Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 32/2024 du 22 mars 2024

Objet: Demande d'avis portant sur :

- **Un avant-projet de loi relatif à la planification d'urgence et à la gestion de crise (CO-A-2024-024), et**
- **Un projet d'arrêté royal relatif à la planification d'urgence et la gestion de situations d'urgence à l'échelon communal et provincial (CO-A-2024-025)**

Mots-clés : plans d'intervention et d'urgence - système d'enregistrement des personnes impliquées et de leurs proches – portail de sécurité – missions d'intérêt public – finalités - principe de minimisation – données de santé - enregistrements audiovisuels - catégories de personnes concernées – catégories de destinataires –- consentement

Version originale

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Juline Deschuyteneer, Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye et Bart Preneel ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

Vu le 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* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis de Madame Annelies Verlinden, Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique reçue le 11 janvier 2024;

Vu les informations complémentaires transmises les 26, 28 février et 5 mars 2024 ;

émet, le 22 mars 2024, l'avis suivant :

I. POINTS D'ATTENTION PAR TYPES DE TRAITEMENT

Les remarques sont formulées ci-dessous en ordre décroissant d'importance, du 1ier au 3e type de traitement envisagé. Le système d'enregistrement des personnes impliquées et de leurs proches étant le type de traitement de données engendrant l'ingérence la plus importante pour les droits et libertés des personnes concernées, il mérite plus d'attention.

1) Système d'enregistrement des personnes impliquées et de leurs proches :

- ✓ Décrire de manière claire et exhaustive les missions d'intérêt public confiées audit système
- ✓ S'assurer du caractère complet de la définition de la notion de « personnes impliquées » et de ce que seules les personnes impliquées concernées soient clairement définies selon la finalité concrète poursuivie
- ✓ S'assurer du caractère pertinent et nécessaire de chaque catégorie de données traitées au regard de chacune des finalités poursuivies et des catégories de personnes concernées
- ✓ Renforcer la prévisibilité de la collecte des enregistrements audiovisuels et s'assurer du caractère nécessaire de ce traitement au regard de la finalité poursuivie et des catégories de personnes concernées
- ✓ Désigner les catégories de données par la/les donnée(s) qui est/seront effectivement collectée(s)
- ✓ Renforcer la prévisibilité de l'avant-projet en ce qui concerne la détermination des catégories de destinataires
- ✓ Refléter idéalement à l'article 40 la méthodologie dont il est question dans le commentaire de l'article afin de garantir un accès limité aux services compétents en fonction de leurs besoins

2) Portail de sécurité :

- ✓ Décrire de manière plus précise les missions d'intérêt public poursuivies par ledit portail
- ✓ Prévoir de manière explicite que le consentement de la personne qui se verrait ajoutée dans le portail de sécurité en vertu de l'article 40, §4, sera demandé

3) Collecte de données par les bourgmestres et gouverneurs (personnes à contacter dans les plans d'urgence et d'intervention):

- ✓ Relier les catégories de données listées à l'article 17, §1er, alinéa 2 aux catégories de personnes listées à l'article 17, §1er, alinéa 1, dans la mesure de ce qui est nécessaire à la réalisation de la finalité poursuivie
- ✓ Dans la mesure du possible préciser les catégories de destinataires visés à l'article 18

II. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. En date du 11 janvier 2024, la Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique a sollicité l'avis de l'Autorité concernant :
   - un avant-projet de loi relatif à la planification d'urgence et à la gestion de crise (ci-après « l'avant-projet »), et
   - un projet d'arrêté royal relatif à la planification d'urgence et la gestion de situations d'urgence à l'échelon communal et provincial (ci-après « le projet d'arrêté »).

2. Fort des enseignements des différentes crises auxquels la Belgique a dû faire face ces dernières années (notamment les attentats terroristes du 22 mars 2016 et la crise sanitaire du Covid-19), l'avant-projet entend créer une base juridique solide pour la planification d'urgence[1] et la gestion

[1] Il s'agit de « *l'ensemble des mesures organisationnelles, procédurales et matérielles, et d'outils contribuant à la détermination des actions et mécanismes de coordination à mettre en place lors de la survenance d'une situation d'urgence, d'un incident national ou d'une crise nationale, afin de pouvoir mobiliser dans les meilleurs délais les moyens humains et matériels nécessaires et ainsi organiser les interventions nécessaires à la protection de la population et des biens* » (voir l'article 2, 6° de l'avant-projet).
Une « situation d'urgence » est définie comme suit à l'article 2, 2° de l'avant-projet « *tout événement qui entraîne ou qui est susceptible d'entraîner des conséquences dommageables pour la vie sociale, comme un trouble grave de la sécurité publique, une menace grave contre la vie ou la santé des personnes et/ou contre des intérêts matériels importants, et qui nécessite une coordination opérationnelle et/ou une coordination stratégique, afin de faire disparaître la menace ou de limiter les conséquences néfastes de l'événement* ».
Un « incident national » est défini comme suit à l'article 2, 3° de l'avant-projet « *tout événement résultant d'activités humaines, de causes naturelles ou de causes technologiques qui ne rencontre pas les conditions pour être qualifié de crise nationale mais qui, de par sa nature ou ses conséquences, ou de par les développements qu'on peut raisonnablement en attendre :*
a) menace ou est susceptible de menacer l'intérêt général, les intérêts vitaux de la nation ou les besoins essentiels de la population, ou qui est susceptible de porter atteinte ou porte atteinte à un ou plusieurs de ces intérêts ou besoins ;
b) et requiert des décisions urgentes au niveau d'un opérateur ou d'un secteur ;
c) et est susceptible de nécessiter une coordination stratégique à l'échelon national, mais pour lequel une gestion au niveau d'un opérateur ou d'un secteur est à ce stade suffisante ».
La « crise nationale » est définie comme suit à l'article 2, 4° de l'avant-projet : « *tout événement, en ce compris les situations d'urgence, résultant d'activités humaines, de causes naturelles ou de causes technologiques qui, par sa nature ou par ses conséquences :*
a) menace ou est susceptible de menacer l'intérêt général, les intérêts vitaux de la nation ou les besoins essentiels de la population, ou qui porte atteinte ou est susceptible de porter atteinte à un ou plusieurs de ces intérêts ou besoins ;
b) et requiert des décisions urgentes ;
c) et nécessite une coordination stratégique à l'échelon national et, le cas échéant, exige une information harmonisée et cohérente de la population ».

de crise et harmoniser autant que possible la réponse aux crises, en définissant le rôle et les responsabilités des différents acteurs[2].

3. Dans ce contexte, l'avant-projet vise à préciser le cadre légal de trois types de traitements de données à caractère personnel déjà existants :

    - La collecte par les bourgmestres et gouverneurs de données relatives aux personnes à contacter reprises dans leurs plans d'urgence et d'intervention[3] et l'encodage de ces données dans le portail de sécurité visé à l'article 50 de l'avant-projet (art. 17 à 20 de l'avant-projet, examinés sous le point B ci-dessous) ;
    - La mise en place d'un système d'enregistrement des personnes impliquées[4] par une situation d'urgence et de leurs proches[5] (dit système « BITS », Belgian Incident Tracking System) (art. 35 à 40 de l'avant-projet, examinés sous le point C ci-dessous) ;
    - La mise en place d'un portail de sécurité permettant l'échange de données concernant les acteurs pertinents à contacter tant pour la planification d'urgence et le suivi de grands événements que pour la gestion d'incidents, de situations d'urgence et de crises nationales (art. 50 de l'avant-projet, examiné sous le point D ci-dessous).

4. Le projet d'arrêté entend exécuter l'avant-projet de loi et abroger l'arrêté royal du 22 mai 2019 *relatif à la planification d'urgence et la gestion de situations d'urgence à l'échelon communal et provincial et au rôle des bourgmestres et des gouverneurs de province en cas d'événements et de situations de crise nécessitant une coordination ou une gestion à l'échelon national*.

III. EXAMEN DE LA DEMANDE D'AVIS

A. Rappel des principes de prévisibilité et de nécessité

[2] Il ressort du formulaire joint à la demande d'avis qu' « *Un avis complet est demandé conformément à l'article 36, point 4 du RGPD, au vu des données à caractère personnel sensibles dont le traitement est organisé aux articles 35 à 40 (en particulier à l'article 37, §2, alinéa 2, 4° et alinéa 4, 4°) du présent avant-projet de loi* ».

[3] L'article 2, 7° de l'avant-projet définit le « plan d'urgence et d'intervention » en renvoyant à l'article 16 de l'avant-projet. En vertu de l'article 16, §1er de l'avant-projet, le bourgmestre établi pour sa commune un plan général d'urgence et d'intervention qui prévoit des directives générales et les informations nécessaires pour assurer la gestion des situations d'urgences, en ce compris les mesures à prendre et l'organisation des secours. L'article 16, §2 prévoit une disposition identique pour le gouverneur de province. En vertu de l'article 16, §3, le gouverneur et le bourgmestre peut établir un plan particulier d'urgence et d'intervention pour un risque spécifique si les directives spécifiques et les informations nécessaires pour assurer la gestion d'une situation d'urgence liée à ce risque, en ce compris les mesures à prendre et l'organisation des interventions, nécessitent soit de déroger aux principes généraux établis dans le plan général d'urgence et d'intervention soit, au regard de leurs spécificités, d'être précisées dans un plan distinct du plan général d'urgence et d'intervention.

[4] Il s'agit de « *toute personne directement ou indirectement impactée par une situation d'urgence, en ce compris les personnes décédées, blessées, non blessées, ou témoins sur les lieux* » (article 2, 5° de l'avant-projet).

