



Avis n° 74/2018 du 5 septembre 2018

Objet : Avant-projet d'arrêté du Gouvernement flamand relatif à la politique sociale locale (CO-A-2018-065)

L'Autorité de protection des données (ci-après "l'Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 ;

Vu la demande d'avis de Monsieur Jo Vandeurzen, Ministre flamand du Bien-être, de la Santé publique et de la Famille, reçue le 17 juillet 2018 ;

Vu le rapport de Monsieur Willem Debeuckelaere ;

Émet, le 5 septembre 2018, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le 17 juillet 2018, le Ministre flamand du Bien-être, de la Santé publique et de la Famille (ci-après "le demandeur") a sollicité l'avis de l'Autorité quant à un avant-projet d'arrêté du Gouvernement flamand relatif à la politique sociale locale, mentionné aux articles 2, 9 à 11 inclus, 17, 19 et 26 du décret du 9 février 2018 *relatif à la politique sociale locale* (ci-après "le Projet").
2. Par son décret du 9 février 2018 *relatif à la politique sociale locale* (ci-après "le décret")¹, l'Autorité flamande souhaite reconnaître les administrations locales en tant que partenaires effectifs et indispensables dans la politique du bien-être, de la santé et de la famille². En vue de la régie de l'aide sociale et des services sociaux, l'administration locale doit élaborer, via la maison sociale (het Sociaal Huis), un partenariat "*geïntegreerd breed onthaal*" (accueil large intégré) reprenant au moins le centre public d'action sociale (CPAS), le centre agréé pour le bien-être général et les services sociaux des mutualités³. L'accueil large intégré sert de point de contact et d'orientation vers les acteurs appropriés qui participent à l'aide sociale et aux services sociaux. La prestation d'une aide sociale ou d'un service social sur mesure, comme il ressort de l'article 10 du décret, n'est possible que si les données à caractère personnel nécessaires sont collectées, comme cela est explicitement prévu à l'article 11, § 2 du décret.

"§ 2. Les acteurs qui doivent au minimum faire partie du partenariat d'accueil large intégré, visé à l'article 9, alinéa 2, qui offrent de l'aide et des services aux usagers, traitent des données à caractère personnel et les échangent entre eux afin que de l'aide et des services responsables puissent être fournis à ces usagers, et que la continuité de l'aide et des services puisse être garantie. Ces données à caractère personnel comprennent aussi les données à caractère personnel visées aux articles 9, alinéa 1^{er}, et 10 du règlement général sur la protection des données. Le traitement des différentes catégories de données à caractère personnel prévoit un niveau de sécurité approprié et la confidentialité nécessaire.

Sans préjudice de l'application des obligations et limitations résultant de la réglementation relative à la protection lors du traitement des données à caractère personnel, entre autres celles qui s'appliquent spécifiquement à la communication de données à caractère personnel, telles qu'elles sont spécifiées le cas échéant au niveau fédéral ou flamand, ou des réglementations des secteurs, cet échange de données est soumis aux conditions suivantes :

¹ Le projet de texte de ce décret a été soumis à l'avis du prédécesseur en droit de l'Autorité, à savoir la Commission de la protection de la vie privée, le 9 juin 2017. Le 1^{er} août 2017, la Commission a informé le demandeur du fait qu'elle ne pouvait pas émettre d'avis sur le projet de texte de l'époque, se référant aux articles 11 et 17 de son Règlement d'ordre intérieur du 26 juin 2013. L'avis de la Commission n'a ensuite plus été demandé au sujet du projet de texte du décret.

² Exposé des motifs, page 1.

³ Article 9 du décret.

*1° l'échange de données ne concerne que les données qui sont nécessaires pour une aide et des services responsables et la continuité de l'aide et des services ;
2° les données ne sont échangées que dans l'intérêt des usagers ;
3° sauf cas de force majeure ou nécessité urgente, l'utilisateur à qui les données ont trait, doit donner son consentement à l'échange de données, de la façon arrêtée par le Gouvernement flamand.*

Le Gouvernement flamand arrête les modalités concernant la forme et la façon dont les données à caractère personnel sont traitées et échangées. Le Gouvernement flamand arrête les catégories de données qui sont traitées et échangées. Dans le présent paragraphe, on entend par consentement : toute manifestation de volonté libre, spécifique, informée et explicite."

