Politique de confidentialité pour les sous-traitants du CPAS de Courcelles

Auteur	CPAS de Courcelles
Statut	Approuvée
Date d'émission	03/04/2020

Critère de Diffusion

Public	~~**Interne**~~	~~**Diffusion restreinte**~~	~~**Hautement Confidentiel**~~

1 Objectifs, cadre et utilisateurs

Ce document a pour objectif de reprendre les droits et obligations des sous-traitants, au sens de la réglementation relative à la protection des données à caractère personnel (ci-après RGPD), agissant pour le compte du CPAS, ci-après dénommé le responsable de traitement au sens de la réglementation relative à la protection des données à caractère personnel.

Cette politique est applicable pour la durée telle que définie dans le contrat entre les deux parties. Dans le cadre de ce contrat, le responsable du traitement ainsi que le sous-traitant s'engagent à respecter les réglementations en matière de vie privée et de protection des données en vigueur.

Le RGPD est un règlement européen mis en application au 25 mai 2018 et bénéficie d'un effet direct dans l'ordre juridique belge à cette date. Toutefois, les Etats membres, dont la Belgique, disposent d'une marge de manœuvre quant à l'implémentation du RGPD dans leur ordre interne, marge de manœuvre susceptible d'impacter l'application du RGPD par le responsable du traitement. Dans le même ordre d'idées, l'Autorité de Protection des Données dispose de la possibilité d'émettre des avis, des recommandations ou d'approuver des codes de conduite qui sont susceptibles d'impacter l'application du RGPD par le responsable du traitement. Enfin, le responsable du traitement est susceptible de devoir faire face aux exigences formulées par les organismes qui lui fournissent un accès à certaines banques de données (par exemple, la BCSS, le RN, etc.). Aussi, il ne peut être exclu que le responsable du traitement sollicite le sous-traitant afin qu'il s'adapte à ces éléments. Ces adaptations sont incluses dans les missions attendues du sous-traitant et ce, sans supplément de prix. Le pouvoir adjudicateur fournit les instructions utiles à l'adjudicataire.

2 Documents de référence

- Règlement général de protection des données,
- Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 30 juillet 2018,
- Charte vie privée du CPAS,
- Standard ISO/IEC 27001[1],
- Standard ISO/IEC 27701[2],

[1] Systèmes de management de la sécurité de l'information - Exigences
[2] Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée – Exigences et lignes directrices

3 Définitions

Au sens des clauses:

a) «*données à caractère personnel*», «*catégories particulières de données*», «*traiter/traitement*», «*responsable du traitement*», «*sous-traitant*», «*personne concernée*» et «*autorité de contrôle*» ont la même signification que dans la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[3];

b) le«*responsable du traitement*» est une personne physique ou morale, une autorité publique, un service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel;

c) le «*sous-traitant* » C'est la personne physique, la personne morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement (il ne s'agit pas ici des personnes qui, sous l'autorité directe du responsable du traitement, sont autorisées à traiter les données).;

d) le «*sous-traitant ultérieur*» est le sous-traitant engagé par le sous-traitants de données ou par tout autre sous-traitant ultérieur de celui-ci, qui accepte de recevoir de l'importateur de données ou de tout autre sous-traitant ultérieur de celui-ci des données à caractère personnel exclusivement destinées à des activités de traitement à effectuer pour le compte de l'exportateur de données après le transfert conformément aux instructions de ce dernier, aux conditions énoncées dans les présentes clauses et selon les termes du contrat de sous-traitance écrit;

e) les «*mesures techniques et d'organisation liées à la sécurité*» sont les mesures destinées à protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement.

[3] Les parties peuvent reprendre, dans la présente clause, les définitions et les significations de la directive 95/46/CE si elles estiment qu'il est préférable que le contrat soit autonome.

4 Caractéristique(s) du/des traitement(s)

A travers le contrat susmentionné, le responsable de traitement mandate le sous-traitant à prester les services tels que spécifiés.

4.1 Finalités du/des traitement(s)

Dans le cadre de ces services, le sous-traitant sera amené à effectuer des traitements de données à caractère personnel pour le compte du responsable de traitement. Les traitements ne seront réalisés que pour les finalités définies dans le contrat entre le sous-traitant et le responsable de traitement et/ou sur la base des instructions données en cours d'exécution du contrat.

4.2 Catégories de données à caractère personnel traitées et personnes concernées

Les catégories de données à caractère personnel et les catégories de personnes concernées par les traitements effectués sont également reprises dans le contrat entre le sous-traitant et le responsable de traitement ou spécifiées lors d'instructions données en cours d'exécution du contrat par le responsable de traitement.