[5] Il s'agit d' « *une personne qui se signale via la chaîne médico-psychosociale des secours comme ayant un lien affectif avec une ou des personnes directement impliquées dans une situation d'urgence* » (article 2, 26° de l'avant-projet)

5. L'Autorité rappelle le cadre théorique de ses observations concrètes concernant la prise en compte des principes de nécessité, de proportionnalité et de légalité en matière de droit à la protection de la vie privée et de droit à la protection des données à caractère personnels, consacrés par la Constitution, le RGPD, la CEDH et la Charte des droits fondamentaux de l'Union européenne. Le lecteur averti pourra se reporter directement à l'application de ces principes sous le titre suivant (B).

6. L'APD souligne que tout traitement de données à caractère personnel constitue une ingérence dans le droit à la protection de la vie privée, consacré à l'article 8 de la CEDH et à l'article 22 de la Constitution. Ce droit n'est toutefois pas absolu. Les articles 8 de la CEDH et 22 de la Constitution n'excluent pas toute ingérence d'une autorité publique dans le droit à la protection de la vie privée (comprenant également les données à caractère personnel), mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un intérêt social général et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit[6]. En plus de devoir être nécessaire et proportionnée, toute norme régissant le traitement de données à caractère personnel (et constituant par nature une ingérence dans le droit à la protection des données à caractère personnel) doit répondre aux exigences de prévisibilité et de précision afin que les personnes concernées au sujet desquelles des données sont traitées aient une idée claire du traitement de leurs données.

7. Conformément à l'article 6.3 du RGPD, lu à la lumière du considérant 41 du RGPD, le traitement de données à caractère personnel qui est nécessaire au respect d'une obligation légale[7] ou 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[8] doit être régi par une réglementation claire et précise dont l'application doit être prévisible pour les personnes concernées. En outre, selon l'article 22 de la Constitution, il est nécessaire que les « éléments essentiels » du traitement de données soient définis au moyen d'une norme légale formelle. Dans ce cadre, il s'agit au moins :
   - de la (des) finalité(s) précise(s) et concrète(s) des traitements de données ;
   - de la désignation du (des) responsable(s) du traitement (à moins que cela ne soit clair).

   Toutefois, si l'ingérence de l'autorité publique représente une ingérence importante dans les droits et libertés des personnes concernées, ce qui est le cas en l'occurrence[9], la norme légale doit également définir les éléments essentiels (complémentaires) suivants:

[6] Jurisprudence constante de la Cour constitutionnelle. Voir par ex. Cour Constitutionnelle, Arrêt du 4 avril 2019, n° 49/2019 (« *Ils n'excluent pas toute ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée mais exigent que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit* »)

[7] Article 6.1.c) du RGPD.

[8] Article 6.1.e) du RGPD.

[9] Le demandeur indique lui-même dans le formulaire joint à la demande d'avis que l'avant-projet constitue un traitement qui porte sur des catégories particulières de données à caractère personnel de personnes vulnérables ; que le traitement implique un croisement ou une combinaison de données à caractère personnel provenant de différentes sources ; que le traitement est

- les (catégories de) données à caractère personnel traitées qui sont pertinentes et non excessives ;
- les (catégories de) personnes concernées dont les données à caractère personnel seront traitées ;
- les (catégories de) destinataires des données à caractère personnel ainsi que les conditions dans lesquelles ils reçoivent les données et les motifs y afférents ;
- le délai de conservation maximal des données à caractère personnel enregistrées ;
- l'éventuelle limitation des obligations et/ou droits mentionné(e)s aux articles 5, 12 à 22 et 34 du RGPD.

8. Cela n'empêche évidemment pas que, pour autant que les éléments essentiels des traitements de données à caractère personnel envisagés soient définis dans l'avant-projet, des modalités d'exécution plus détaillées puissent être laissées au Roi[10], certes, après avis complémentaire de l'Autorité, conformément à l'article 36.4 du RGPD.

B. Collecte des données par les bourgmestres et gouverneurs et encodage de ces données dans le portail de sécurité (art. 17 à 20 de l'avant-projet)

9. Les articles 17 à 20 de l'avant-projet encadrent la collecte des données à caractère personnel effectués par les bourgmestres et gouverneurs, qui sont chargés d'élaborer leurs plan d'urgence et d'intervention, de les actualiser et de les mettre en œuvre lors des situations d'urgence, ainsi que l'encodage desdites données dans le portail de sécurité visé à l'article 50 de l'avant-projet lorsqu'elles sont contenues dans lesdits plans d'urgence et d'intervention.

1) Prévisibilité et finalités

10. Rappel théorique : la finalité d'un traitement de données à caractère personnel étant un élément essentiel de ce traitement, elle doit être formulée de manière suffisamment précise dans la loi pour répondre à l'exigence de prévisibilité rappelée ci-dessus quant à la raison concrète et opérationnelle pour laquelle ces données sont traitées (article 5.1.b) du RGPD).

11. Il ressort de l'article 17, §1er de l'avant-projet que la finalité poursuivie par la collecte des catégories de données qui y sont listées est de permettre aux bourgmestres et gouverneurs d'élaborer leurs plans d'urgence et d'intervention, de les actualiser et de les mettre en œuvre lors

effectué à grande échelle en raison d'un volume important de données et/ou du nombre de personnes concernées ; que les données sont communiquées ou accessibles à un tiers.

[10] Comme le prévoit notamment l'article 17, §1er, alinéa 2 ainsi que l'article 50, §§2 à 4, alinéa 2 de l'avant-projet.

de situation d'urgence. Ces finalités sont exprimées de manière suffisamment claires dans le projet, à la lumière des considérants.

12. Certes, la définition du plan général d'urgence et d'intervention ainsi que celle du plan particulier d'urgence et d'intervention[11], ne se réfère pas explicitement au fait que ces plans contiennent des données à caractère personnel des personnes à contacter lors de situation d'urgence.

13. Il ressort du commentaire de l'article 17 que « *l'objectif majeur* » des plans d'urgence et d'intervention, justifiant la collecte de données en cause est de « *permettre aux autorités et aux services d'intervention de mobiliser rapidement du personnel et du matériel lors de la survenance d'une situation d'urgence afin de protéger la vie et l'intégrité physique et mentale des personnes et bien impliqués* ». Il s'ensuit que la finalité relative à la mise en œuvre des plans d'urgence et d'intervention lors de situation d'urgence est exprimée suffisamment clairement.

14. **Remarque mineure de formulation :** La **détermination du champ d'application *ratione personae*** de l'article 17 de l'avant-projet **participe également à la délimitation de la finalité** du traitement. Il importe donc de veiller à ce que les catégories de personnes dont les catégories de données seront mentionnées dans les plans d'urgence et d'intervention soient désignées en des termes suffisamment clairs et précis. Ainsi, la catégorie de personnes visée au point 2° entend se référer, selon le commentaire de l'article 17, aux gestionnaires de réseau de gaz, d'électricité ou d'eau, les exploitants des barrages ou d'établissements Seveso[12]. Il s'agit donc de personnes responsables auprès d'organismes, d'entreprises ou d'établissements qui en raison de leur localisation ou de leurs activités sont susceptibles d'être à l'origine d'une situation d'urgence ou d'aggraver ses conséquences dommageables. Or, la formulation laisse supposer que c'est la localisation ou les activités des personnes visées (et non des organismes, entreprises ou établissements auprès desquelles ces personnes travaillent) qui sont susceptibles d'être à l'origine d'une situation d'urgence ou d'aggraver ses conséquences dommageables. La formulation gagnerait en clarté s'il était précisé qu'il s'agit des « personnes qui en raison de la localisation ou des activités des organismes, entreprises ou établissements dont elles sont employées ou prestataires », De même, la catégorie de personnes visée au point 3° entend se référer, selon le commentaire de l'article 17, aux responsables de certaines institutions qui doivent être avertis de la prise de certaines mesures dans le cadre de la gestion d'une situation d'urgence, telles que les écoles, maisons de repos ou centre de soins qui abritent des personnes à laquelle une attention particulière devra être portée notamment lors de la prise de mesures telles qu'une évacuation ou

[11] Voir la note de bas de page numéro 2.

[12] Selon le site Internet du Centre de crise National (https://centredecrise.be/fr/risques-en-belgique/risques-technologiques/seveso), les entreprises Seveso sont des entreprises qui produisent, transforment, traitent ou stockent des substances dangereuses, par exemple les raffineries, les usines pétrochimiques, les usines chimiques, les dépôts de pétrole ou les sites de stockage de substances explosives.

un confinement. A nouveau, l'intention de l'avant-projet est de mentionner dans les plans d'urgence des personnes qui sont responsables auprès d'établissements ou d'institutions qui en raison de leur localisation ou de leurs activités sont particulièrement exposées aux conséquences dommageables d'une situation d'urgence. **Le champ d'application *ratione personae* gagnerait dès lors être à être revu et précisé** à la lumière de ces observations.

15. Il y a lieu de relever également que, selon le commentaire de l'article 17 de l'avant-projet, la **finalité relative à la prise de contact rapide avec les personnes mentionnées dans les plans d'urgence et d'intervention lors de situation d'urgence** est une finalité qui peut être considérée comme une finalité qui **se décline en sous-finalité en fonction de la catégorie de personnes visées**. En effet, ainsi que cela ressort du commentaire de l'article 17, les personnes visées au point 1° sont des personnes à contacter dans le cadre de la gestion d'une situation d'urgence et « *pouvant, le cas échéant, participer à une structure de coordination mise en place pour la gestion des situations d'urgence* ». Les personnes visées au point 2° sont des personnes à *« mobiliser afin de les associer aux travaux de gestion de crise ou de rapidement pouvoir les contacter pour prendre des mesures adéquates* ». Les personnes visées au point 3° sont des personnes qui « *doivent être averties de la prise de certaines mesures dans le cadre de la gestion d'une situation d'urgence* » eu égard au fait qu'une « *attention particulière* » devra leur être portée notamment lors de la « *prise de mesures telles qu'une évacuation ou un confinement* ». Ces sous-finalités opérationnelles sont suffisamment exprimées à travers l'exposé des motifs.