3. Le Projet vise à exécuter le décret, notamment en concrétisant les fonctions et les principes de fonctionnement du partenariat 'accueil large intégré'. Il contient également un article spécifique régissant le traitement de données à caractère personnel par et entre les collaborateurs impliqués dans le partenariat précité :

"Article 6. Pour réaliser les fonctions de l'accueil large intégré, les collaborateurs des acteurs du partenariat d'accueil large intégré, mentionné à l'article 9 du décret du 9 février 2018, traitent les données à caractère personnel suivantes de l'utilisateur :

- 1° les données d'identité et coordonnées de l'utilisateur ;*
- 2° les données nécessaires à l'exploration et à l'exécution des droits du client, notamment l'identification du droit, la date de la demande, la date et la nature de la décision ;*
- 3° les demandes de soutien, les finalités et les actions que l'utilisateur formule dans les différents domaines de la vie ;*
- 4° les données d'identité et coordonnées pertinentes des personnes impliquées dans l'aide et les services à l'utilisateur.*

Si différents travailleurs de base et organisations sont impliqués dans le parcours d'accueil individuel, ils peuvent s'échanger les données mentionnées au premier alinéa.

Le client possède les droits mentionnés aux articles 12 à 19 inclus du Règlement général sur la protection des données.

Tout travailleur de base informe adéquatement le client de ses droits dans le cadre du traitement de données à caractère personnel, conformément à la réglementation en vigueur." [Tous les passages du Projet cités dans le présent avis ont été traduits librement par le Secrétariat de l'Autorité de protection des données, en l'absence de traduction officielle].

II. EXAMEN DE LA DEMANDE D'AVIS

1. Finalité

4. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes.
5. Dans le présent contexte, les données de clients du partenariat 'accueil large intégré' seront traitées, ce qui ressort explicitement de l'article 6 du Projet, cité au point 3. Par ailleurs, des "*données d'identité et coordonnées*" de prestataires d'aide et de services seront également traitées. Il ressort de l'article 11, § 2 du décret (cf. supra, point 2) que l'aide et les services aux clients constituent les finalités générales des traitements de données précités. À l'article 4 du Projet, ces finalités sont également précisées plus avant :

"Le partenariat d'accueil large intégré remplit les fonctions suivantes :

1° mettre en place des actions proactives : mise en place d'actions communes dans lesquelles le partenariat prend lui-même l'initiative de chercher à contacter des personnes vulnérables afin de veiller à ce que ces personnes obtiennent des droits et reçoivent des soins et un soutien ;

2° écouter la demande d'aide et la clarifier depuis une perspective généraliste large : contextualiser la demande d'aide avec l'utilisateur, dresser l'inventaire des problèmes et les cerner pour avoir une meilleure vue de la nature des problèmes, permettre à l'utilisateur de comprendre sa situation et explorer toutes les solutions alternatives ;

3° explorer les droits des utilisateurs et informer les utilisateurs de manière proactive de leurs droits sociaux fondamentaux ;

4° donner des informations objectives et transparentes quant à l'intégralité de l'offre d'aide et de services sociaux locaux : fournir des informations individuelles et sur mesure appropriées dans le cadre de l'aide et des services ;

5° fournir un avis ciblé : informer l'utilisateur de manière objective et transparente, compte tenu de sa situation personnelle ; proposer des perspectives de solutions, des possibilités de choix et des comportements alternatifs, afin que l'utilisateur dispose de plus de connaissances et puisse opérer un choix réfléchi. L'offre est clarifiée de manière à pouvoir déterminer avec l'utilisateur quelle offre d'aide est recommandée à l'égard de la demande ;

6° réaliser les droits des utilisateurs : soutenir les utilisateurs afin de réaliser au maximum leurs droits sociaux fondamentaux et apporter au besoin une aide socio-administrative ;

