Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 33/2024 du 12 avril 2024

Objet : Avis relatif à un projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, *relatif à l'exécution coordonnée du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)* (CO-A-2024-054)
Mots-clés : DSA (règlement sur les services numériques) – procédure de plainte – IBPT - autorités compétentes - système de partage de l'information – responsable de traitement

Traduction[1]

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, Bart Preneel et Gert Vermeulen ;

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 "la 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* (Règlement général sur la protection des données, ci-après "le 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 "la LTD") ;

[1] Pour la version originale validée collégialement, cf. la version néerlandaise du texte qui est disponible sur la version NL de la rubrique « avis » du site web de l'Autorité

Vu la demande d'avis de Monsieur Pierre-Yves Dermagne Ministre de l'Économie et du Travail, (ci-après "le demandeur"), reçue le 12/02/2024 ;

Émet, le 12 avril 2024, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le 12/02/2024, le demandeur a sollicité l'avis de l'Autorité au sujet du projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, *relatif à l'exécution coordonnée du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)* (ci-après : le projet).

2. Le projet entend régir les compétences respectives et l'exécution coordonnée entre les parties en ce qui concerne certains aspects du règlement sur les services numériques (ci-après : le règlement) qui vise à prévoir des règles harmonisées pour la fourniture de services intermédiaires dans le marché intérieur. Plus concrètement, on établit :
   - un cadre pour l'exemption conditionnelle de responsabilité des fournisseurs de services intermédiaires ;
   - des règles relatives à des obligations de diligence spécifiques, adaptées à certaines catégories spécifiques de fournisseurs de services intermédiaires ;
   - des règles relatives à la mise en œuvre et à l'exécution du présent règlement, y compris en ce qui concerne la coopération et la coordination entre les autorités compétentes.

3. Dans ce cadre, le règlement requiert que chaque État membre désigne un coordinateur pour les services numériques (ci-après : le coordinateur) faisant office de point de contact unique pour la Commission européenne, les autres coordinateurs des États membres, le comité européen pour les services numériques, les fournisseurs de services intermédiaires et les autres autorités compétentes lorsque cela présente de l'intérêt pour l'exécution de leurs missions respectives. Conformément à l'article 4, § 1er du projet, l'Institut belge des services postaux et des télécommunications (ci-après : l'IBPT) est désigné comme coordinateur[2].

[2] Plus concrètement, l'IBPT est désigné comme autorité compétente pour l'État fédéral, qui assurera également le rôle de coordinateur pour les services numériques (voir l'article 14, § 1er de la loi du 17 janvier 2003 *relatif* [sic] *au statut du régulateur des secteurs des postes et des télécommunications belges*).

4. Par ailleurs, compte tenu des règles de répartition des compétences en Belgique, les entités suivantes sont désignées comme autorités compétentes pour l'application du règlement pour les matières qui relèvent de la compétence des Communautés :
   - en ce qui concerne la Communauté flamande : l'autorité compétente visée dans le décret du 27 mars 2009 *relatif à la radiodiffusion et à la télévision*, article 175/2 ;
   - en ce qui concerne la Communauté française : l'autorité compétente visée dans le décret du 4 février 2021 *relatif aux services de médias audiovisuels et aux services de partage de vidéos*, article 9.1.1 – 3- ;
   - en ce qui concerne la Communauté germanophone : l'autorité compétente visée dans le décret du 1er mars 2021 *relatif aux services de médias et aux représentations cinématographiques*, article 112, troisième alinéa.

5. Les autorités compétentes et le coordinateur mettent en œuvre le règlement dans le respect de leurs compétences respectives et du principe de proportionnalité. À cet effet, le but est que toutes les informations transmises via le coordinateur soient placées dans un système de partage de l'information, afin que les autres autorités puissent être informées de cas qui relèvent de leur compétence.

