ORDRE DES ARCHITECTES
CONSEIL FRANCOPHONE & GERMANOPHONE

RGPD - MODE D'EMPLOI DE LA *CHECK-LIST*

1. Identifier et inventorier les méthodes de collecte de Données personnelles

La première étape consiste en l'identification des différentes méthodes de collecte de données opérées, étant, sans que cette énumération ne soit exhaustive :

- *Opération de traitement n°1 : Gestion des clients – Missions d'architecte*

  Il s'agit des données personnelles collectées concernant les maitres de l'ouvrages / clients et parties intervenant dans le cadre de l'exercice des prestations d'architecte, en ce compris d'éventuelles missions d'expertises.

- *Opération de traitement n°2 : Traitement Ressources humaines*

  Dans le cadre du recrutement d'un collaborateur ou encore du personnel support (par exemple un informaticien ou une secrétaire), de la gestion de la paie et de la gestion administrative, l'organisation du travail du personnel, l'architecte employeur est amené à effectuer des traitements de données à caractère personnel.

- *Opération de traitement n°3 : Gestion des fournisseurs et prestataires de services*

  Il s'agit des données collectées à l'égard des fournisseurs de produits et services, que ce soit pour le fonctionnement du bureau ainsi que la gestion de la facturation et de l'interaction des prestataires de services, surtout lorsque ces derniers interviennent en qualité d'indépendants.

- *Opération de traitement n°4 : Site internet*

  Il s'agit des données personnelles collectées automatiquement par le site internet (cookies) de même que les données collectées via un questionnaire en ligne, une consultation en ligne, un formulaire de contact, la création d'un compte en ligne, etc.

- *Opération de traitement n°5 : Gestion des prospects*

  Il s'agit des données de personnes qui ne sont ni clients, ni prestataires, ni employés.

- *Opération de traitement n°7 : Caméra de surveillance*

  Les images collectées par des caméras de surveillance constituent des données à caractère personnelles qui doivent être reprises au sein des registres de traitement

Ces énumérations constituent une base qui peut bien entendu être adaptée et complétée selon les modalités d'exercice de son activité par chacun.

Pour informations, le modèle de registre disponible sur le site www.ordredesarchitectes.be reprend sous l'onglet "Listes APD BE" une série d'exemples types d'opérations de traitement et types de données concernées.

Matthieu Aladenise
Avocat au Barreau de Bruxelles - Avenue Louise 523 – 1050 Ixelles
maladenise@buylelegal.eu - 02/600.52.00

2. Établir des Registres de traitement devant couvrir l'ensemble des méthodes de collecte identifiées :

Le RGPD impose au responsable de traitement l'établissement et la conservation de registres de traitement de données personnelles.

Ces registres constituent une description de la politique et des procédés de collecte et traitement de données personnelles par les architectes et doivent comporter les informations suivantes :

- l'identité de l'architecte ou du bureau;
- les finalités du traitement, c'est-à-dire les motifs précis pour lesquels les données sont collectées ;
- une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement ;
- 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;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou vers une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale, et les documents attestant de l'existence de garanties appropriées ;

Les registres ne doivent donc pas reprendre précisément les données personnelles en tant que telles, mais bien la manière dont les données sont collectées et conservées.
Chacune des opérations de traitement doit faire l'objet d'un registre particulier reprenant chacun en substance les données suivantes :

- *Les catégories de données personnelles*

  Les catégories généralement collectées sont des données d'identification (nom, prénoms, âge, adresse, numéro de registre national, numéro de téléphone, email, etc.), données d'identification financières, données d'emprunts (crédits hypothécaires, crédits, etc.) données d'identification électronique (cookies, adresse IP, etc.), situation familiale ou maritale, diplômes, curriculum vitae et expérience professionnelle, salaire, images vidéos, photos, enregistrements sonores, etc.

  Ces différentes catégories de données ne sont bien évidemment pas toutes collectées dans le cadre de chacune des opérations de traitement. Il est nécessaire de déterminer pour chacune de ses opérations le type de données collectées et traitées. En effet les données relatives aux clients sont différentes des données relatives aux employés.

- *Le délai de conservation des données*

  L'une des plus grandes particularités du RGPD est l'obligation imposée au responsable de traitement de déterminer la durée pendant laquelle il conserve les données personnelles. Cette durée doit bien évidemment être en adéquation avec la finalité poursuivie (durée de la mission d'architecte, délai de conservation d'un dossier client après la fin de la mission, délai de responsabilité légale ou fiscale, etc.).

  La principale conséquence de ce principe est qu'un architecte ne peut pas détenir des données personnelles au-delà de la durée qui a été renseignée dans les registres et est donc tenu d'effacer les données périmées, notamment au sein de ses archives.

