



Avis n° 144/2018 du 19 décembre 2018

Objet: Projet d'Arrêté royal relatif à la planification d'urgence et la gestion des situations d'urgence à l'échelon national 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. (CO-A-2018-159)

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

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

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 « RGDP»);

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 Monsieur Jan Jambon, Ministre de la Sécurité et de l'Intérieur reçue le 6 novembre 2018;

Vu les informations complémentaires reçues en date du 19 novembre 2018;

Vu le rapport de Monsieur Debeuckelaere Willem;

Émet, le 19 décembre 2018, l'avis suivant :

I. Objet et contexte de la demande

1. Le Ministre de la Sécurité et de l'Intérieur (ci-après « le demandeur ») sollicite l'avis de l'Autorité concernant les articles 5 à 7 de son projet d'Arrêté royal (AR) relatif à la planification d'urgence et la gestion des situations d'urgence à l'échelon national 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.
2. Le projet d'AR impose aux gouverneurs et aux bourgmestres de rédiger des plans d'urgence qui contiennent notamment les données de contact de personnes concernées par la gestion et la prévention des situations d'urgence¹. Selon le document explicatif du projet communiqué par le demandeur, il peut s'agir de personnes physiques et plus spécifiquement de personnes travaillant auprès des « *autorités et services publics concernés par la gestion des situations d'urgence, des centres d'accueil, des responsables des établissements à la source ou dans l'environnement d'un risque particulier* » et encore des adresses et numéros de téléphone d'instituts privés disposant d'une expertise concernant un risque particulier ou encore de fournisseurs d'eau potable, de gaz, d'électricité, transport, travaux, génie civil.

II. Examen

3. Toute législation prévoyant des traitements de données à caractère personnel doit répondre aux critères usuels de qualité édictés par la jurisprudence afin qu'à leur lecture les personnes concernées à propos desquelles des données sont traitées puissent entrevoir clairement les traitements qui sont fait de leurs données à caractère personnel. A ce titre, elles doivent notamment décrire avec précision la ou les finalités concrètes et opérationnelles du traitement de données encadré par la législation, les types de données qui font l'objet du traitement, les catégories de personnes concernées dont les données sont traitées, les catégories de destinataires auxquels le cas échéant les données sont communiquées et les finalités pour lesquelles ces communications ont lieu, les durées de conservation des données et toutes mesures visant à assurer un traitement licite et loyal des données à caractère personnel.

¹ La notion de situation d'urgence est définie à l'article 1,3° du projet d'AR en ces termes : « 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 la coordination des acteurs compétents, en ce compris les disciplines, afin de faire disparaître la menace ou de limiter les conséquences néfastes de l'événement ».

4. L'article 5 en projet prévoit que ces « *plans généraux d'urgence et d'intervention (PGUI) comprendront au moins :*

1° les informations générales relatives à la province ou à la commune concernée, à savoir :

a) le répertoire des services opérationnels et stratégiques des autorités concernées, des services spécialisés, des centres d'information et des experts (...) »

5. Il ressort des informations complémentaires obtenues auprès du fonctionnaire délégué que, par « *répertoire des services opérationnels et stratégiques des autorités concernées*», il convient d'entendre « les coordonnées des responsables administratifs et opérationnels (nom, fonction, téléphone, fax, gsm, mail, heures de contact) ». Au vu de ce qui précède, le libellé de cette disposition doit être revu pour

- a. tout d'abord, préciser la finalité concrète et opérationnelle de cette mention obligatoire dans les PGUI et ensuite,
- b. préciser les catégories de données à caractère personnel devant être mentionnées et ce, dans la mesure où les informations complémentaires obtenues du délégué ne se reflètent pas dans le texte en projet.
- c. Seront également précisées les catégories de personnes concernées² dont les coordonnées doivent être mentionnées et la notion d' « *autorités concernées* » sera utilement remplacée par la notion d'autorités dont la mission de service public consiste en la gestion de situations d'urgence.

Sans ces précisions, non seulement le traitement manquera de transparence et de prévisibilité tel que requis par la jurisprudence mais le caractère obligatoire de la mention de ces données dans le PGUI s'en trouvera affecté et impactera négativement le but de l'auteur du projet d'AR. Ce dernier ne perdra pas de vue que ces précisions doivent se faire en adéquation avec le principe de minimisation des données (art. 5.1.c RGPD) qui requiert que seules peuvent être traitées des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées.