2) Principe de minimisation des données

16. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (principe de « minimisation des données »).

17. **L'article 17, §1er, alinéa 2**, de l'avant-projet liste les catégories de données à caractère personnel qui peuvent être traitées par les bourgmestres et gouverneurs comme suit (sans les relier aux catégories de personnes concernées visées à l'article 17, §1er, alinéa 1) :

« *1° les données d'identification personnelles ;*
2° les mandats publics détenus ;
3° les qualifications professionnelles ;
4° l'expérience professionnelle ;
5° l'emploi actuel ».

18. **L'article 17, §1er, alinéa 3** confère au Roi la compétence de préciser ces catégories de données à caractère personnel, sans pouvoir les étendre.

19. Le principe de prévisibilité exige que la loi offre au bénéfice des personnes concernées une description suffisamment claire et prévisible des catégories de données les concernant qui vont être collectées, avec pour chaque catégorie un lien clair avec les finalités de traitement envisagées, tout en respectant le principe de minimisation juste rappelé. Il revient dès lors au demandeur de revoir l'avant-projet afin de veiller à ce que **les catégorie(s) de données listées à l'article 17, §1er, alinéa 2 de l'avant-projet soient reliées aux catégories de personnes listées à l'article 17, §1er, alinéa 1, dans la mesure de ce qui est nécessaire à la réalisation de la finalité poursuivie.**

20. En ce qui concerne la délégation au Roi pour préciser les catégories de données listées à l'article 17, §1er, alinéa 2 de l'avant-projet, l'Autorité relève que, dans le cas d'espèce, les données minimales à collecter, visées aux articles 8 et 9 du projet d'arrêté, sont gages de prévisibilité et de proportionnalité au regard de la finalité poursuivie (à savoir l'élaboration de plans d'urgence et d'intervention et leur mise en œuvre lors de situation d'urgence), laquelle implique par nature qu'une marge de manœuvre soit accordée. Cela étant, tout traitement de données se doit de répondre au principe de minimisation consacré à l'article 5.1.c) du RGPD, ce qui implique que si dans un cas concret une donnée supplémentaire n'ayant pu être anticipée par le législateur venait à être collectée, il appartient au responsable du traitement de s'assurer de son caractère nécessaire et proportionné. Il convient de constater que les catégories de personnes mentionnées à l'article 8 du projet d'arrêté ne semble pas correspondre aux catégories de personnes listées à l'article 17, §1er, alinéa 1 de l'avant-projet. Il convient de **remédier à cette discordance** afin d'assurer un niveau adéquat de prévisibilité.

3) Mise à jour des données (art. 17, §3 de l'avant-projet)

21. **L'article 17, §3** de l'avant-projet prévoit que lorsque les données à caractère personnel visées à l'article 17, §1er, sont modifiées dans les plans d'urgence et d'intervention, les bourgmestres et gouverneurs mettent à jour ces données sur le portail de sécurité dans les trente jours de cette modification.

22. Interrogé quant au caractère nécessaire du délai de 30 jours à des fins de mises à jour, le fonctionnaire délégué a répondu ce qui suit :
« *Ce délai tient compte du fait que toutes les communes ne travaillent pas uniquement ou même principalement « en ligne », sur le portail de sécurité. Les bourgmestres et gouverneurs ont le droit de travailler « hors ligne », de manière déconnectée du portail de sécurité, c'est-à-dire*

d'élaborer et de mettre à jour ses plans d'urgence et d'intervention en dehors du portail de sécurité. Si par exemple un bourgmestre décide de premièrement mettre à jour ses plans d'urgence et d'intervention en dehors du portail de sécurité, ce délai de trente jours lui permettra de mettre à jour dans un délai raisonnable ses plans d'urgence et d'intervention se trouvant sur le portail de sécurité. L'objectif est que les bourgmestres et gouverneurs mettent aussi vite que possible ces données à jour, néanmoins un délai de 30 jours a été fixé afin de laisser un laps de temps suffisant aux services fédéraux auprès des Gouverneurs, ainsi qu'aux bourgmestres et leurs équipes, travaillant souvent en sous-effectifs, pour effectuer les ajouts ou modifications dans le portail de sécurité. »

23. Si l'Autorité comprend la nécessité de laisser un délai aux communes et aux provinces qui ne travaillent pas « en ligne » sur le portail de sécurité, afin de leur permettre de mettre à jour leurs plans d'urgence et d'intervention, il convient de rappeler le principe d'exactitude consacré à l'article 5.1.d) du RGPD qui requiert que toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder. Dans le contexte précité, l'Autorité recommande de veiller à ce que le responsable du traitement insère une information appropriée à l'attention de tout utilisateur du portail de sécurité afin d'attirer l'attention sur le caractère potentiellement non mis à jour des données figurant sur ledit portail (mise à jour en deçà d'un délai de trente jours).

4) Destinataires des données (art. 18 de l'avant-projet)

24. **L'article 18** de l'avant-projet prévoit que les bourgmestres et gouverneurs peuvent donner accès aux données comprises dans les catégories de données listées à l'article 17, aux « *autorités et services* » qui y sont énumérés, « *dont la mission d'intérêt public consiste en la gestion de situations d'urgence, dans les limites de ce qui est nécessaire à l'exécution de celle-ci* », à savoir « *les services opérationnels et stratégiques* » ; « *les autorités concernées* » ; « *les services spécialisés* » et « *les centres d'informations* ».

25. Eu égard à la désignation de chaque catégorie de destinataire en des termes relativement généraux, le demandeur a été interrogé quant à la portée concrète de chacune de ces catégories. Il a été répondu qu' « *il n'est pas possible d'énumérer exhaustivement tous les destinataires se trouvant sous une catégorie, sous risque d'oublier un destinataire* » et que « *compte tenu de la nature évolutive des partenaires, il a été décidé de ne pas les énumérer individuellement* ».

26. L'Autorité attire l'attention du demandeur sur le fait que, conformément au principe de minimisation (qui est une expression du principe de proportionnalité), l'accès et la consultation des données à caractère personnel reprises dans le portail de sécurité doivent être strictement

limités aux personnes compétentes qui sont habilitées, en vertu de leurs fonctions/missions ou en vertu de critères desquels ils résultent la nécessité d'avoir accès aux données concernées, à contacter les personnes y mentionnées afin de les mobiliser le plus rapidement possible et de gérer la situation d'urgence.

27. Partant, **dans la mesure du possible,** l'Autorité invite le demandeur à **renforcer la prévisibilité de l'avant-projet en précisant les catégories de destinataires** visées par les expressions « services opérationnels et stratégiques »[13], « autorités concernées »[14], « services spécialisés » et « centres d'information », soit en définissant ces expressions dans l'avant-projet soit en désignant les destinataires qui sont concrètement visés par une formulation plus précise.

28. Il ressort des informations complémentaires que cet accès sera effectué via le portail de sécurité visé à l'article 50 de l'avant-projet. Afin d'améliorer la prévisibilité de l'article 18 de l'avant-projet, il convient de **compléter** cette disposition en ce sens.

C. Système d'enregistrement es des personnes impliquées par des situations d'urgence et de leurs proches (art. 35 à 40 de l'avant-projet)

1) Prévisibilité et finalités

29. **L'article 35** de l'avant-projet créé un système d'enregistrement des personnes impliquées par une situation d'urgence et de leurs proches, dont le SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement (ci-après le « SPF Santé publique ») assure le développement, la gestion, le fonctionnement et la mise à disposition de ces partenaires et des entités fédérées. Il est précisé que cette mise à disposition est effectuée en vue du partage des données avec les services visés à l'article 38 de l'avant-projet. L'article 36 prévoit que, lors d'une situation d'urgence[15], les services visés audit article, à savoir les services d'intervention concernant les secours médicaux, sanitaires et psychosociaux (ci-après les « services de secours visés à l'article 36 »), sont chargés d'établir et de gérer les listes des personnes impliquées dans la situation d'urgence et de leur proches et ce, uniquement pour les finalités visées à l'article 37, §2.

---

[13] Il ressort des informations complémentaires que sont visés les services d'intervention visés à l'article 10 de l'avant-projet qui sont répartis en 5 disciplines : discipline 1 qui concerne les opérations de secours ; discipline 2 qui concerne les secours médicaux, sanitaires et psychosociaux, discipline 3 qui concerne la police du lieu de la situation d'urgence ; discipline 4 qui concerne l'appui logistique ; discipline 5 qui concerne l'alerte et l'information de la population. Ainsi, à titre d'exemple, les « services opérationnels et stratégiques » pourraient être définis par référence aux services d'intervention visés à l'article 10 de l'avant-projet.

[14] Dans le même ordre d'idées, il ressort des informations complémentaires qu'il s'agit d'autorités relevant du niveau communal, provincial, régional et fédéral. Cela devrait être précisé dans l'avant-projet.

