapport à fin de sanction, est consulté pour la rédaction des observations en réponse et s'assure du suivi des actions.

VIII. GESTION DES RÉCLAMATIONS ET EXERCICE DES DROITS DES PERSONNES

Une procédure de gestion des réclamations et demandes d'exercice des droits par les personnes est annexée au présent document **(Annexe 4)**. Celle-ci mentionne notamment les modalités d'exercice des droits, la chaîne de traitement et les délais de communication et de réponse.

Chaque demande parvenant à un salarié doit remonter au Référent.

Le DPO pilote la gestion des réclamations et l'exercice des droits des personnes, notamment en étant informé de la réception de chaque demande, du traitement qui y est apporté, et en s'assurant du respect des délais. Un registre des demandes est tenu.

IX. JOURNALISATION DES ÉVÈNEMENTS DE SÉCURITÉ

Une procédure de Sécurité interne prévoit notamment la mise en place d'une architecture de journalisation permettant de conserver, sur une durée de 6 mois hors contraintes légales spécifiques, une trace des événements de sécurité et du moment où ils ont eu lieu, en choisissant les événements à journaliser en fonction du contexte, des supports (postes de travail, pare-feu, équipements réseau, serveurs…), des risques et du cadre légal.

Cette politique de sécurité, révisée a minima tous les trois ans comprend une démarche particulière pour préserver la confidentialité, l'intégrité et la disponibilité des données à caractère personnel au regard des risques présentés par chaque traitement mis en œuvre.

X. GESTION ET NOTIFICATION DES VIOLATIONS DE DONNEES

Dans le cas où une violation quelconque de données a été détectée, il appartient à toute personne l'ayant constaté de signaler la faille au service informatique et d'en

d'informer le Référent, qui en informera le DPO dans un délai de 24 heures à compter de la détection de la violation.

Cette information devra comporter un descriptif de la violation constatée, l'heure de survenance (le cas échéant) ou de constatation, et les catégories de données potentiellement impactées. Le DPO détermine alors la nature de la violation.

Dès réception de l'information, le DPO formulera alors un plan d'actions adapté pour le proposer au responsable de traitement. Après validation par le responsable de traitement, le DPO réalisera ou fera réaliser les actions correctives nécessaires. Le DPO sera toujours informé de l'état d'avancement des mesures correctives. L'analyse d'impacts correspondant au(x) traitement(s) visé(s) par la violation sera révisée le cas échéant, notamment, la pertinence des mesures mises en place via les actions correctives, devra être évaluée.

Le DPO informera, dans les 72 heures, la CNIL de :

- la nature de la violation,
- les catégories et nombre de personnes concernées par la violation,
- les catégories et nombre approximatif d'enregistrements de données à caractère personnel concernés,
- le nom et les coordonnées du délégué,
- les conséquences probables de la violation de données,
- ainsi que les mesures prises et/ou à prendre pour remédier ou atténuer les éventuelles conséquences négatives.

La même information sera fournie dans les meilleurs délais au Responsable de traitements pour le cas où la faille surviendrait pendant une prestation au cours de laquelle TOURS HABITAT agit en tant que sous-traitant.

Le Responsable de traitement, sur conseil et validation du DPO, alertera également toute personne, dont les données personnelles ont été interceptées de quelque manière par un tiers non autorisé, de l'incident par une notification dans un délai maximal de 72 heures.

XI. ANNEXES

Sont annexés à la présente procédure les documents suivants :

- Annexe 1 : Référentiel « Les données personnelles au quotidien »
- Annexe 2 : Fiche Projet
- Annexe 3 : Procédure « Comment réagir en cas de contrôle de la CNIL ? »
- Annexe 4 : Procédure de gestion des réclamations et demandes d'exercice des droits
- Annexe 5 : Procédure d'habilitation du personnel de TOURS HABITAT
- Annexe 5bis : Formulaire des droits d'accès
- Annexe 6 : Politique interne de gestion et de sécurisation des mots de passe
- Annexe 7 : Politique d'accès aux locaux de TOURS HABITAT
- Annexe 8 : Procédure de notification des failles de sécurité
- Annexe 9 : Charte d'utilisation des véhicules de TOURS HABITAT

- Annexe 10 : Mention d'information à l'attention des collaborateurs

XII. PUBLICITÉ ET ACTUALISATION DE LA PROCÉDURE

La présente politique entre en vigueur le

Cette procédure fera l'objet d'une relecture *a minima* tous les trois ans et fera l'objet d'une mise à jour si nécessaire. Cette procédure fera également l'objet d'une actualisation en cas de désignation d'un nouveau DPO.

Fait à TOURS, le