5 Obligations et droits du responsable de traitement

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données nécessaires pour être en ordre avec les réglementations idoines ;
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
- s'assurer, avant la conclusion du contrat et pendant son exécution, que le sous-traitant se conforme bien aux dispositions prévues par les réglementations applicables ;
- contrôler la bonne exécution du traitement par le sous-traitant, y compris éventuellement réaliser les audits et les inspections auprès de celui-ci.

6 Obligations et droits du sous-traitant

Le sous-traitant ne procèdera au traitement des données que pour les finalités prévues par les modalités du contrat et sur la base des instructions documentées ou données en cours d'exécution du contrat par le responsable du traitement.

L'utilisation des données à caractère personnel à d'autres fins telles que la publicité, le marketing direct, le profilage, le courtage d'adresses, est strictement prohibée, de même que la communication de ces données à des tiers.

Le sous-traitant informe le responsable de traitement si une des instructions communiquées lui semble contraire à la réglementation relative à la protection des données à caractère personnel ou au droit en général.

Tout transfert de données vers un autre pays ou vers une tierce partie est interdit, sauf accord du responsable de traitement. Si le sous-traitant est tenu de procéder à ce type de transfert par obligation légale, il est tenu d'informer le responsable de traitement avant le traitement concerné.

Le sous-traitant ne recrute pas un autre sous-traitant (ultérieur) sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.
Le sous-traitant communique au responsable de traitement les informations nécessaires à la réalisation et la mise à jour de son registre des activités de traitement, aux analyses d'impact relatives à la protection des données ainsi qu'aux respects des obligations du responsable de traitement envers l'Autorité de protection des données.

6.1 Confidentialité, intégrité et accessibilité des données

Le sous-traitant s'engage à respecter la confidentialité des données qu'il sera amené à traiter notamment en s'assurant de disposer de dispositifs légaux contraignants[4] à l'égard des personnes amenées à traiter ces données en son sein.

En plus de leur caractère confidentiel, le sous-traitant s'engage également à garantir la sécurité, l'intégrité et la disponibilité des données traitées en procédant à une analyse des risques concernant le traitement de ces données. Sur base de cette analyse et compte tenu de l'état des connaissances, le sous-traitant met en œuvre les mesures techniques et organisationnelles appropriées au(x) traitement(s). Sans toutefois s'y limiter, il peut s'agir de :

- la pseudonymisation et le chiffrement des données à caractère personnel;
- moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
- 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;
- mettre en place une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement[5].

[4] Il peut s'agir de clauses de confidentialité présentes dans le contrat de travail de l'employé par exemple.
[5] Il s'agit des mesures exemplatives telles que reprises dans le RGPD, article 32. Pour plus d'exemple, nous vous invitons notamment à consulter le code de bonne pratique pour le management de la sécurité de l'information, ISO 27002.

Sauf indications contraires spécifiques prévues dans le contrat, le sous-traitant supprimera ou enverra au responsable de traitement les données à caractère personnel au terme de la prestation de services relatifs aux traitements concernés.
Le sous-traitant met à la disposition du responsable du traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits.

6.2 Registre des activités de traitement

Le sous-traitant tient par écrit un registre de toutes les activités de traitement effectuées pour le compte du responsable de traitement selon l'article 30 du RGPD.

7 Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).
Le sous-traitant informe sans tarder le responsable de traitement de toute plainte ou tout avis d'une personne concernée par les traitements des données du responsable de traitement, par courrier électronique à dpd@cpascourcelles.eu ou par courrier postal adressé à Rue Baudouin 1er, 119, 6180 Courcelles.

8 Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance par courrier électronique à dpd@cpascourcelles.eu. Cette notification doit décrire la nature (dont la catégorie et le nombre approximatif de personnes concernées), ses conséquences probables et les mesures envisagées. Elle est accompagnée de toute documentation utile afin de permettre au pouvoir adjudicateur, si nécessaire, de notifier cette violation à l'Autorité de Contrôle compétente et aux personnes concernées.

9 Délégués à la protection des données

Afin de garantir une communication efficace entre le responsable de traitement et le sous-traitant, ce dernier désignera une personne de contact en son sein pour les questions relatives à la protection des données à caractère personnel et transmettra ses coordonnées au délégué à la protection des données du responsable de traitement, par courrier électronique à dpd@cpascourcelles.eu ou par courrier postal adressé à Rue Baudouin 1er, 119, 6180 Courcelles.