[15] Suite aux informations complémentaires transmises, l'Autorité comprend que la référence à une « *situation d'urgence collective* » faite dans le commentaire de l'article 37 de l'avant-projet vise la situation d'urgence, telle que définie à l'article 2,2° de l'avant-projet et que le terme « collective » sera donc supprimé du commentaire afin d'éviter toute confusion à cet égard.

30. Dans la mesure où la base de licéité des traitements de données à caractère personnel effectués par le biais du système d'enregistrement visé est l'article 6.1.e) du RGPD, les finalités desdits traitements ne peuvent être réalisées que dans la mesure nécessaire à l'exécution des missions d'intérêt public incombant au SPF Santé publique, en tant que responsable du traitement,[16] en vertu de l'avant-projet. C'est pourquoi, l'avant-projet doit **déterminer de manière suffisamment claire et précise les missions d'intérêt public dont est investi le SPF Santé publique/le système d'enregistrement visé** pour assurer la licéité des traitements de données envisagés.

31. A la lumière des informations complémentaires[17] [18] , l'Autorité comprend que l'avant-projet entend, en substance, encadrer des traitements de données à caractère personnel nécessaires à la réalisation des missions d'intérêt public suivantes :
    - La coordination et la réorientation de l'aide medico-psychosociale afin d'offrir aux personnes impliquées et aux proches une aide rapide, adéquate et de qualité ;
    - L'information des proches qui sont à la recherche de personnes impliquées dans une situation d'urgence sur le lieu où se trouve ces personnes ;
    - La facilitation du processus d'identification des personnes blessées et décédées ;

---

[16] Voir l'article 39 de l'avant-projet.

[17] Interrogé quant aux objectifs poursuivis par le système d'enregistrement tel que crée par l'article 35 de l'avant-projet, le demandeur a indiqué que le système d'enregistrement est développé en fonction des objectifs suivants :

- « *Het coördineren en bijsturen van de medisch- psychosociale hulpverlening om de beschreven doelgroepen snelle, adequate en kwalitatieve hulpverlening aan te bieden. In de lijn hiervan het verbeteren van de hulpverlening op langere termijn;*
- *Het informeren van verwanten over de locatie van getroffenen die zelf niet in staat zijn om hun verwanten te informeren. Met als doel het herenigen van getroffenen met hun verwanten;*
- *Het faciliteren van identificatie processen van (onbewuste) getroffenen en overledenen;*
- *Het Informeren van de bevoegde overheidsinstanties en diensten betrokken bij de rampenhulpverlening – ter ondersteuning van taken die men moet uitvoeren;*
- *Verzamelen van gegevens noodzakelijk voor de organisatie van de hulpverlening in navolging van de noodsituatie (nafase of herstel) – in samenwerking met de bevoegde partners;*
- *De ontwikkeling van een systeem dat het mogelijk maakt om gegevens uit te wisselen op een manier die tegemoet komt aan de regelgeving, waaronder AVG;*
- *Het ondersteunen dat getroffenen hun rechten als slachtoffer kunnen uitoefenen, binnen de context van de rechtspositie van slachtoffers die schade hebben geleden ten gevolg van ofwel een burgerrechtelijke incident, bv. een natuurramp, ofwel een misdrijf, bv. Een terroristische aanslag, overeenkomstig Europese of Belgische wetgeving.*»

[18] Interrogé sur l'interaction entre le système d'enregistrement visé à l'article 35 de l'avant-projet et les listes des personnes impliquées et de leur proches établies par les services visés à l'article 36 de l'avant-projet, il a été répondu que :

« *De diensten die instaan voor de verwerking van persoonsgegevens, bedoeld in artikel 36, voorzien deze verwerking in het registratiesysteem besproken in artikel 35. Het betreft dus een gecentraliseerde verwerking van de lijsten van getroffenen die bij de noodsituatie betrokken zijn en hun verwanten binnen dit registratiesysteem.*

Een belangrijk principe van het Belgian Incident Tracking Systeem (hierna "BITS") is dat gegevens over getroffenen en verwanten worden gecentraliseerd om zo te voorkomen dat er dubbele, onjuiste en onvolledige lijsten ontstaan. Het uitgangspunt is één dossier dat bestaat voor elke unieke persoon in het programma. Dit wordt bekomen door de bevestiging van een polsband met unieke code op het moment dat de getroffene in contact komt met een hulpverlener op het rampterrein. […]

Dit "dossier" van gegevens wordt dus aangevuld vanuit verschillende locaties. Dit heeft tot gevolg dat alle deelnemende diensten van Discipline 2 mogelijk een verwerking zullen doen van bepaalde gegevens uit het dossier. Alle diensten uit Discipline 2, zowel het medisch luik (medisch interventieplan) als het psychosociaal luik (psychosociaal interventieplan), komen in contact met de getroffenen. Al deze diensten zullen bijdragen en zorgen dat er gegevens worden geregistreerd om getroffenen zo snel mogelijk te lokaliseren, traceren en identificeren.

[…].»

- L'information des autorités compétentes et des services concernés par la situation d'urgence afin de soutenir les tâches qui doivent être réalisées ;
- Le soutien des personnes impliquées d'exercer leurs droits en tant que victimes.

Elle comprend également que les traitements de données envisagés aux fins de l'exécution de ces missions d'intérêt public sont en substances les suivants :

- la collecte et l'enregistrement de données de chaque personne impliquée sur le lieu de la situation d'urgence dès qu'elle est en contact avec un des services de secours visés à l'article 36 en vue de constituer un dossier concernant cette personne ;
- l'établissement des listes des personnes impliquées et des proches par les services de secours visés à l'article 36 et la centralisation de ces listes ;
- la consultation des dossiers et des listes par les utilisateurs du système d'enregistrement dans la limite de leurs compétences ;
- la communication de données à des destinataires.

32. Dans ces conditions, afin d'améliorer la prévisibilité des traitements de données à caractère personnel engendrés par le système d'enregistrement visé, il convient de **revoir l'article 35** de l'avant-projet à la lumière des observations émises ci-dessus. Cela implique, en l'occurrence, de **décrire de manière claire et exhaustive dans l'avant-projet les missions d'intérêt public confiées audit système d'enregistrement/au SPF Santé publique** (et desquels découlent en principe les finalités desdits traitements de données), **et de s'assurer que chacun des traitements de données susmentionnés (et leurs éléments essentiels) y soit prévu de manière claire**.

33. A cet égard, il convient encore de relever que prévoir à l'article 35 que le système d'enregistrement est « *mis à disposition* » des « *partenaires* » du SPF Santé publique ne peut pas être considéré comme répondant à l'exigence de prévisibilité dans la mesure où l'avant-projet ne définit pas ce qu'il y a lieu d'entendre par « partenaires ». De même, indiquer que la « *mise à disposition est effectuée en vue du partage des données avec les services visés à l'article 38* » peut être interprétée comme ne permettant une communication des données enregistrées dans le système visé qu'avec les services visés audit article 38. Or, tel ne semble pas être le cas du système visé puisqu'il entend également permettre la consultation des données par les utilisateurs du système, à savoir les services de secours visés à l'article 36.

34. L'Autorité constate qu'en vertu de l'article 36 de l'avant-projet, les services de secours y visés sont désignés en tant que sous-traitant qui traitent les données à caractère personnel au nom du SPF Santé publique. L'Autorité en profite pour rappeler que la désignation des responsables du

traitement doit être adéquate au regard des circonstances factuelles[19]. En d'autres termes, il est nécessaire de vérifier pour chaque traitement de données à caractère personnel qui, *dans les faits*, poursuit la finalité du traitement et dispose de la maitrise du traitement. En l'occurrence, l'Autorité se demande si les services visés peuvent être considérés comme des sous-traitants à la lumière, notamment de l'article 38, §§ 2 et 3 de l'avant-projet qui prévoit qu'il revient auxdits services de pouvoir accorder l'accès aux données aux destinataires qui y sont mentionnés. Le demandeur est dès lors invité à **revoir l'article 36** à la lumière de cette observation.

35. Il y a encore lieu de rappeler que si la désignation des services de secours visés à l'article 36 en tant que sous-traitant est maintenue, il incombe au SPF Santé publique de conclure un contrat de sous-traitance (article 28 du RGPD) et attire l'attention du demandeur quant à la responsabilité du responsable du traitement en matière de sélection de son/ses sous-traitant(s) et de contrôle de ses opérations ainsi que quant à la responsabilité qui lui incombe en cas de défaillance.

2) Etablissement et gestion des listes des personnes impliquées et de leurs proches

36. **L'article 37** de l'avant-projet liste en son **paragraphe 1er**, les catégories de personnes concernées par l'établissement et la gestion des listes des personnes impliquées et de leurs proches réalisés par les services de secours visés à l'article 36. Le **paragraphe 2** dudit article 37 énumère les catégories de données à caractère personnel des catégories de personnes visées au paragraphe 1er qui sont traitées pour chacune des quatre finalités poursuivies par l'établissement et la gestion desdites listes.