7° renvoyer de manière neutre vers l'aide sociale et les services sociaux appropriés : rediriger les utilisateurs vers l'aide sociale et les services sociaux appropriés de leur choix ;

8° garder un aperçu du parcours d'aide de l'utilisateur, faire office de point de retour s'il est mis fin à l'aide et aux services à l'utilisateur, rester disponible pour les autres questions

de l'utilisateur et assurer une médiation entre l'utilisateur et d'autres acteurs locaux en cas d'imprécisions ou de problèmes ;

9° signaler les seuils : signaler aux différents acteurs locaux concernés les seuils qui menacent l'accès à l'aide et aux services sociaux locaux ainsi que les facteurs qui renforcent la sous-protection.

Au premier alinéa, on entend par droits sociaux fondamentaux : les droits mentionnés aux articles 23 et 24, § 3 de la Constitution."

6. L'Autorité constate que ces finalités sont déterminées, explicites et légitimes.

2. Base juridique

7. Tout traitement de données à caractère personnel doit reposer sur une base juridique au sens de l'article 6 du RGPD. En outre, le traitement de catégories particulières de données à caractère personnel, dont par exemple des données relatives à la santé, est en principe interdit en vertu de l'article 9.1. du RGPD. Cette interdiction ne s'applique pas si le responsable du traitement peut invoquer un des motifs de justification de l'article 9.2. du RGPD.
8. Le décret semble *prima facie* désigner le "consentement" (article 6.1.a) & 9.2.a) du RGPD) comme base juridique : *"sauf force majeure ou urgence, l'utilisateur auquel les données se rapportent doit marquer son accord sur l'échange de données (...) "*⁴ Mais l'Exposé des motifs du décret avance un autre fondement⁵: *"Le traitement est basé sur l'article 6, premier alinéa, e) du Règlement général sur la protection des données. S'il s'agit de catégories particulières de données à caractère personnel, il est fait usage des exceptions à l'interdiction de traitement décrites à l'article 9, alinéa 2, g). Pour les données à caractère personnel pénales, le traitement tient compte de l'article 10 du Règlement général sur la protection des données. (...) Le dernier alinéa reprend également une définition de l' "accord". Cette définition est basée sur celle du Règlement général sur la protection des données, sans pour autant y correspondre entièrement. Cela est dû au fait que cet accord ne constitue pas une base juridique pour le traitement de données à caractère personnel, mais uniquement une garantie supplémentaire lors du partage de données avec des tiers. (...) "*⁶ Vu cette explication dans l'Exposé des motifs, l'Autorité estime que l' "accord" préalable prévu dans le décret n'implique pas que l'auteur du décret ait voulu retenir la base juridique du "consentement"⁶.
9. Pour les traitements de données à caractère personnel en question qui ne font pas partie des catégories particulières de l'article 9 du RGPD, l'Autorité estime qu'ils peuvent reposer

⁴ Article 11, § 2 du décret, cité in extenso au point 2.

⁵ Pages 18 & 19, doc. Parlement flamand n° 1375 (2017-2018) (<http://docs.vlaamsparlament.be/pfile?id=1348978>).

⁶ Il se pose d'ailleurs la question de savoir quelle est la valeur ajoutée de cet "accord", vu que les traitements de données auront lieu quoi qu'il en soit, que les personnes concernées donnent ou non leur "accord".

effectivement sur l'article 6.1.e) du RGPD : l'exécution d'une mission d'intérêt public. Dans ce contexte, l'Autorité attire l'attention sur l'article 6.3 du RGPD⁷ qui prescrit quels éléments essentiels de traitements de données trouvant leur fondement dans l'article 6.1.e) du RGPD doivent en principe être repris dans la réglementation. L'Autorité constate que certains éléments sont en partie repris dans le Projet (par exemple les finalités), alors que d'autres aspects ne sont pas abordés (comme par exemple la désignation du responsable du traitement, les délais de conservation,...). L'Autorité insiste pour que les éléments qui manquent encore soient repris dans le Projet⁸ ou le cas échéant dans une délibération d'un comité sectoriel ou du Comité de sécurité de l'information^{9 10}.