6. Le coordinateur est responsable de la coordination au niveau national de toutes les questions en lien avec la surveillance et l'exécution du règlement et contribue à une surveillance et une exécution efficaces et cohérentes du règlement dans toute l'Union européenne. Ses missions sont énoncées de manière exhaustive à l'article 4, § 2 du projet. Les compétences résiduelles reviennent aux autorités compétentes des Communautés au sens de l'article 1er, 2° du projet (voir le point 4).

7. Les informations échangées dans le cadre du traitement de plaintes et d'enquêtes concernant la surveillance du règlement peuvent contenir le cas échéant des données à caractère personnel. L'Autorité se limite ci-après à l'analyse des dispositions du projet qui concernent directement ou indirectement le traitement de données à caractère personnel.

II. EXAMEN QUANT AU FOND

a. Remarque préalable

8. Dans un souci d'exhaustivité, l'Autorité rappelle que conformément à l'article premier du RGPD, lu à la lumière du considérant 14 du RGPD, la protection conférée par le RGPD concerne des personnes physiques et ne s'étend donc pas au traitement de données relatives à des personnes morales et, plus concrètement, à des entreprises constituées en tant que personnes morales.

Dès lors, le présent avis concerne uniquement le traitement de données de personnes physiques qui sont concernées par les dispositions du projet, pour autant que ces traitements doivent être qualifiés de traitements de données à caractère personnel au sens des articles 2 et 3 du RGPD.[3]

9. Dans le contexte du règlement et des compétences de surveillance et d'enquête attribuées au coordinateur et aux autorités compétentes, le traitement de données à caractère personnel reste en principe limité (1) aux personnes qui sont le cas échéant mentionnées dans les documents ou pièces obtenu(e)s dans le cadre de la surveillance ou de l'exécution du règlement (et plus précisément les données de plaignants (personnes physiques) ou de collaborateurs ou administrateurs de services intermédiaires (dans la mesure où leur identification est nécessaire au traitement d'une plainte ou à la réalisation d'enquêtes)) et (2) aux collaborateurs du coordinateur et des autorités compétentes chargés de la gestion du système de partage de l'information visé à l'article 5 du projet ou qui peuvent y accéder d'une autre manière.

b. Base juridique

10. *Rappel des principes :* 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 être nécessaire et proportionnée et répondre aux exigences de prévisibilité et de précision dans le chef des personnes concernées. En vertu de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la *Constitution* et 8 de la CEDH, une telle norme légale doit définir les éléments essentiels des traitements allant de pair avec l'ingérence de l'autorité publique. 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 les traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique représentent une ingérence importante dans les droits et libertés des personnes concernées, la norme légale doit également définir les éléments essentiels (complémentaires) suivants :
    - 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 ;

[3] Par souci d'exhaustivité, l'Autorité fait remarquer que cela ne porte pas préjudice à la protection dont les personnes morales bénéficient le cas échéant en vertu des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Voir dans ce cadre par exemple la CJUE, 9 novembre 2010, C-92/09 et C-93/09 (Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen).

- le délai de conservation maximal des données à caractère personnel enregistrées ;
- l'éventuelle limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD.

11. *Application des principes :* Sans toutefois porter préjudice au caractère sensible ou confidentiel des informations ou des données qui, dans le cadre de la surveillance, des enquêtes et de l'application du règlement, seront échangées ou traitées par le coordinateur et les autorités compétentes, l'Autorité estime que les traitements de données à caractère personnel, dont la nature et l'ampleur restent limitées (tant sur le plan personnel que matériel) et sont purement secondaires à la lumière des finalités du règlement, ne représentent pas nécessairement une ingérence importante dans les droits et libertés des personnes concernées et, sauf exceptions éventuelles, sont **prévisibles**.

c. Finalités

12. Comme déjà expliqué brièvement ci-avant, le règlement a pour but de contribuer au bon fonctionnement du marché intérieur de services intermédiaires en prévoyant des règles harmonisées pour un environnement en ligne sûr, prévisible et fiable qui favorise l'innovation et dans lequel les droits fondamentaux consacrés par la Charte, dont notamment le principe de protection des consommateurs, sont efficacement protégés.