37. Dans la mesure où la détermination du champ d'application *ratione personae* d'une finalité participe à la détermination de ladite finalité, il revient au demandeur de **s'assurer du caractère complet de la définition de la notion de « personnes impliquées ».** Ainsi, les personnes impliquées sont définies à l'article 2,5° de l'avant-projet comme étant « *toute personne directement ou indirectement impactée par une situation d'urgence, en ce compris les personnes décédées, blessées, non blessées ou témoins sur les lieux* ». L'Autorité se demande si cette définition est complète dans la mesure où l'article 37, §1, liste en tant que personnes impliquées également les « *personnes impliquées disparues dont les données sont collectées auprès des proches* ». De plus, il revient au demandeur de **veiller à ce que seules les personnes**

[19] En effet, tant le Comité européen à la protection des données que l'Autorité insiste sur la nécessité d'approcher le concept de responsable du traitement dans une perspective factuelle. Voir : Comité européen à la protection des données, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, adopted on 02 september 2020, p 10 et s (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en) et Autorité de protection des données, *Le point sur les notions de responsable de traitement/sous-traitant au regard du au regard du Règlement EU 2016/679 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats*, p.1. https://www.autoriteprotectiondonnees.be/publications/notions-de-responsable-de-traitement-sous-traitant-au-regard-du-reglement-eu-2016-679.pdf

impliquées concernées soient clairement définies selon la finalité concrète poursuivie. Ainsi, en ce qui concerne la finalité visée à l'article 37, §2, alinéa 3 relative au soutien du processus d'identification des personnes impliquées à identifier, il ressort du commentaire de l'article que ne sont visées que les personnes impliquées gravement blessées ou décédées (à l'exclusion donc des personnes non-blessées ou disparues).

38. **Suggestion mineure de reformulation : L'article 37, §2, alinéa 2**, de l'avant-projet mentionne les catégories de données à caractère personnel collectées par les services visés à l'article 36 « *afin d'assurer la chaîne médico-psychosociale des secours* ». Il ressort du commentaire de l'article[20] ainsi que des informations complémentaires[21] qu'il s'agit concrètement **d'assurer l'organisation et l'optimalisation de l'assistance/l'aide médico-psychosociale des services de secours en fonction des besoins, tels qu'ils ressortent du système d'enregistrement.** Afin de renforcer la prévisibilité de l'avant-projet, il est loisible au demandeur de **revoir la formulation de la finalité** visée à l'article 37, §2, alinéa 2 en ce sens.

39. En ce qui concerne les catégories de données à caractère personnel collectées pour chacune des finalités visées, il convient de rappeler qu'en vertu du principe de minimisation, seules peuvent être traitées des données pertinentes, adéquates et limitées à ce qui est nécessaire au regard de la finalité visée. Il revient au demandeur de **s'assurer du caractère nécessaire et pertinent de chaque catégorie de données traitées au regard de la finalité poursuivie et des catégories de personnes concernées (personnes impliquées et/ou proches) et de le justifier le cas échéant dans le commentaire de l'article**.

40. L'Autorité suppose que par « *données d'identification personnelles des personnes impliquées et de leurs proches* » (art. 37, §2, alinéas 1 à 4), il convient d'entendre les nom et prénom des personnes concernées. Il conviendrait de le **préciser** dans l'avant-projet à des fins de prévisibilité dans la mesure où il n'y a pas de délégation conférée au Roi pour préciser dans une norme réglementaire les données à caractère personnel visées par cette catégorie de données. Si les **données de contact** sont visées par cette catégorie de données, il convient d'établir la distinction dans l'avant-projet.

---

[20] « *Les services participant à la mise en oeuvre du plan monodisciplinaire d'intervention de la discipline 2 traitent des données à caractère personnel afin de pouvoir fournir les informations nécessaires pour ajuster l'assistance en fonction des besoins.* »

[21] « *De doelstelling hier is de organisatie van de medisch-psychosociale hulpverleningsketen afstemmen en optimaliseren door rekening te houden met de output van het registratiesysteem. Zijn er bijvoorbeeld nog een groot aantal gewonden geregistreerd op het registratiepunt vooruitgeschoven medische post, dan weten we dat er nog heel wat medische transportmiddelen ter beschikking dienen te zijn. Het aantal geregistreerde betrokkenen en verwanten op het registratiepunt onthaalcentrum, geef ons inzicht in de hoeveelheid catering, personeel, hulpmiddelen die we dienen te voorzien gedurende de eerstvolgende periode.* […] »

41. En ce qui concerne la catégorie de données relative aux « *détails personnels des personnes impliquées et de leurs proches* » (art. 37, §2, alinéas 1 à 4), il ressort du commentaire de l'article que les données visées sont notamment l'âge, le sexe, la date de naissance, le lieu de naissance, l'état civil et la nationalité. Si ces données peuvent être pertinentes et nécessaires pour ce qui concerne les personnes impliquées, l'Autorité doute que tel soit le cas pour les proches. Le demandeur est dès lors invité à **distinguer dans le dispositif de l'avant-projet les données nécessaires et pertinentes selon les catégories de personnes concernées** (personnes impliquées/proches) **au regard de la finalité qui est poursuivie** et de **justifier dans l'exposé des motifs en quoi chaque donnée visée est nécessaire et pertinente au regard de la finalité poursuivie**.

42. En ce qui concerne les « *données de localisation des personnes impliquées et de leurs proches* » (art. 37, §2, alinéa 1, 3°), il ressort des informations complémentaires qu'il s'agit des données relatives au lieu où se trouve la personne impliquée recherchée, à savoir le lieu de l'incident, le poste médical avancé, l'hôpital ou le centre d'accueil. L'expression « *données de localisation* » étant en principe utilisée pour se référer à la position géographique à un moment donné d'une personne émise grâce à un appareil électronique, il parait **plus approprié** -pour éviter toute ambiguïté- **de se référer en l'occurrence au lieu** où se trouve la personne recherchée ou de préciser cette notion dans l'exposé des motifs. L'Autorité comprend tout à fait le caractère nécessaire et pertinent de cette catégorie de donnée au regard de la finalité en ce qui concerne les personnes impliquées, et suppose, en ce qui concerne les proches, qu'il s'agit de permettre de les « réunir » dans le cadre de l'incident/la catastrophe. Ce point n'appelle donc pas plus de commentaire.

43. En ce qui concerne « *la composition de ménage et le lien des personnes impliquées avec leurs proches* » (art. 37, §2, alinéas 1 et 3), le commentaire de l'article expose que ces données sont « *utiles*[22] *pour déterminer le proche (au sens large tel que défini dans la loi, c'est-à-dire au sein ou en dehors du ménage) ayant le lien le plus étroit avec la personne impliquée disparue* ». Il s'ensuit que la composition de ménage ne sera pas une donnée systématiquement nécessaire afin de définir la relation étroite entre la personne impliquée disparue et le proche qui la recherche. Afin d'éviter de bloquer inutilement le processus de réunion des personnes concernées, en fonction de l'expérience de terrain du demandeur, il y a dès lors lieu **d'envisager une adaptation de** l'article 37, §2, alinéas 1 et 3, en **précisant** que la composition de ménage **sera collectée « le cas échéant et si nécessaire », tout en explicitant dans l'exposé des motifs les cas où une telle demande pourrait être nécessaires au regard de la finalité poursuivie** (réunir

[22] Afin de répondre pleinement au principe de minimisation, il convient de remplacer ce terme par celui de « nécessaire ».

les proches avec les personnes impliquées ou soutenir le processus d'identification des personnes impliquées à identifiées)**,** afin d'améliorer la prévisibilité de l'avant-projet.

44. En ce qui concerne les « *habitudes de vie des personnes impliquées et de leurs proches* » (art. 37, §2, alinéas 1, 2 et 4), il ressort du commentaire de l'article qu'est visé la langue et qu' elle « *peut ainsi être déterminée afin de trouver un interprète ou de rendre compréhensible les informations mises à disposition après la phase aiguë dans le cadre d'une correspondance ou d'un contact. Cela permet d'offrir une assistance aux personnes impliquées et aux proches dans une langue qu'ils maîtrisent. Cela contribue à l'accessibilité de l'aide*. » L'expression « habitudes de vie » étant large, il convient de **remplacer cette expression par ce qui est concrètement visé** en l'espèce, à savoir la **langue**, afin d'améliorer la prévisibilité de l'avant-projet et d'éviter d'exposer les personnes concernées à la collecte de données disproportionnées au regard de la finalité visée.

45. En ce qui concerne la collecte de données de santé des personnes impliquées (art. 37, §2, alinéas 2 et 4) , il y a lieu de rappeler que, en plus d'être fondée sur une base de licéité au sens de l'article 6.1. du RGPD, celle-ci doit relever de l'une des dix exemptions prévues à l'article 9.2[23] et, le cas échéant, être assortie de mesures spécifiques et appropriées nécessaires. Parmi ces mesures, l'Autorité relève que l'article 9.3 du RGPD - pour autant que la collecte en cause puisse être fondée sur l'article 9.2.h) du RGPD (traitement nécessaire aux fins de la prise en charge sanitaire ou sociale) – prévoit que les données concernées ne peuvent être traitées que notamment par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit applicable, ou par une autre personne également soumise à une obligation de secret conformément au droit applicable. De plus, en exécution de l'article 9.4 du RGPD, l'article 9, 1° de la LTD prévoit notamment que « *les catégories de personnes ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées* ». En outre, eu égard à l'importance de l'ingérence engendrée par le traitement de cette catégorie particulière de données au sens de l'article 9 du RGPD dans les droits et libertés des personnes concernées, l'Autorité accueille favorablement l'approche de l'avant-projet visant à limiter ce type de traitement de données à ce qui est nécessaire au suivi de l'état de santé des personnes impliquées durant la situation d'urgence. L'Autorité prend bonne note et accueille favorablement également le commentaire de l'article qui ajoute que cela doit être **nécessaire également à l'évaluation de l'état de santé** des personnes impliquées.

[23] Voy. GEORGIEVA, L. et KUNER, C., "Article 9. Processing of special categories of personal data" in KUNER, C., BYGRAVE, L.A. and DOCKSEY, C., The EU General Data Protection Regulation (GDPR). A Commentary, Oxford University Press, Oxford, p. 37; voy. également la décision quant au fond n°76/2021, point 33.