Dans ce contexte, l'Autorité attire également l'attention sur l'article 20 de la loi-cadre en matière de protection des données¹¹ et sur un récent décret flamand¹² qui impose aux autorités de conclure des protocoles d'accord pour les échanges de données basés sur l'article 6.1.e) du RGPD. Comme le précise l'Exposé des motifs de la loi-cadre en matière de protection des données, un tel protocole ne peut en soi pas constituer une base légale et chaque échange sur la base de l'article 6.1.e) du RGPD doit quoi qu'il en soit disposer d'une

⁷ "(...) 3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par:

a) le droit de l'Union ; ou

b) le droit de l'État membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi. (...)"

⁸ On peut faire référence ici aux types ou catégories de données à caractère personnel à traiter, aux personnes concernées, aux entités auxquelles les données à caractère personnel peuvent être communiquées et aux finalités pour lesquelles elles peuvent l'être, aux durées de conservation et à la désignation du (des) responsable(s) du traitement.

⁹ Les comités sectoriels se trouvent actuellement dans une phase de transition et seront remplacés à terme par le Comité de sécurité de l'information (voir article 114, §§ 3 et 4 de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, ainsi que les pp. 4 et 5 de l'Exposé des motifs de la loi du 25 mai 2018 qui a remplacé cet article 114 dans la loi de décembre 2017 (DOC 54 3104/001 (<http://www.dekamer.be/doc/flwb/pdf/54/3104/54k3104001.pdf>)). Voir également le projet de loi *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE*, Chambre, DOC. 54, 3185/007, approuvé le 19 juillet 2018).

¹⁰ Bien qu'en vertu de l'article 6.3 du RGPD, ainsi que de l'article 8 de la CEDH et de l'article 22 de la Constitution, la réglementation qui encadre le traitement de données à caractère personnel doit en principe au moins mentionner plusieurs éléments essentiels de ce traitement, l'Autorité estime que dans des cas exceptionnels, la réglementation peut aussi prévoir qu'un certain nombre de ces éléments essentiels (à l'exception de la finalité) doivent être précisés ultérieurement dans le cadre d'une délibération qui sera émise par le comité compétent en la matière.

¹¹ Loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

¹² Cf. l'article 16 du décret *portant adaptation des décrets au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*.

base légale claire avant que l'échange de données et la conclusion d'un protocole y afférent ne soient possibles¹³.

10. L'article 11, § 2, premier alinéa, du décret dispose que les acteurs qui font partie du partenariat 'accueil large intégré' peuvent également traiter les catégories particulières de données à caractère personnel au sens de l'article 9.1 du RGPD. Sans préjudice de ses remarques fondamentales quant à la pertinence de certaines de ces données (cf. infra, points 13 et 14), l'Autorité fait remarquer que si le demandeur veut fonder ce traitement sur l'article 9.2.g) du RGPD, il doit démontrer l'intérêt public important qui requiert le traitement de ces données. En outre, la réglementation doit contenir des règles spécifiques pour veiller à la protection des droits fondamentaux et des intérêts fondamentaux des personnes concernées. À défaut d'une justification pour le traitement de cette catégorie particulière de données à caractère personnel et sans les garanties nécessaires, le Projet n'offre aucune base juridique afin de traiter ces données à caractère personnel particulières. Le décret contient un certain nombre de garanties. Il précise ainsi qu'un niveau de sécurité adéquat sera prévu et que la confidentialité nécessaire sera prise en compte lors du traitement¹⁴. On peut également se référer à la loi-cadre en matière de protection des données¹⁵, qui impose en son article 9 des mesures spécifiques pour le traitement de données sensibles (cf. infra, point 25). L'Autorité recommande toutefois de prévoir encore des garanties complémentaires dans le Projet, comme par exemple :
- imposer des mesures pour garantir un niveau élevé de transparence (par exemple une obligation d'informer les personnes concernées via différents canaux, comme via un site Internet et des clauses standard dans des formulaires papier et en désignant un *point de contact unique* où les personnes concernées peuvent obtenir des informations par téléphone ...) ¹⁶ ;
 - imposer des mesures de sécurité strictes (par exemple un cryptage obligatoire) (cf. infra, points 22 à 26 inclus) ¹⁷.
11. Par ailleurs, l'Autorité constate qu'en vertu de l'article 11, § 2, premier alinéa du décret, des données seront également traitées au sujet de condamnations pénales et d'infractions