13. À cet effet, le règlement requiert que chaque État membre désigne une ou plusieurs autorités compétentes, ainsi qu'un coordinateur pour les services numériques pour la surveillance des fournisseurs de services intermédiaires et l'exécution de ce règlement.

14. En vue d'une coopération efficace entre le coordinateur et les autorités compétentes, un système de partage de l'information est établi à l'article 5 du projet, lequel indique en temps réel l'état d'avancement des dossiers qu'ils traitent, en ce compris la décision prise, le cas échéant. Les articles 8 – 16 décrivent les modalités ainsi que les obligations en vertu du règlement dans le chef du coordinateur et des autorités compétentes en ce qui concerne le partage de données via le système de partage de l'information[4]. L'article 17, § 2 du projet (qui concerne spécifiquement le traitement de données à caractère personnel) précise enfin que "*La transmission, le stockage et tout autre traitement de données à caractère personnel dans le système de partage de l'information visé à l'article 5 ne peuvent avoir lieu que de manière nécessaire et proportionnée et uniquement aux fins suivantes :*

[4] L'article 4, § 1er du projet renvoie de manière exhaustive aux dispositions du règlement (lisez : missions) qui sont assurées par le coordinateur. Les autres missions reviennent, conformément à l'article 4, § 2 du projet, aux autorités compétentes, compte tenu des règles de répartition des compétences.

1° échange d'information entres les autorités compétentes dans le cadre de la surveillance, des enquêtes et de l'application du règlement ;
2° traitement de dossiers par les autorités compétentes dans l'exercice de leurs compétences dans le cadre de la surveillance, des enquêtes et de l'application du règlement.

L'article 17, § 3 du projet prévoit en outre que le traitement de données à caractère personnel peut uniquement avoir lieu via le système de partage de l'information visé à l'article 5 du projet.

15. À cet égard, l'Autorité estime qu'à la lumière des finalités générales du règlement, les finalités du traitement sont déterminées, explicites et légitimes. **Néanmoins, il semble recommandé de formuler également ces finalités dans les lois organiques relatives à l'organisation et aux compétences du coordinateur (l'IBPT) et des autres autorités compétentes**.

d. Responsable du traitement

16. Conformément à l'article 4.7) du RGPD, le responsable du traitement est toute personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. Dans un souci d'exhaustivité, l'Autorité rappelle que la désignation du responsable du traitement doit être adéquate au regard des circonstances factuelles.

17. À cet égard, l'article 17, § 1er du projet dispose ce qui suit : "*Les autorités compétentes sont chacune responsable du traitement des données pour la gestion des données en leur possession ou mises à leur disposition en vertu du présent accord.*"

18. L'Autorité se demande toutefois – compte tenu du fonctionnement de la plateforme de partage de l'information et de la relation sous-jacente entre les différentes autorités – s'il n'est pas question d'une responsabilité conjointe au sens de l'article 26 du RGPD pour certains aspects du traitement. Il résulte en effet du projet que les plaintes et injonctions au sens des articles 9 et 10 du règlement doivent être mises immédiatement à la disposition du coordinateur et des autorités compétentes via la plateforme de partage de l'information et que l'attribution d'une plainte déterminée requiert en principe un consensus entre les différentes autorités. Dès lors, l'Autorité estime qu'en ce qui concerne au moins la gestion du système de partage de l'information et le partage de données

dans ce système, il est question d'une responsabilité conjointe, ce qui implique l'obligation de respecter les conditions fixées à l'article 26 du RGPD[5].

19. En outre, étant donné que l'article 5 du projet mentionne simplement la 'mise en place d'un système de partage de l'information', il est également incontestablement nécessaire de préciser quelle(s) entité(s) assure(nt) effectivement la gestion de ce système de partage de l'information[6].

20. La désignation correcte du responsable du traitement est enfin cruciale dans le contexte de l'exercice des droits des personnes concernées (voir à cet égard l'article 17, § 6 du projet[7]). L'Autorité demande d'examiner cet élément plus avant et, au besoin, de l'adapter.

e. Proportionnalité/Minimisation des données

21. 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').