Matthieu Aladenise
Avocat au Barreau de Bruxelles - Avenue Louise 523 – 1050 Ixelles
maladenise@buylelegal.eu - 02/600.52.00

- *Les finalités et sous-finalités du traitement* :

  A titre d'exemple, dans le cadre de la gestion des clients, les finalités sont la réalisation de la mission d'architecte (établissement de plans et études architecturales, contrôle de l'exécution des travaux, facturation des clients, etc.)

- *Le fondement du traitement*

  Il s'agit de la justification sur base de laquelle les données personnelles sont collectées.

  Ce fondement doit impérativement correspondre à l'une des catégories suivantes :

  - Consentement de la personne concernée, pouvant être recueilli par l'intermédiaire d'un formulaire ad hoc.

    Il est important de préciser que le consentement ne peut être donné que pour des finalités très précises et ne peut en aucune manière être utilisé à des fins autres que celles annoncées ; dans ce cadre il est donc envisageable qu'il faille procéder à plusieurs collectes de consentement pour une même personne physique (ex. : premier consentement d'un client pour les données nécessaires à la réalisation de la mission d'architecte et second consentement pour l'envoi de newsletters ou autre information)

  - Nécessaire à l'exécution d'un contrat, tels que par exemple des données personnelles d'un client obtenues via une administration ou les données sociales d'un employé communiqué par le secrétariat social ;

  - Obligation légale ;

  - Intérêt légitime, lorsqu'un traitement non consenti et ne ressortissant pas à l'exécution contractuelle en tant que telle s'impose (ex : transfert à des fins administratives ou de facturation vers un tiers comptable)

- *Les mesures de sécurité*

  Description des mesures informatiques et techniques ainsi que des mesures de sécurité physique du bâtiment où sont stockées les données sur papier ainsi que les ordinateurs qui donnent accès aux serveurs.

- *Le lieu de stockage des données*

  Identification du lieu de stockage ou du prestataire de services informatiques en charge de ce stockage.

- *Les catégories de destinataires lors de transfert de données,*

  Par exemple : service public, secrétariat social, organisation professionnelle, prestataires de services externes ou indépendants, services juridiques, avocats, huissiers de justices, etc.

- *Transfert en dehors de l'Union européenne*

3. Établir des Politiques de gestion des données à caractère personnel à destination des personnes concernées

Le RGPD impose un devoir d'information des personnes dont les données sont collectées. Dans ce cadre, il doit être procédé à l'établissement de documents intitulés Politiques de vie privée reprenant les informations suivantes :

- l'identité du responsable de traitement et du délégué à la protection des données ;
- le type de Données personnelles collectées ;
- les finalités pour lesquelles les données sont collectées et traitées ;
- l'identité des destinataires des Données personnelles en cas de transfert :
- la localisation du stockage des Données personnelles ;
- la durée de conservation des Données personnelles ;
- les modalités d'accès, rectification ou demande de suppression ;
- les modalités pour retirer son consentement ;
- la faculté d'introduire une réclamation auprès de l'Autorité de la Protection des données (avec mention de ses coordonnées).

Il doit être établi autant de Politiques de vie privée qu'il existe de types de personnes dont les données sont collectées. En effet, la politique de vie privée encadrant la collecte et le traitement des données des clients sera bien évidemment différente de celle encadrant la collecte et le traitement des données des employés :

4. Communiquer les Politiques de gestion des données à caractère personnel à l'ensemble des personnes concernées avec qui l'architecte est en relation

- la Politique de vie privée des données personnelles des clients devra être spontanément transmise aux clients existants au 25 mai 2018 et par après être transmise au moment de la conclusion du contrat ;

- la Politique de vie privée des données des employés devra être notifiée aux personnes sous contrat de travail et affichée dans les bureaux

- la Politique générale de vie privée des données personnelles prospects et utilisateurs du site internet devra être disponible sur ledit site ;

- la Politique de vie privée des données personnelles des prestataires de services, fournisseurs, etc. devra être notifiée au plus tard le 25 mai 2018 et par après au moment de la conclusion d'une relation contractuelle ;

5. Établir une Analyse d'impact et auditer les mesures de sécurité existantes

Une des nouvelles obligations figurant dans le RGPD concerne l'obligation de réaliser - dans certaines circonstances - une "analyse d'impact relative à la protection des données", en abrégé "AIPD".

Il s'agit d'un processus dont l'objet est de décrire le traitement de données à caractère personnel, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques qui y sont liés en les évaluant et en déterminant les mesures nécessaires pour y faire face.

Concrètement, cette analyse d'impact est un document devant reprendre les informations suivantes :

- une description détaillée et claire des opérations de traitement envisagées et des finalités (synthèse des données reprises dans les registres de traitement) ;
- une évaluation de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques.

Une telle analyse doit être réalisée en cas de traitement de données personnelles à grande échelle et/ou de surveillance systématique ou lorsqu'il existe un risque pour les droits et libertés des personnes concernées en cas de détournement desdites données (usurpation d'identité, vol, perte financière, perte de données couvertes par le secret professionnel, etc.)