¹³ Voir l'Exposé des motifs de l'article 20 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* : "À ce titre, cet article prévoit que des protocoles doivent être rédigés pour formaliser les modalités de l'échange de données, qui trouve son origine dans une base légale. (...) Par base légale, il faut entendre tout texte de loi national ou supranational qui peut amener une administration à devoir traiter des données pour remplir ses missions au sens large. (...)".

¹⁴ Article 11, § 2, premier et deuxième alinéas du décret.

¹⁵ Loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

¹⁶ Voir les points 55 et 64 des lignes directrices du Groupe 29 à cet égard (WP260) : <https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Transparency.pdf>.

¹⁷ La délégation au pouvoir exécutif prévue dans le décret (cf. l'article 11, § 2, avant-dernier alinéa du décret) indique d'ailleurs aussi que le Projet doit arrêter les modalités "concernant la forme et la façon dont les données à caractère personnel sont traitées et échangées." et l'imposition de mesures de sécurité spécifiques dans le Projet pourrait donc s'inscrire dans ce cadre.

pénales, ce qui concerne des traitements qui, en vertu de l'article 10 du RGPD, ne sont permis que sous le contrôle d'une autorité publique ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. En l'espèce, les données seront traitées principalement par des autorités publiques, mais il est également possible que des organisations privées procèdent au traitement de ce type de données¹⁸. Le Projet doit dès lors prévoir des garanties appropriées telles qu'imposées par l'article 10 du RGPD. À cet égard, l'Autorité renvoie aux suggestions qu'elle a déjà formulées au point 10.

En outre, ces instances ne pourront en effet traiter ce type de données (sur la base de la loi-cadre en matière de protection des données¹⁹) que "*lorsque le traitement est nécessaire pour des motifs d'intérêt public important pour l'accomplissement de tâches d'intérêt général confiées par ou en vertu d'une loi (...)*". Dans l'Exposé des motifs du décret, le traitement de données de l'article 10 du RGPD est motivé comme suit : "*des données à caractère personnel relatives aux condamnations pénales et aux infractions pénales sont également conservées dans une moindre mesure étant donné que les centres d'aide sociale générale prévoient notamment de l'aide et des services aux détenus.*" L'Autorité recommande dès lors de préciser dans le Projet que les données de l'article 10 du RGPD ne seront traitées que dans le cadre de l'aide et des services aux détenus, étant donné qu'il semble que ce soient les seuls cas pour lesquels le traitement de ce type de données sont nécessaires.

3. Principe de minimisation des données

12. L'article 5.1.c) du RGPD dispose que les données à caractère personnel doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ("minimisation des données"). Le décret indique que le partenariat 'accueil large intégré' ne peut traiter que des données "*qui sont nécessaires pour un responsable d'aide et de services et pour la continuité de l'aide et des services*"²⁰, ce qui correspond au principe de minimisation des données.
13. Le décret dispose par ailleurs dans son Exposé des motifs – de manière générale et sans motivation – que des données à caractère personnel seront traitées au sens de l'article 9.1. du RGPD. L'Autorité s'interroge à cet égard sur la mesure dans laquelle il est nécessaire que le partenariat 'accueil large intégré' traite toutes les catégories de données à caractère personnel énoncées à l'article 9.1. du RGPD (cf. 11, § 2, premier alinéa du décret). Qu'en est-il par exemple des données à caractère personnel qui révèlent les opinions politiques, les

¹⁸ Cf. l'article 3, 5° & 6° du décret.