46. En ce qui concerne la collecte d' « *enregistrements audiovisuels qui permettent d'identifier les personnes impliquées* » par les services de secours visés à l'article 36 (art. 37, §2, alinéa 2, 5°), l'Autorité estime qu'il convient de **clarifier la finalité concrète** qui est poursuivie par le traitement de ces enregistrements audiovisuels dans la mesure où la formulation porte quelque peu à confusion. En effet, s'il s'agit d'identifier les personnes impliquées, il convient de supprimer cette catégorie de données puisqu'elle n'est pas pertinente ni nécessaire afin de d'assurer l'organisation et l'optimalisation de l'assistance/l'aide médico-psychosociale des secours en fonction des besoins. Si, en revanche, il s'agit d'une donnée nécessaire et pertinente afin de réaliser la finalité juste précitée – ainsi que cela semble ressortir des informations complémentaires[24]- , il convient alors de clarifier le libellé de l'article 37, §2, alinéa 2, 5° en ce sens, en veillant à ce que soient visées uniquement les personnes impliquées (gravement) blessées (à l'exclusion donc des personnes décédées, non blessées, disparues). En outre, l'Autorité comprend que **cet enregistrement audiovisuel ne sera effectué que dans la mesure de ce qui est strictement nécessaire au suivi médical de la personne impliquée.** Il convient d'**adapter** l'avant-projet afin de clarifier la finalité.

47. En ce qui concerne les « *enregistrements audiovisuels des personnes impliquées* » par les services de secours visés à l'article 36 (art. 37, §2, alinéa 3, 3°), le commentaire de l'article mentionne des photos ainsi que des enregistrements vidéos ou sonores.

48. Interrogée quant au caractère nécessaire et proportionné de la collecte de cette catégorie de données au regard de la finalité d'identification visée, le demandeur a répondu ce qui suit :

> « *Audiovisueel materiaal is een belangrijk instrument om identificatieprocessen op te starten. Dit geef een eerste noodzakelijke indicatie van welke persoon dit mogelijks zou kunnen zijn – in functie van het nemen van beslissingen voor waar de diensten van de geïntegreerde politie starten met een gedetailleerd identificatieproces en het bevragen van verwanten, zoals blijkt uit het volgende voorbeeld: de aanwezigheid van een tatoeage op de foto op het lichaam van de persoon dat aankomt in het ziekenhuis, geeft een eerste indicatie dat wanneer verwanten op zoek zijn naar een persoon met een tatoeage, dit mogelijks over deze persoon gaat. Deze informatie wordt in eerste instantie dus aangeleverd via BITS en is fundamenteel voor de ondersteuning van het identificatieproces. Door het faciliteren en versnellen van de identificatie door geïntegreerde politie, draagt dit bij aan de doelstelling van Discipline 2 om verwanten zo snel als mogelijk te informeren over de locatie van de betrokken personen waarnaar ze op zoek zijn.* »

49. L'Autorité comprend la nécessité de collecter des photos de personnes impliquées à identifier afin de soutenir le processus d'identification et recommande au demandeur d'insérer cette justification dans le commentaire de l'article et d'adapter l'article 37, §2, alinéa 3, 3° en ce sens. En revanche,

---

[24] « *Bij (zwaar)gewonden dragen audiovisuele opnamen bij tot de bepaling van de noodzakelijk medische opvolging vanop afstand. Een ziekenhuis kan vb. al een inzicht krijgen over de mogelijke letsels van een patiënt die onderweg is naar hun ziekenhuis om zo de nodige middelen en personeel te voorzien bij aankomst (relevantie*). »

elle ne perçoit pas *a priori* la raison pour laquelle il serait nécessaire et pertinent de collecter des enregistrements vidéos ou sonores des personnes impliquées afin de soutenir le processus d'identification. L'Autorité recommande **d'insérer dans l'exposé des motifs une justification appropriée du caractère nécessaire des enregistrements vidéos ou sonores visés (au moyen d'exemples pertinents, le cas échéant).**

50. Par souci d'exhaustivité, l'Autorité attire l'attention du demandeur sur le fait que la photographie du visage d'une personne peut être considérée comme une donnée biométrique au sens de l'article 4.14) du RGPD[25]. Dans une telle hypothèse, le traitement d'une telle donnée nécessitera d'être fondé sur une des exceptions visée à l'article 9.2. du RGPD[26], en plus de l'article 6.1 du RGPD.

3) Communication de données

51. **L'article 38** de l'avant-projet entend encadrer la communication des catégories de données collectées en vertu de l'article 37, §2, alinéas 3 et 4, aux catégories de destinataires qui y sont mentionnés, afin de réaliser les finalités visées audit article 37, §2, alinéas 3 et 4 :

- Les services de la police fédérale chargés de l'identification des personnes décédées et l'accompagnement des proches dans ce processus peuvent avoir accès aux données visées à l'article 37, §2, alinéa 3, dans la limite des missions légales de ces services et uniquement afin de soutenir le processus d'identification des personnes impliquées à identifier (art. 38, §1er);
- Les services chargés du fonctionnement de la cellule nationale victime visée par l'arrêté royal du 18 mai 2020 *portant fixation du plan d'urgence national relatif à l'approche d'une prise d'orage terroriste ou d'un attentat terroriste* et les services chargés de l'organisation du rétablissement peuvent avoir accès aux données visées à l'article 37, §2, alinéa 4, afin de poursuivre la finalité visée audit article et dans la limite des missions légales de ces destinataires (art. 38, §2) ;
- Les services concernés par des situations d'urgence dans le cadre desquelles des personnes impliquées de nationalité étrangère sont concernées peuvent avoir accès aux

[25] À savoir « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ». Voir aussi le considérant 51 du RGPD selon lequel « *Le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique* ». Pour de plus amples informations, il est renvoyé à la recommandation 1/2021 de l'Autorité relative au traitement de données biométriques (disponible via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/recommandation-01-2021-du-1-decembre-2021.pdf).

[26] L'Autorité estime que ce traitement pourrait être fondé sur l'article 9.2.g), pour autant que les garanties y prévues soient respectées.

données visées à l'article 37, §2, alinéas 3 et 4, afin de réaliser les finalités visées à ces deux dispositions, dans la limite des missions légales de ces services (art. 38, §3).

52. Sans préjudice de l'avis du COC pour ce qui concerne l'analyse des traitements de données à caractère personnel relevant de sa compétence, il convient de rappeler qu'afin de répondre au principe de prévisibilité, l'avant-projet doit déterminer de manière suffisamment claire et précise quelle(s) catégorie(s) de destinataire(s) sont visés. Désigner ces catégories de destinataires en identifiant dans l'avant-projet les missions légales qui leur incombent (pour ce qui concerne la catégorie de destinataires visée à l'article 38, §1er) est une bonne approche en ce sens. Cela permet en plus une certaine flexibilité en cas de changement d'appellation d'un service concerné au cours des années[27]. Toutefois, afin de renforcer la prévisibilité de la communication des données visées aux services de la police fédérale concernés, il est **recommandé de prévoir dans l'avant-projet une habilitation au Roi afin qu'il désigne dans une norme réglementaire ultérieure les services concrètement visés**. De même, désigner la catégorie de destinataires concernée en se référant à la norme organique qui les régit (pour ce qui concerne la catégorie de destinataires visée à l'article 38, §2, premier tiret) est aussi une bonne approche pour assurer un niveau adéquat de prévisibilité. En revanche, il n'est pas aisé de comprendre quels sont les « *services chargés de l'organisation du rétablissement* » dans la mesure où les fonctions/tâches incombant à ces services ne sont pas déterminées dans l'avant-projet. Dans le même ordre d'idées, la catégorie de destinataires désignée par les « *services concernés par des situations d'urgence dans le cadre desquelles des personnes impliquées de nationalité étrangère sont concernées* » est formulée par des termes relativement larges. Il ressort des informations complémentaires que sont visés le Ministère des affaires étrangères ainsi que le Centre National de Crise. **A défaut d'indiquer les fonctions/tâches incombant aux services chargés de l'organisation du rétablissement et de désigner nominativement dans l'avant-projet le Ministère des affaires étrangères et le Centre National de Crise, il est recommandé de prévoir une habilitation au Roi** pour désigner dans une norme réglementaire ces destinataires.

53. De plus, afin d'assurer un niveau adéquat de prévisibilité en ce qui concerne les catégories de données concernées par la communication de données visée à l'article 38, il convient de s'assurer que le commentaire de l'article 38 corresponde à ce que prévoit le dispositif de l'avant-projet. L'article 38 prévoit une communication des catégories de données collectées en vertu des alinéas 3 et 4 de l'article 37, §2, alors qu'il semble ressortir dudit commentaire que les catégories de

[27] Il ressort en effet des informations complémentaires que le choix, à l'article 38, §1er, de désigner la catégorie de destinataires visée en se référant à sa mission d'identification des personnes décédées et à l'accompagnement des proches dans ce processus, est précisément motivé par cette volonté de flexibilité afin de pallier le changement d'appellation du service compétent ainsi que la décision concernant le service responsable d'une tâche particulière. Est concrètement visé le service d'aides aux victimes au niveau fédéral et le « Disaster Victim Identfication team » (DVI) de la police fédérale.

données visée sont celles collectées en vertu des alinéas 1, 2 et 4 de l'article 37, §2. De même, l'article 40, §1er, de l'avant-projet qui prévoit une période maximale pendant laquelle l'échange de données peut avoir lieu avec les catégories de destinataires visés à l'article 38 se réfère de manière générale aux données visées à « l'article 37, §2 ». Il y a dès lors lieu de clarifier ce point.