22. À cet égard, l'article 17, §§ 3-4 du projet dispose ce qui suit : *"§ 3. Le traitement des données à caractère personnel peut avoir lieu via le système de partage de l'information visé à l'article 5 uniquement en ce qui concerne les catégories suivantes de personnes concernées :*

1° les personnes physiques dont les informations sont contenues dans des documents obtenus dans le cadre de la surveillance, des enquêtes et de l'application du règlement ;

2° les administrateurs du système de partage de l'information visé à l'article 5, ainsi que les personnes ayant accès à ce système.

§ 4. Le traitement des données à caractère personnel peut avoir lieu via le système de partage de l'information visé à l'article 5 uniquement pour les catégories de données à caractère personnel suivantes :

---

[5] Par extension, l'Autorité renvoie au point 2 de la deuxième partie des Lignes directrices 07/2020 de l'EDPB *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*. Consultable via le lien suivant : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr.

[6] Par souci d'exhaustivité, étant donné qu'il semble probable que pour la mise en place et, par la suite, la gestion du système de partage de l'information, les différents responsables du traitement feront appel à des sous-traitants au sens de l'article 4.8) du RGPD, l'Autorité attire l'attention sur l'obligation de conclure avec ces sous-traitants un contrat au sens de l'article 28.3 du RGPD.

[7] En marge, l'Autorité fait remarquer que l'applicabilité directe des règlements européens emporte l'interdiction de leur retranscription dans le droit national en raison du fait qu'un tel procédé peut "(créer) une équivoque en ce qui concerne tant la nature juridique des dispositions applicables que le moment de leur entrée en vigueur". Voir : CJUE, 7 février 1973, Commission c. Italie (C-39/72), Recueil de jurisprudence, 1973, p. 101, § 17). Voir également : CJUE 10 octobre 1973, Fratelli Variola S.p.A. c. Service des impôts italien (C-34/73), Recueil de jurisprudence, 1973, p. 981, § 11 ; CJUE, 31 janvier 1978, Ratelli Zerbone Snc c. Amministrazione delle finanze dello Stato, Recueil de jurisprudence (C-94/77), 1978, p. 99**,** §§ 24-26). L'article 17, § 6 précité du projet constitue *de facto* une paraphrase des articles 5.2 et 12.1-2 du RGPD et viole ainsi l'interdiction de retranscription du RGPD. Vu ce constat, le paragraphe en question doit en principe être supprimé.

1° *les données d'identification, les coordonnées, les données relatives à un dossier et toute autre information jugée nécessaire à la surveillance, aux enquêtes et à l'application du règlement ;*

2° *un dossier et toute autre information jugée nécessaire à la surveillance, aux enquêtes et à l'application du règlement ;*

3° *le nom, l'adresse, les informations de contact, numéro de contact, (numéro d'utilisateur) des administrateurs du système de partage de l'information visé à l'article 5 et des personnes ayant accès à ce système."*

23. En ce qui concerne en premier lieu les données à caractère personnel de personnes physiques dont les informations sont contenues dans des documents enregistrés dans le système de partage de l'information, l'Autorité fait remarquer qu'il n'est ni souhaitable, ni possible de régir au préalable et de manière exhaustive quelles données sont pertinentes ou nécessaires pour la surveillance ou l'exécution du règlement (par exemple lorsqu'il s'agit de tiers cités dans une plainte ou qui font l'objet (indirectement[8]) d'une enquête). Néanmoins, il incombe aux responsables du traitement de veiller, à la lumière du principe de responsabilité conformément aux articles 5.2 et 24 – 25 du RGPD et du principe de minimisation des données, à ce que les données à caractère personnel qui ne sont pas nécessaires pour les finalités visées soient supprimées de la documentation (ou si possible, soient anonymisées) ou soient pseudonymisées[9]. Cette remarque vaut en particulier pour la catégorie de données "*toute autre information jugée nécessaire à la surveillance, aux enquêtes et à l'application du règlement*".