6. Par ailleurs, l'Autorité attire l'attention sur le fait que des données à caractère personnel ne doivent pas nécessairement être traitées pour s'assurer de pouvoir contacter les personnes *ad hoc* en cas de réalisation d'une situation d'urgence. Des adresses de contact génériques (de type contactcrisismanagement@province.be, contactcrisispompiers@commune.be) peuvent être créées pour remplir cette fonction. Une telle façon de procéder permet de pallier au roulement de personnel, à son indisponibilité pour maladie ou congé et à la nécessité de devoir actualiser en

² En tout état de cause, en application du principe de minimisation des données, les personnes désignées doivent être celles dont il ressort de leur fonction qu'elles doivent pouvoir être contactées en cas de réalisation d'une situation d'urgence dans la mesure où leur fonction/mission est liée à la gestion des risques/situations d'urgence.

permanence les données sans parler du fait que, pour certains types de personnes concernées dans la gestion de certaines situations spécifiques d'urgence (par exemple les personnes spécialisées dans la gestion des attaques terroristes), il peut être opportun pour la protection de leur propre personne que leur identité ne soit pas reprise dans un tel plan ou centralisée dans un registre. Une telle façon de procéder nécessite d'imposer aux autorités compétentes de veiller à la tenue à jour de leur répertoire d'adresses génériques (ou de contacts téléphoniques génériques) pour assurer que les membres de leur personnel en charge de ces gestions de crise reçoivent bien les courriers électroniques (ou tél) adressés à ces adresses. En application du principe de minimisation des données, l'Autorité recommande à l'auteur du projet d'AR de prévoir dans son projet d'AR la mention de ce type d'adresse générique et cette obligation de mise à jour, à tout le moins pour les personnes dont la fonction ou l'expertise spécifique rend nécessaire l'adoption de mesures de protection pour leur propre personne.

7. Quant à la notion d'expert visée à l'article 5.1.a) du projet d'AR, il s'agit, selon les informations complémentaires obtenues auprès de la déléguée du Ministre, de « *personnes qui en raison de leurs connaissances par rapport à un ou des aspect(s) de la gestion de crise stratégique ou opérationnelle ou par rapport à un risque spécifique, sont à même de fournir des informations utiles pour les décisions à prendre en gestion de crise* ». Selon ces mêmes informations complémentaires, ces experts peuvent faire partie des services des communes ou provinces ou encore émaner du secteur privé (professeurs d'université, personne émanant d'un service extérieur au pays venu en soutien aux autorités compétentes,...). Le projet d'AR appelle sur ce point les deux remarques suivantes :
 - a. Tout d'abord, au regard des critères précités de qualité des lois, la notion d'expert visée à l'article 5, 1°, a) du projet d'AR, doit faire l'objet d'une définition pour être déterminée avec précision.
 - b. Ensuite, en ce qui concerne les experts qui n'exercent pas une mission de service public en vertu de laquelle ils doivent pouvoir être contactés en situation d'urgence ou pour la prévention de ce type de situation, il convient de préciser dans le dispositif que la mention de leurs coordonnées de contact ne se fait qu'après que ces derniers aient été informés spécifiquement des détails du traitement de leurs données dans ce cadre et des traitements liés (mention dans le portail sécurisé national Incident & Crisis Management mis à disposition des autorités) et qu'on leur ait donné la possibilité de renoncer sans motif à cette mention (opt out). Cet opt-out constitue une mesure appropriée pour s'assurer de la pertinence de leur traitement de données dans ce cadre (s'assurer auprès d'eux qu'ils sont bien experts pour la gestion du risque visé,...)