¹⁹ Voir l'article 10, § 1, 3° de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

²⁰ Article 11, § 2, deuxième alinéa, 1° du décret.

convictions religieuses ou philosophiques ou l'appartenance syndicale ou des traitements de données génétiques ou biométriques ? Le demandeur doit vérifier quelles sont les catégories de données véritablement nécessaires pour les finalités avancées. Entre-temps, l'Autorité estime que le renvoi général actuel dans le décret à l'article 9.1. du RGPD ne répond pas à l'article 5.1.c) du RGPD. Une limitation de la base juridique aux données pertinentes – par exemple par une mention explicite dans le Projet des catégories de données qui peuvent être traitées – s'impose dès lors.

14. Étant donné ces éléments et de manière plus générale, l'Autorité rappelle également que la détermination des types de données qui seront traitées par finalité est considérée comme un des éléments essentiels qui doivent en principe être établis dans la réglementation (voir aussi le point 9 ci-avant). Et la délégation au pouvoir exécutif prévue dans le décret (cf. article 11, § 2, avant-dernier alinéa du décret) prévoit aussi que le Projet doit définir les catégories de données qui sont traitées et échangées. L'Exposé des motifs du décret y ajoute encore l'élément suivant : *"Lors de l'exécution de cette disposition, le Gouvernement flamand devra accorder une attention particulière à la limitation du traitement et de l'échange catégories particulières de données."*²¹ L'Autorité constate toutefois que le Projet fait défaut sur ce point. La motivation et l'encadrement du traitement de données de l'article 9.1. du RGPD ne sont en effet pas suffisamment développés et l'Autorité insiste pour que le Projet soit corrigé sur ce point.

4. Délai de conservation

15. Selon l'article 5.1.e) du RGPD, les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.
16. Le Projet ne prévoit pas de délai de conservation. À la lumière de l'article 6.3. du RGPD, l'Autorité recommande, lorsque c'est possible, de prévoir encore par finalité de traitement – dans le Projet (ou dans une délibération d'un comité sectoriel ou du Comité de sécurité de l'information)²² – des délais de conservation spécifiques ou des critères de détermination pour les délais de conservation (cf. supra, point 9).

5. Responsabilité

17. L'article 4.7. du RGPD prévoit que pour les traitements dont les finalités et les moyens sont déterminés par la réglementation, le responsable du traitement est celui qui est désigné par la réglementation en question. Le Projet ne contient aucune disposition spécifique à cet égard.

²¹ P. 17, doc. Parlement flamand n° 1375 (2017-2018) (<http://docs.vlaamsparlament.be/pfile?id=1348978>).

²² Voir le point 9 ci-dessus.

Il importe toutefois que la personne concernée (utilisateur de l'aide et des services, dont les données sont traitées) puisse par exemple savoir à qui elle doit s'adresser pour faire valoir ses droits en vertu du RGPD. Une seule phrase du Projet y fait allusion de manière sommaire. L'article 6, avant-dernier alinéa dispose notamment qu'il relève de la responsabilité de tout *"travailleur de base"*²³ d'informer le client de manière appropriée de ses droits en matière de protection des données²⁴. Il ne s'agit toutefois pas d'une désignation explicite du ou des responsables du traitement ni d'une répartition des rôles parmi ces travailleurs de base.

18. L'Autorité recommande dès lors de désigner le(s) responsable(s) du traitement dans le Projet. Si plusieurs responsables du traitement étaient désignés, il faut le cas échéant également tenir compte de l'article 26 du RGPD qui impose l'obligation de prévoir entre responsables conjoints du traitement un accord contractuel où sont définies leurs obligations respectives. Pour chaque traitement, on doit en tout cas savoir clairement quel(s) acteur(s) intervient(interviennent) en tant que responsable du traitement.
19. Par souci d'exhaustivité – et sans préjudice de toutes les autres obligations imposées par le RGPD et la loi-cadre en matière de protection des données²⁵ –, l'Autorité souligne l'obligation de tout responsable du traitement de vérifier s'il est nécessaire ou non de désigner un délégué à la protection des données (article 37 du RGPD)²⁶ et/ou de réaliser une analyse d'impact relative à la protection des données (article 35 du RGPD)^{27 28}.