S'il existe une tolérance à ce qu'un architecte agissant seul ne soit pas contraint de procéder à l'établissement d'une telle analyse, il est néanmoins conseillé de faire examiner chacune des situations particulières par un professionnel afin de s'assurer qu'aucune des conditions prévues par le RGPD n'est rencontrée.

En cas de nécessité d'établir une telle analyse, il existe un logiciel gratuit et très performant permettant de procéder à l'établissement de la documentation selon les dispositions du RGPD. (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil)

6. Examiner l'ensemble des contrats de sous-traitance et de prestations de services et s'assurer de leur conformité avec le RGPD

Prestataires de services externes

Au terme du RGPD, le responsable de traitement est tenu de s'assurer que les prestataires de services à qui il transmet directement ou indirectement des données personnelles soient en conformité avec ce même règlement, sous peine d'engager sa responsabilité personnelle.

Si recourir à des prestataires externes est bien évidemment autorisé, cette relation contractuelle doit impérativement être assortie de garanties quant au sort réservé aux données personnelles communiquées.

Les prestataires les plus usuels sont les prestataires informatiques (cloud, stockage de serveurs, etc.), secrétariat social mais peuvent également être des bureaux d'études, de design, des bureaux d'architectes, etc.

Dans ce cadre, il doit être veillé à ce que les contrats de prestations de services prévoient à minima :

- l'objet et la durée du contrat, les finalités et la nature du traitement, le type de données personnelles, les catégories de personnes concernées et les droits et obligations des deux parties ;

- une garantie que les données personnelles ne seront traitées que sur la base d'instructions écrites et qu'aucune utilisation pour quelque autre finalité ne sera réalisée (sauf obligation légale explicite);

- une garantie que des mesures techniques et organisationnelles appropriées sont prises afin de garantir un niveau de sécurité adapté au risque ;

- engagement de ne transférer de données personnelles vers un autre sous-traitant sans autorisation écrite préalable et en cas d'autorisation, prévision d'un même niveau de garantie à l'égard de ce nouvel acteur ;

- une garantie que les personnes habilitées à traiter les Données personnelles sont tenues par des engagements de confidentialité (contractuels ou légaux) valables et appropriés ;

- une garantie que les Données personnelles ne sont pas transmises en dehors de l'Union européenne vers des destinations n'offrant pas un niveau de protection adéquat ou sans garanties appropriées supplémentaires qui seront convenues au préalable

- une garantie qu'au terme de la prestation de services, toutes les données personnelles seront supprimées en toute sécurité ou renvoyées au responsable de traitement et que les copies existantes seront détruites ;

- une autorisation de mettre à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par lui ou par un autre contrôleur qu'elle a mandaté, et de contribuer à ces audits.

7. Désigner un délégué à la protection des données

Aux termes du RGPD, les responsables de traitement devront obligatoirement procéder à la désignation d'un délégué :

- Si leurs activités de base (principales) les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;

  Les activités de base peuvent être considérées comme l'ensemble des activités pour lesquelles le traitement de Données personnelles fait partie intégrante des activités du responsable du traitement.

  Les termes "à grande échelle" peuvent se référer à un volume de données, au nombre de personnes concernées, à la durée de conservation des données, à la couverture géographique, etc. Il n'y a pas de seuil déterminé.

- Si leurs activités de base (principales) les amènent à traiter (toujours à grande échelle) des catégories particulières de données, dites « sensibles » ;

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible, et même recommandée.

Le délégué à la protection des données, qui peut être une personne en interne ou un externe, se voit concéder différentes missions et charges :

- informer et conseiller le responsable de traitement, ainsi que leurs employés quant à la problématique des données personnelles ;
- assurer du respect du RGPD et du droit national en matière de protection des données ;
- conseiller le responsable quant à la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci ;
- s'informer sur le contenu des nouvelles obligations ;

- réaliser l'inventaire des traitements de données;
- concevoir des actions de sensibilisation.

En conséquence, la personne qui agit en tant que délégué à la protection des données endossera d'importantes responsabilités.

Les architectes n'ont, en principe, pas pour activité de base de procéder à une collecte de données à caractère personnel.

Dans ces conditions, un parallèle peut être réalisé avec les recommandations officielles adressées aux cabinets d'avocats, selon lesquelles pour l'exercice d'une activité à titre individuel l'obligation permet de passer outre la désignation un délégué à la protection des données.

En ce qui concerne les architectes réunis en société ou groupement, il convient de réaliser un examen afin de s'assurer qu'aucune des conditions prévues par le RGPD n'est réunie (par exemple collecte de nombreuses données personnelles via l'utilisation d'un site internet ou d'une application mobile).

Ici également, les situations de chaque organisation ou bureau étant différentes, il est vivement conseillé de faire procéder à un examen de la situation afin de vérifier si la désignation d'un tel délégué est obligatoire ou non.

8. Afficher sur les sites internet la Politique de gestion des données ainsi que la politique de gestion des cookies