8. L'article 6, §1^{er} du projet d'AR prévoit que « *les plans particuliers d'urgence et d'intervention (PPUI) comprennent au minimum :*
1° la description du risque en cause et la fixation de la zone ou des zones de planification d'urgence ;
2° les coordonnées des acteurs spécifiquement concernées par le risque ;
3°... »
9. Dans le même ordre d'idées que les remarques précédemment faites, la notion d' « acteur spécifiquement concerné par le risque », visée à l'article 6, §1^{er}, 2° en projet, fera aussi l'objet d'une définition dans le projet d'AR pour assurer la détermination précise et claire de ces catégories de personnes physiques en application du principe de minimisation des données. En vertu de quel(s) critère(s), un acteur peut-il être concerné par le risque (en raison de sa mission de service public et du fait qu'il intervient dans la prévention et la gestion de ce risque? En raison de sa situation dans une zone à risque et de son statut de victime potentielle ?...) Pour le surplus, il est renvoyé aux remarques précédentes sur l'utilisation d'adresses de contact génériques.
10. L'article 7 du projet d'AR prévoit que « *§1^{er} les autorités compétentes transmettent, chacune pour ce qui la concerne, le PUI (plan d'urgence et d'intervention) aux autorités, services et personnes qui y sont repris comme destinataires, notamment via le portail national de sécurité. §2. Les destinataires visés au §1^{er} du présent article sont tenus de communiquer immédiatement à l'autorité compétente concernée toute modification aux données qui les concernent, notamment via le portail national de sécurité. »*
11. Il ressort des informations complémentaires obtenues auprès de la déléguée du Ministre que le libellé de l'article 7, §1^{er} en projet doit être revu. Selon ces informations, le PUI doit être communiqué par l'Autorité compétente aux acteurs de la gestion de crise qui ont un rôle à jouer dans le plan concerné et qui doivent dès lors en être informés. Il convient de réviser le libellé de cette disposition en projet afin que les détails de ces communications de données y soient déterminés avec clarté.
12. De plus, il ressort du document introductif à la demande d'avis que les plans d'urgence et les coordonnées des acteurs clés en situation d'urgence sont centralisés dans un portail sécurisé dénommé ICMS (Incident & crisis management system) qui est mis en place par le SPF Intérieur (DG centre de crise) depuis le 1^{er} janvier 2017 et qui a pour finalité de permettre l'échange d'informations entre tous les partenaires concernés en planification d'urgence et gestion de crise et ce, tant dans la phase de planification que lors des situations d'urgence. L'auteur du projet d'AR veillera à ce que cette centralisation et ces échanges de données se reflètent également dans le

libellé de l'article 7 en projet afin d'y assurer un bon degré de prévisibilité de ces traitements de données. Il y sera également fait mention de la finalité opérationnelle et concrète de ce portail sécurisé, de la durée de conservation des données à caractère personnel y mentionnées et du responsable de traitement de ce portail.

13. Concernant ce portail sécurisé ICMS, le chapitre «protection des données» du document introductif à la demande d'avis adressée à l'Autorité de protection des données fait référence au fait que le maintien et la mention des coordonnées de contact de toutes personnes impliquées dans la gestion des crises et situations d'urgence est soumis respectivement au non exercice de leur opt-out ou à leur consentement préalable et ce à raison de deux fois par an. Il est également précisé que leurs données sont supprimées dans le mois de leur notification de leur volonté de voir leurs données retirées. A ce sujet, l'Autorité de protection des données relève que la mise en place de ce type de portail cadre avec les missions de service public du Centre gouvernemental de Coordination et de Crise créé au sein du SPF Intérieur par Arrêté royal du 18 avril 1988³. Parmi celles-ci, figurent en effet « *le rassemblement de manière permanente de toute information se rapportant à ses compétences et l'information des services et personnes responsables de situations de crise nationale⁴ ou susceptibles de conduire à une telle situation et la mise à disposition des autorités compétentes l'infrastructure et les moyens nécessaire à la gestion d'une telle crise, et notamment assurer la coordination, la préparation des décisions, leur exécution éventuelle et le suivi* » (art. 3 de l'AR précité du 18/04/1988). C'est donc en exécution de sa mission de service public (art. 6.1.e du RGPD) que le Centre de crise du SPF Intérieur met en place le portail ICMS. Il peut donc légitimement y intégrer les données à caractère personnel de personnes qui exercent une fonction de service public liée à la gestion de situations de crise ou d'urgence ou à la prévention de telles situations sans devoir leur demander leur consentement préalable à ce sujet mais moyennant bien sûr réalisation de toutes les obligations qui sont les siennes en vertu du RGPD (et notamment l'information des personnes concernées conformément aux articles 13 ou 14 du RGPD en fonction qu'il s'agit d'une collecte de données directe auprès de la personne concernée dont les données sont mentionnées ou pas) et d'adoption de mesures spécifiques au titre de garantie de protection pour les personnes de contact. Ce n'est que s'il est fait mention dans ce portail de coordonnées de personnes qui n'exercent pas une telle mission de service public que l'Autorité de protection des données considère qu'un opt-out doit leur être offert à titre de mesure de garantie (cf. supra).
14. Concernant l'article 7, § 2 en projet qui impose aux personnes, dont les données sont reprises dans le portail national de sécurité, de communiquer toute modification de leurs données de contact, l'Autorité de protection des données attire l'attention du SPF Intérieur sur le fait que, en