²³ Il s'agit des collaborateurs des CPAS, du "erkende centrum voor algemeen welzijnswerk" (centre agréé d'aide sociale générale) et des "erkende diensten maatschappelijk werk" (services sociaux agréés) des mutualités qui collaborent au sein du partenariat 'accueil large intégré' (cf. article 1, 1° & 4° du Projet).

²⁴ Article 6, avant-dernier alinéa du Projet.

²⁵ Loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

²⁶ Pour des directives en la matière, voir :

- Informations sur le site Internet de l'Autorité : <https://www.autoriteprotectiondonnees.be/dossier-thematique-delegue-a-la-protection-des-donnees>

- recommandation de la CPVP n° 04/2017

- (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_04_2017.pdf)

- Lignes directrices du Groupe 29 (WP 243)

- (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/wp243rev01_fr.pdf)

²⁷ Pour des directives en la matière, voir :

- Informations sur le site Internet de l'APD : <https://www.autoriteprotectiondonnees.be/analyse-dimpact-relative-a-la-protection-des-donnees>

- recommandation de la CPVP n° 01/2018

- (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf)

- Lignes directrices du Groupe 29 (WP 248)

- (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/wp248%20rev.01_fr.pdf)

²⁸ Une analyse d'impact relative à la protection des données peut d'ailleurs aussi être réalisée dès le stade de préparation de la réglementation (comme par exemple le Projet et/ou son arrêté d'exécution). Voir à cet égard l'article 35.10 du RGPD et les points 90-91 de la recommandation CPVP n° 01/2018.

Voir aussi l'article 23 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, qui prévoit l'obligation de réaliser quoi qu'il en soit une analyse d'impact relative à la protection

6. Droit des personnes concernées

20. L'article 6, avant-dernier alinéa du Projet précise que les clients disposent des droits mentionnés aux articles 12 à 19 inclus du RGPD. L'Autorité se demande pourquoi on ne mentionne pas les droits repris aux articles 21 et 22 du RGPD²⁹. Si le but est de limiter ces droits, l'article 23 du RGPD doit alors être respecté, ce qui n'est pas le cas en l'occurrence. L'Autorité insiste dès lors pour que l'article 6, avant-dernier alinéa du Projet renvoie également aux articles 21 et 22 du RGPD (ou pour que l'article 23 du RGPD soit respecté³⁰).
21. L'Autorité constate par ailleurs que l'Exposé des motifs du décret mentionne ce qui suit : *"S'il n'est pas possible d'informer la personne concernée pour certaines raisons, le transfert d'information peut également se faire sans fournir des informations au préalable"*³¹. L'Autorité fait remarquer que l'obligation d'information est une condition de base pour un traitement licite de données à caractère personnel (articles 12 à 14 inclus du RGPD) et que l'on ne peut en principe y déroger en l'espèce. Si le demandeur estime qu'il y a des motifs légitimes de limiter ou d'exclure l'information, cela doit se faire dans les limites de l'article 23 du RGPD, comme expliqué plus haut (cf. point 20) ou il convient de respecter les conditions des articles 13.4 ou 14.5. du RGPD. Étant donné que ni le Projet, ni (l'Exposé des motifs du) décret ne mentionnent ces motifs d'exception du RGPD, l'Autorité part du principe que l'obligation d'information est d'application sans aucune limitation, en dépit du passage précité de l'Exposé des motifs du décret.

7. Mesures de sécurité

22. L'article 32 du RGPD oblige le responsable du traitement à prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état des connaissances en la matière et des coûts qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

des données pour l'activité de traitement, même si une analyse d'impact générale relative à la protection des données a déjà été réalisée dans le cadre de l'adoption de la base légale.

²⁹ Ces articles traitent respectivement du droit d'opposition et de la prise de décision individuelle automatisée.

³⁰ Si le demandeur devait envisager de prévoir des dérogations spécifiques en vertu de l'article 23 du RGPD, l'Autorité conseille de tenir compte des points d'attention formulés par la Commission de la protection de la vie privée dans les points 36 et suivants de son avis n° 34/2018.