4) Conservation des données

54. **L'article 40, §1er**, de l'avant-projet prévoit que les données à caractère personnel visées à l'article 37, §2, sont échangées avec les destinataires visés à l'article 38 jusqu'à au plus tard trois mois après la fin de la situation d'urgence.

55. Le commentaire de l'article précise qu'il s'agit de la « *période où il est attendu que les identifications nécessaires aient été effectuées et que le début de la période de rétablissement ait été entamée* ». Les informations complémentaires ajoutent que « *Omdat de noodzakelijke tijd om dit te voorzien bij noodsituaties moeilijk te bepalen is (denk aan overstromingen die een lange acute fase kunnen hebben versus een brand of explosie in een appartement die een kortere acute fase inhoudt) en erg afhankelijk is van de complexiteit van de noodsituatie, besloten we hier op maximaal 3 maanden. Het is logisch dat wanneer de noodzaak voor ontvangende diensten voor gegevensuitwisseling korter is dan de maximale termijn, dat we de uitwisseling vroeger afronden*.» L'Autorité prend note de la justification du caractère nécessaire de la durée maximale d'échange de données exposée par les informations complémentaires et invite le demandeur à l'**insérer** dans le commentaire de l'article.

56. En outre, le commentaire de l'article se réfère à une « *méthodologie* » qui est prévue « *complémentairement pour garantir que, dès que possible, les données à caractère personnel ne soient accessibles qu'aux services qui en ont effectivement besoin en fonction de leurs missions* » et cite en exemple « *l'application BITS, dans laquelle sont stockées les données à caractère personnel des personnes impliquées, offre la possibilité de restreindre l'accès aux données à caractère personnel en ajustant le statut de l'incident en fonction des étapes par lesquelles il passe* ».

57. Eu égard au risque d'accès abusif auxquelles les personnes impliquées qui se trouvent dans le système d'enregistrement sont exposées, l'Autorité estime qu'afin de respecter le principe de minimisation des données et à titre de garanties appropriées pour les droits et libertés des personnes concernées, cette **méthodologie devrait idéalement être reflétée dans le dispositif de l'avant-projet**.

58. **L'article 40, §2** de l'avant-projet prévoit que les données à caractère personnel visées à l'article 37, §2 peuvent être conservées pendant une durée maximum de dix ans par le SPF Santé publique.

59. Il ressort du commentaire de l'article ainsi que des informations complémentaires que la nécessité d'une telle durée de conservation se justifie par le fait que cette durée couvre la durée moyenne d'un suivi juridique à la suite d'une situation d'urgence et permet, si nécessaire de (i) confirmer que les personnes impliquées étaient enregistrées comme telles au moment de la situation d'urgence et de (ii) faire valoir leurs droits en tant que victimes. Le commentaire de l'article précise qu'au terme de ce délai de dix ans, les données seront archivées à des fins d'évaluation.

60. L'Autorité prend note de la justification de la nécessité d'une période de conservation de dix ans des données concernées. Afin de renforcer la prévisibilité de l'avant-projet, elle recommande d'**insérer** dans l'avant-projet qu'au terme de ce délai de conservation des données à caractère personnel, les **données anonymisées seront archivées à des fins d'évaluation**.

61. L'article 89.1 RGPD prévoit que tout traitement de données à caractère personnel à des fins statistiques doit être encadré de garanties appropriées assurant que des mesures techniques et organisationnelles soient en place pour assurer le respect du principe de minimisation et que, lorsque les finalités statistiques peuvent être réalisées au moyen de traitements ultérieurs qui ne permettent pas ou plus d'identifier les personnes concernées, cette dernière façon de procéder doit être appliquée.

62. Le traitement ultérieur à des fins statistiques se fait donc de préférence à l'aide de données anonymes[28]. S'il n'est pas possible d'atteindre la finalité de traitement visée à l'aide de données anonymes, des données à caractère personnel pseudonymisées[29] peuvent être utilisées. Si ces données ne permettent pas non plus d'atteindre la finalité visée, des données à caractère personnel non pseudonymisées peuvent aussi être utilisées, uniquement en dernière instance.

63. Au sujet de l'anonymisation et de la pseudonymisation, l'Autorité réitère les considérations qu'elle exprime de manière constante dans ses avis.

64. La transparence quant à la méthode d'anonymisation utilisée ainsi qu'une analyse des risques liés à la réidentification constituent des éléments qui contribuent à une approche réfléchie du

[28] Données anonymes : informations qui ne peuvent pas être reliées à une personne physique identifiée ou identifiable (article 4.1) du RGPD, *a contrario*).

[29] *« Pseudonymisation : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. »* (voir l'article 4.5) du RGPD).

processus d'anonymisation. Or, l'Autorité constate que l'exposé des motifs de l'avant-projet ne contient aucune information quant à la stratégie d'anonymisation envisagée.

65. L'Autorité attire l'attention du demandeur sur le fait qu'il existe une différence entre des données pseudonymisées définies par l'article 4(5) du RGPD comme des données *« qui ne peuvent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires »* et des données anonymisées qui ne peuvent plus par aucun moyen raisonnable être attribuées à une personne précise et que seules ces dernières ne constituent plus des données personnelles et sont donc exclues du champs d'application du RGPD, conformément à son considérant *26* »[30].

66. Dès lors, eu égard à la définition de donnée à caractère personnel telle que figurant à l'article 4, 1) du RGPD[31], il convient de s'assurer que le standard élevé requis pour l'anonymisation est bien atteint[32] et que les données ne sont pas simplement pseudonymisées. En effet, le traitement de données, même pseudonymisées, doit être considérée comme un traitement de données à caractère personnel au sens du RGPD.

67. Il résulte de ce qui précède que, si c'est bien de pseudonymisation (et non d'anonymisation) qu'il est question :

- il conviendra de se référer au rapport de l'Agence de l'Union européenne pour la cybersécurité relatif aux techniques et meilleures pratiques de pseudonymisation[33] ;
- et ce traitement devra être encadré par toutes les garanties requises et répondre aux principes prévalant en la matière[34].

[30] Pour plus d'informations, voir l'avis 5/2014 (WP216) relative aux techniques d'anonymisation, 2.2.3, p. 11 du Groupe 29, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

[31] A savoir : « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» 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* ».

[32] L'identification d'une personne ne vise pas uniquement la possibilité de retrouver son nom et/ou son l'adresse mais également la possibilité de l'identifier par un processus d'individualisation, de corrélation ou d'inférence.

[33] ENISA : https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases et https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation;

[34] Il en va ainsi du principe de proportionnalité renvoyant à celui, plus spécifique, de « *minimisation* » des données impliquant que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard, des finalités pour lesquelles elles sont traitées, conformément à l'article 5, § 1er, c) du RGPD.

D. Portail de sécurité (art. 50)

68. **L'article 50** de l'avant-projet entend encadrer la mise en place du portail de sécurité dont le Centre de crise national (ci-après le « NCCN ») assure le développement, la gestion, le fonctionnement ainsi que sa mise à disposition des « partenaires »[35].

1) Finalités / prévisibilité

69. **L'article 50, §1er** , vise à définir les missions d'intérêt public poursuivies par ce portail en prévoyant qu'il est « *une plateforme en ligne de communication sécurisée, permettant l'échange d'informations entre partenaires, tant pour la planification d'urgence et le suivi de grands événements que pour la gestion d'incidents de situations d'urgence et de crises nationales* ». Les **paragraphes 2 à 4**, déterminent les catégories de données à caractère personnel traitées pour l'exécution de ces missions/tâches[36] .

70. Dans la mesure où la/les finalité(s) d'un traitement de données à caractère personnel effectué par une autorité publique découle en principe de la/des mission(s) d'intérêt public incombant à ladite autorité et pour l'exécution de laquelle/desquelles le traitement de données est nécessaire, il importe de veiller à ce que la/les mission(s) d'intérêt public soi(en)t définie(s) de manière suffisamment claire et exhaustive. Cela permet aux personnes concernées de pouvoir identifier aisément la/les finalité(s) poursuivie(s) par le traitement de données en cause et comprendre les circonstances dans lesquelles les traitements de données envisagés auront lieu. A la lumière des informations complémentaires[37], il est recommandé **d'adapter l'article 50, §1er** afin qu'y soit reflété que le portail de sécurité :

---

[35] L'article 50, §1er, alinéa 3, définit ce qu'il y a lieu d'entendre par « partenaires » comme « *les services opérationnels et stratégiques, les autorités administratives compétentes, les services spécialisés et les centres d'information compétents pour la planification d'urgence, le suivi de grands événements ou la gestion d'incidents, de situations d'urgence ou de crises nationales* ».

[36] La version française de l'article 50, §3, se réfère à l'exécution de tâches et non à l'exécution des missions. Il conviendrait d'harmoniser la terminologie par souci de cohérence.