24. Il est par contre possible de conclure d'ores et déjà des conventions (contraignantes) concernant les procédures (internes) en matière d'introduction ou de traitement des plaintes ou de réalisation d'enquêtes, et plus particulièrement de préciser davantage et de définir (au besoin dans les lois organiques portant création des différents responsables du traitement[10], ou dans un arrêté d'exécution ou un règlement d'ordre intérieur/une déclaration de confidentialité accessibles au public) les catégories de données à caractère personnel de personnes qui introduisent une plainte (y compris les collaborateurs ou personnes de contact d'organisations ou d'entreprises qui introduisent une plainte), ainsi que de tiers qui sont entendus dans le cadre d'une enquête en cours. Il va de soi que de tels règlements doivent s'appliquer de manière harmonisée à tous les responsables du traitement.

[8] Compte tenu du champ d'action du règlement, une personne physique ne fera en effet jamais l'objet exclusif d'une plainte ou d'une enquête.

[9] Tout traitement de données à caractère personnel à cet égard doit nécessairement se limiter à ce qui est nécessaire et pertinent dans le cadre de la violation alléguée ou présumée du règlement.

[10] Voir les points 3 et 4.

25. En ce qui concerne en deuxième lieu les administrateurs du système de partage de l'information ainsi que les personnes qui ont accès à ce système, l'Autorité estime que vu l'intégrité professionnelle requise de ces personnes ainsi que la protection élevée qui est attendue pour les informations dans le système de partage précité, il est tout simplement légitime et même nécessaire pour les responsables du traitement de connaître à tout moment l'identité des collaborateurs qui peuvent accéder au système de partage de l'information. En outre, en vue du contrôle *ex post* et afin d'éviter les abus, il semble également opportun de **mettre en place *des systèmes de journalisation fiables***. Cela ne porte bien entendu pas préjudice à l'obligation dans le chef des responsables du traitement de prendre des mesures techniques et organisationnelles appropriées conformément à l'article 24 du RGPD afin de protéger adéquatement les données de leurs collaborateurs.

f. Délai de conservation

26. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

27. À cet égard, l'article 17, § 5 du projet prévoit que : *"Les données à caractère personnel collectées sont conservées pendant le temps nécessaire au traitement de dossiers relatifs à l'application du règlement.*"

28. L'Autorité prend acte de ce délai, mais elle estime que la notion du "*temps nécessaire au traitement de dossiers*" laisse la porte ouverte à l'interprétation et elle demande dès lors de préciser expressément que les données doivent le cas échéant être conservées jusqu'à la fin définitive des procédures administratives ou judiciaires (y compris l'épuisement de toutes les voies de recours) auxquelles le traitement d'un dossier a donné lieu.

29. Par ailleurs, l'Autorité demande de fixer aussi un délai de conservation (éventuellement par la suite, dans un arrêté d'exécution) pour les données à caractère personnel des collaborateurs des responsables du traitement chargés de la gestion du système de partage de l'information (ou qui ont accès au système d'une autre manière), en particulier en ce qui concerne les 'données de journalisation'. Dans le cadre des contrôles *ex post* au niveau de la licéité de consultations dans le système de partage de l'information ou de litiges juridiques concernant la surveillance ou l'exécution du règlement, de telles données jouent en effet un rôle important. Ces délais ne peuvent en effet pas être inférieurs aux délais de conservation maximaux qui s'appliquent aux (données à caractère personnel comprises dans les) dossiers.

g. Directives complémentaires

30. Pour conclure, l'Autorité estime qu'il est nécessaire de définir les éléments suivants dans le projet, ou par la suite dans un arrêté d'exécution :
    - prévoir un cadre de coordination pour les (DPO des) responsables du traitement concernés afin d'harmoniser la politique de protection des données (incluant les modalités des traitements de données à caractère personnel sous-jacents) ;
    - prévoir une intervention humaine pour la gestion des accès (de certains aspects) du système de partage de l'information.