³ AR du 18 avril 1988 portant création du « du Centre gouvernemental de Coordination et de Crise ».

⁴ Selon cet AR, une crise est nationale « *lorsque la menace trouve son origine sur le territoire national ou doit être combattue par des moyens principalement nationaux* ».

tant que responsable de traitement du portail ICMS, c'est à lui que, en application de l'article 5.1.d du RGPD, revient l'obligation d'adopter toutes mesures raisonnables pour s'assurer de l'exactitude et de la mise à jour des données à caractère personnel reprises dans le portail⁵.

15. L'autorité de protection des données attire également l'attention du SPF Intérieur sur le fait que les articles 5.1.f et 32 du RGPD lui imposent de paramétrer le portail ICMS de manière telle que soit garantie une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.
16. 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.
17. Pour l'exécution concrète de ces mesures, l'Autorité renvoie à la recommandation⁶ visant à prévenir les fuites de données et aux mesures de référence⁷ qu'il convient de respecter dans le cadre de tout traitement de données à caractère personnel. De plus, étant donné que le portail ICMS est accessible et alimenté par l'ensemble des acteurs de la gestion de crise, du niveau communal au niveau national, l'Autorité souligne spécialement l'importance d'une bonne gestion des utilisateurs et des accès⁸.

⁵ Ceci sans préjudice du fait que les communes et provinces peuvent être considérées comme responsable de traitement de leur propre plan de sécurité concernant les données à caractère personnel qu'elles collectent pour l'établir.

⁶ Recommandation d'initiative de la Commission n° 01/2013 du 21 janvier 2013 *relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*

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

⁷ Mesures de référence de la Commission 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_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf).

⁸ Voir aussi la recommandation de la Commission n° 01/2008 du 24 septembre 2008 *relative à la gestion des accès et des utilisateurs dans le secteur public*

(https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2008_0.pdf).

18. Enfin, la DG Centre de crise du SPF Intérieur veillera à prévoir la désignation d'un point de contact facilement accessible (mention explicite sur le site web du portail sécurité) afin que les personnes concernées puissent lui adresser aisément leurs requêtes quand elles souhaiteront exercer les droits dont elles disposent en vertu de la législation en matière de la protection des données à caractère personnel.

Par ces motifs,

L'Autorité,

émet un **avis favorable** sur le projet d'Arrêté royal moyennant la prise en compte des remarques suivantes :

1. Mention claire de la finalité de la mention obligatoire de coordonnées des personnes dans le PGUI, détermination précise des catégories de personnes concernées et des types de données à mentionner et ce, conformément au principe de minimisation des données (point 5) ;
2. Utilisation obligatoire d'adresse de contact générique pour les personnes de contact pour lesquelles cela s'impose et imposition d'une obligation de mise à jour de ces adresses de contact générique aux autorités concernées (point 6) ;
3. Ajout d'une définition des notions d'experts et d'acteur spécifiquement concerné par le risque visées aux articles 5,1°, a et 6,§1, 2° en projet et mise en place d'un opt-out pour certains d'entre eux (points 7 et 8) ;
4. Révision du libellé de l'article 7 en projet comme recommandé aux points 11 et 12.

Pour le surplus, l'Autorité **recommande** que le SPF Intérieur se conforme à ses recommandations reprises aux points 12 à 18 pour le paramétrage de son portail sécurité ICMS.

L'Administrateur f.f.,

Le Président

(sé) An Machtens

(sé) Willem Debeuckelaere