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_34_2018.pdf)

³¹ Exposé des motifs du décret (Doc. Parlement flamand n° 1375 (2017-2018) (<http://docs.vlaamsparlement.be/pfile?id=1348978>))

23. L'article 32 du RGPD se réfère à cet égard à plusieurs exemples de mesures afin d'assurer, au besoin, un niveau de sécurité adapté au risque :
- la pseudonymisation et le chiffrement des données à caractère personnel ;
 - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes de traitement ;
 - 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 ;
 - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
24. Pour l'exécution concrète de ces mesures, l'Autorité renvoie à la recommandation³² visant à prévenir les fuites de données et aux mesures de référence³³ qu'il convient de respecter dans le cadre de tout traitement de données à caractère personnel. Vu le caractère sensible des données qui peuvent être traitées dans le cadre du Projet et le grand nombre d'acteurs différents (et de leurs collaborateurs) qui sont impliqués, l'Autorité souligne l'importance d'une gestion correcte des utilisateurs et des accès.³⁴ Les échanges de données par les institutions de sécurité sociale – comme par exemple les CPAS et les mutuelles – doivent d'ailleurs se faire via la Banque Carrefour de la Sécurité Sociale et pour ces flux, une gestion des utilisateurs et des accès correcte sera dès lors déjà d'application.
25. Les catégories particulières de données à caractère personnel au sens des articles 9 et 10 du RGPD requièrent des mesures de sécurité plus strictes. La loi-cadre en matière de protection des données³⁵ indique quelles mesures de sécurité supplémentaires devront être prévues :
- désigner les catégories de personnes, ayant accès aux données à caractère personnel, avec une description précise de leur fonction par rapport au traitement des données visées ;
 - tenir la liste des catégories des personnes ainsi désignées à la disposition de l'Autorité ;

³² Recommandation CPVP n° 01/2013

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf)

³³ Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel, Version 1.0, (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_scurite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf)

³⁴ Voir également la recommandation CPVP n° 01/2008

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf)

Différentes instances peuvent proposer à cet effet des solutions technologiques appropriées (comme par exemple la Banque Carrefour de la Sécurité Sociale).

³⁵ Article 9 et 10, § 2 de loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

- veiller à ce que ces personnes désignées soient tenues par une obligation légale ou statutaire ou par une disposition contractuelle au respect du caractère confidentiel des données visées.
26. Le Projet ne mentionne rien à propos de la sécurité des données à caractère personnel. Bien que cette obligation découle bien entendu de la qualité du responsable du traitement, l'Autorité recommande de mieux encadrer l'obligation de sécurité dans le Projet (et/ou dans une délibération d'un comité sectoriel ou du Comité de sécurité de l'information), en particulier en ce qui concerne l'élaboration de la gestion des utilisateurs et des accès.

III. CONCLUSION

27. À condition que les remarques suivantes soient intégrées dans le texte :
- intégrer tous les éléments essentiels des traitements de données envisagés dans le Projet (voir les points 9, 16 & 18) ;
 - mettre le fondement juridique prévu dans le Projet pour le traitement de données sensibles en conformité avec les articles 9.1 et 10 du RGPD et avec la loi-cadre en matière de protection des données (voir les points 10 et 11) ;
 - respecter le principe de la "minimisation des données" en ce qui concerne le traitement de données sensibles (voir les points 13 et 14) ;
 - lever les imprécisions relatives à l'applicabilité de certains droits du RGPD (points 20-21) ;
 - préciser des garanties supplémentaires afin d'assurer un niveau de protection adéquat, en particulier au niveau de la gestion des utilisateurs et des accès (voir le point 26) ;

l'Autorité estime que le Projet peut offrir suffisamment de garanties quant à la protection des données à caractère personnel des personnes concernées.

PAR CES MOTIFS,

l'Autorité émet un **avis favorable** sur l'avant-projet d'arrêté du Gouvernement flamand *relatif à la politique sociale locale, mentionné aux articles 2, 9 à 11 inclus, 17, 19 et 26 du décret du 9 février 2018 relatif à la politique sociale locale*, et ce à la condition expresse que les remarques précitées soient intégrées.

L'Administrateur f.f.,

Le Président,

(sé) An Machtens

(sé) Willem Debeuckelaere