31. Par ailleurs, et de manière générale, il est recommandé (dans le chef des responsables du traitement) de d'ores et déjà tenir compte des directives suivantes en matière de prévention, de détection et de contrôle, afin de limiter au maximum les risques inhérents liés aux systèmes de partage de l'information (tant en ce qui concerne le traitement de données à caractère personnel que les autres informations (sensibles et confidentielles) dont le partage est visé) :
    - définir des paramètres pour la surveillance de la consultation des dossiers ou pour l'imposition d'exigences supplémentaires en matière d'accès à ces dossiers (incluant les données à caractère personnel qui y sont reprises) (journalisation) ;
    - prévoir des plans de continuité et de résilience via des sauvegardes afin de pouvoir assurer la continuité du traitement et du partage ;
    - protéger les sauvegardes avec le même niveau de protection qui s'applique aux données et systèmes initiaux ;
    - implémenter des stratégies d'isolation entre systèmes (internes) qui préviennent la diffusion de 'ransomwares' (ou autres malwares) dans toute l'organisation ;
    - implémenter une politique actualisée de mots de passe, incluant l'impossibilité d'utiliser des mots de passe plus faibles ou compromis, et – idéalement – recourir à l'authentification à deux facteurs ;
    - définir un quota/une limitation de la consultation par utilisateur ou par compte pour des ensembles de données sensibles, compte tenu des finalités concrètes pour lesquelles ces données sont utilisées ;
    - implémenter des systèmes de détection de tentatives échouées d'accéder à des données ainsi que des systèmes de détection d'exfiltration de données.

32. Enfin, il ne faut pas non plus sous-estimer l'importance des mesures suivantes qui sont plus organisationnelles :
    - définir des plans efficaces de lutte contre les incidents qui encadrent la gestion de violations ;

- établir des canaux d'information souples et efficaces entre le DPO et la direction (tant en interne par responsable du traitement que pour les responsables du traitement entre eux) ;
- établir des directives en matière de communication de violations (liées au droit à la protection des données) à l'autorité de contrôle compétente et, le cas échéant, aux personnes concernées[11] ;
- définir des procédures d'évaluation concernant les transferts de données via le système de partage de l'information, les évolutions technologiques et les nouveaux développements en matière de réglementation, d'évolutions sociales ou politiques, … (outre les obligations d'évaluation existant déjà dans le chef du coordinateur et des autorités compétentes en vertu du règlement) ;
- réaliser périodiquement des audits en matière de vie privée et de sécurité.

PAR CES MOTIFS,
l'Autorité,

estime que le système de partage de l'information qui doit être créé par le projet peut en principe offrir suffisamment de garanties en matière de protection des données à caractère personnel, à condition que les remarques suivantes soient prises en compte :

- il est recommandé de reprendre les finalités du traitement, les modalités de ce traitement ainsi que les compétences à cet égard dans les lois organiques portant création des différents responsables du traitement (points 3 et 4 *j°* 15) ;
- il convient d'examiner s'il n'est pas question d'une responsabilité conjointe au sens de l'article 26 du RGPD (à tout le moins en ce qui concerne certains aspects des traitements de données sous-jacents) (points 17 – 20) ;
- le délai de conservation fixé doit être adapté afin d'éviter des problèmes d'interprétation. Un délai de conservation doit également être défini pour les données de journalisation (et plus concrètement pour les données à caractère personnel des collaborateurs des responsables du traitement qu'elles contiennent) (points 28 – 29) ;
- les directives énoncées aux points 31 – 32 doivent être prises en compte.

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

[11] Déterminer quand une telle communication est requise, la voie par laquelle elle doit avoir lieu, indiquer quelles mesures sont prises pour limiter autant que possible les conséquences de la violation, formuler des recommandations aux personnes concernées en fonction de la nature de la violation (par exemple modifier les mots de passe ou les noms d'utilisateur).