[37] Interrogé quant aux fonctionnalités/missions d'intérêt public du portail de sécurité visé, il a été répondu ce qui suit :

« *Le portail de sécurité visé à l'article 50 regroupe pour l'instant les fonctionnalités suivantes :*

- *Une partie « répertoire », sorte d'annuaire reprenant l'ensemble des données à caractère personnel listées à l'article 17, § 1er de l'avant-projet de loi, des acteurs pertinents à contacter en cas d'incidents, de situations d'urgence et de crises nationales ;*
- *Une partie reprenant les plans d'urgence et d'intervention enregistrés par les autorités pertinentes ;*
- *Un espace permettant l'échange d'informations pertinentes tant pour la planification d'urgence et le suivi de grands événements que pour la gestion d'incidents, de situations d'urgence et de crises nationales afin de les gérer de manière proactive et efficace. Cette gestion des incidents comprend la création et la mise à jour d'un tableau de la situation avec l'état actuel de la crise, l'évolution prévue, l'intervention en cours et son impact, ainsi que les besoins en termes de personnes et de ressources pour lutter contre la crise.* »

- (1) reprend **sous forme de répertoire les données** à caractère personnel **des acteurs pertinents** (visés aux paragraphes 2 à 4 de l'article 50) **à contacter en cas d'incident national[38], de situations d'urgence et de crises nationales** et
- (2) qu'il permet **l'échange d'informations tant pour la planification d'urgence et le suivi de grands événements que pour la gestion efficace et proactive d'incidents nationaux, de situations d'urgence et de crises nationales**.

71. Afin d'assurer un niveau adéquat de prévisibilité, il est également recommandé de **définir dans l'avant-projet ce qui est visé par le suivi de grands événements.** Selon les informations complémentaires, il s'agit d'événements qui, par leur ampleur (foule importante amassée), ou par la présence de personnalités importantes (famille royale, « VIP »), ou par les valeurs/croyances/appartenances représentées nécessitent de faire l'objet d'une vigilance particulière. De même, l'avant-projet doit **déterminer clairement quels sont les destinataires de l'échange d'informations qui sera effectué par le biais du portail de sécurité visé**. En effet, selon le dispositif de l'avant-projet, sont visés les « *partenaires* » [39] alors que selon le commentaire de l'article, sont visés « *les services d'urgence, les autorités, les partenaires et les entités fédérées* ».

72. Il revient également au demandeur de **s'assurer que l'enregistrement des données à caractère personnel visées à l'article 50, §§2 à 4 est bien nécessaire à l'exécution de toutes les missions inscrites à l'article 50, §1er**. Si tel n'est pas le cas, il conviendrait d'adapter les paragraphes 2 à 4 de l'article 50 afin qu'y soit reflété la finalité qui est concrètement visée. En effet, il ressort des informations complémentaires que les catégories de données visées à l'article 50, §4 « *sont importantes et peuvent être mobilisées dans le cadre de la gestion d'un incident ou d'un grand événement* » mais pas dans le cadre de l'élaboration des plans d'urgence et d'intervention.

73. Il ressort également des informations complémentaires qu'en ce qui concerne les personnes visées à l'article 50, §4, de l'avant-projet qui se verraient ajoutées dans le portail de sécurité par les personnes qui se sont volontairement enregistrées dans ledit portail conformément à l'article 50, §3, leur consentement est explicitement demandé. L'Autorité en prend acte. Et elle rappelle que le consentement de la personne concernée ne peut pas constituer la base de licéité d'un traitement de données à caractère personnel réalisé par une autorité publique dans le cadre de l'exécution de ses missions d'intérêt public : la base de licéité est en effet la nécessité par cette autorité publique d'exécuter la mission d'intérêt public qui lui est attribuée (article 6.1.e) du RGPD). Le

[38] L'Autorité suppose qu'est en effet visé l' « *incident national* », notion définie à l'article 2, 3° de l'avant-projet. Si tel n'est pas le cas, il convient de définir la notion d'incident visée.

[39] Voir la note de bas de page 35 ci-dessus.

consentement de la personne concernée constitue donc une **garantie appropriée complémentaire** au traitement des données les concernant. Elle souligne que cette garantie **doit être reprise de manière explicite dans l'avant-projet**. A cet égard, l'Autorité relève que l'alinéa 3 du paragraphe 4 prévoit que les données à caractère personnel ne peuvent pas être conservées plus de six mois après que l'intéressé ne s'est pas enregistré dans un délai d'un mois à la suite d'une notification envoyée par le NCCN concernant ses données à caractère personnel sur le portail de sécurité. Si par cette disposition, l'intention du demandeur est de permettre à l'intéressé d'exprimer son consentement à ce que ses données soient reprises dans le portail de sécurité (par le biais de l'enregistrement dans ledit portail), l'avant-projet doit indiquer que le consentement sera exprimé par le biais de l'enregistrement à des fins de prévisibilité et de sécurité juridique. Si telle n'est pas l'intention, il convient de compléter l'avant-projet afin d'y prévoir que l'inscription des données de personnes visées ne sera effectuée que si la personne concernée a consenti de manière libre, éclairée et spécifique à cette inscription.

2) Obligation d'information

74. **L'article 50, §7,** prévoit une obligation à charge du NCCN d'informer les personnes introduites dans le portail de sécurité dans le cadre des missions visées au paragraphe 1, de ce qu'elles sont enregistrées dans ledit portail. En vertu de l'article 14 du RGPD, l'obligation d'information incombant au responsable du traitement lorsque les donnes n'ont pas été collectées directement auprès de la personne concernée est plus large que ce que prévoit l'article 50, §7 de l'avant-projet. Dans cette mesure, cette disposition en projet n'apporte pas de réelle plus-value et **devrait être supprimée**.

PAR CES MOTIFS,
L'AUTORITE

Estime qu'il convient de/d' :

A. Pour ce qui concerne la collecte par les bourgmestres et gouverneurs des données des personnes à contacter :

1. reformuler de manière plus précise les finalités poursuivies à la lumière des observations émises aux points 14 ;
2. relier les catégorie(s) de données listées à l'article 17, §1er, alinéa 2 de l'avant-projet aux catégories de personnes listées à l'article 17, §1er, alinéa 1, dans la mesure de ce qui est nécessaire à la réalisation de la finalité poursuivie (point 19) ;

3. remédier à la discordance concernant les catégories de personnes à contacter entre celles listées à l'article 17, §1er, alinéa 1 de l'avant-projet et l'article 8 du projet d'arrêté (point 20);
4. définir, dans la mesure du possible, les catégories de destinataires visées par les expressions « services opérationnels et stratégiques », « autorités concernées », « services spécialisés » et « centres d'information » visées à l'article 18 (point 27) ;
5. préciser à l'article 18 de l'avant-projet que l'accès sera effectué via le portail de sécurité visé à l'article 50 de l'avant-projet (point 28) ;

B. Pour ce qui concerne le système d'enregistrement des personnes impliquées et de leurs proches:

6. décrire de manière claire et exhaustive les missions d'intérêt public confiées audit système d'enregistrement et s'assurer que chacun des traitements de données envisagés (et leurs éléments essentiels) soit prévu de manière claire (points 30 à 33) ;
7. revoir la désignation des services de secours visé à l'article 36 de l'avant-projet en tant que sous-traitants, à la lumière de l'observation émise au point 34 ;
8. s'assurer du caractère complet de la définition de la notion de « personnes impliquées » et de ce que seules les personnes impliquées concernées soient clairement définies selon la finalité concrète poursuivie (point 37) ;
9. s'assurer du caractère nécessaire et pertinent de chaque catégorie de données traitées en vertu de l'article 37, §2 au regard de la finalité poursuivie et des catégories de personnes concernées (personnes impliquées/proches) et de la justifier le cas échéant dans le commentaire de l'article (points 39, 41 et 42) ;
10. préciser à l'article 37 de l'avant-projet ce qu'il convient d'entendre par les « *données d'identification personnelles des personnes impliquées et de leurs proches* » et indiquer si les données de contact seront aussi collectées (point 40) ;
11. remplacer l'expression « *données de localisation* » par les données relatives au lieu ou préciser cette notion dans l'exposé des motifs (point 42) ;
12. adapter l'article 37, §2, alinéas 1 et 3, 4° en précisant que la composition de ménage sera collectée « le cas échéant et si nécessaire » et préciser dans l'exposé des motifs les cas dans lesquels cette donnée serait nécessaire au regard de chacune des finalités poursuivies (point 43) ;
13. remplacer l'expression « *habitudes de vie des personnes impliquées et de leurs proches* » par la langue (point 44) ;
14. clarifier la finalité poursuivie par la collecte d'enregistrements audiovisuels visés à l'article 37, §2, alinéa 2, 5° en veillant à préciser les catégories de personnes concernées par ce traitement de données (point 46) ;

15. insérer la justification du caractère nécessaire de la collecte de photos des personnes impliquées à identifier dans le commentaire de l'article 37, §2, alinéa 3 et adapter l'article 37, §2, alinéa 3, 3 en ce sens ainsi qu'une justification appropriée du caractère nécessaire des enregistrements vidéos ou sonores visés (point 49) ;
16. adapter l'article 38 ainsi que son commentaire à la lumière des observations émises aux points 52 et 53 ;
17. insérer dans le commentaire de l'article 40, §1, de l'avant-projet la justification du caractère nécessaire de la durée maximale d'échange des données qui y est visé (point 55) ;
18. refléter idéalement la méthodologie visée au commentaire de l'article 40 dans le dispositif de l'avant-projet (point 57) ;
19. insérer à l'article 40, §2 de l'avant-projet qu'au terme du délai de conservation de dix ans, les données anonymisées seront archivées à des fins d'évaluation (point 60) ;

C. Portail de sécurité

20. adapter l'article 50, §1 de l'avant-projet afin qu'y soient reflétées les missions d'intérêt public poursuivies par le portail de sécurité visé (point 70 et 71);
21. prévoir explicitement à l'article 50, §4 de l'avant-projet que le consentement de la personne qui se verrait ajoutée dans le portail de sécurité sera bien demandé (point 73) ;
22. supprimer l'article 50, §7 de l'avant-projet (point 74).

Pour le Centre de Connaissances,
(sé) Cédrine Morlière, Directrice