DÉCISION (UE) 2021/2243 DE LA COMMISSION

du 15 décembre 2021

portant adoption de règles internes relatives à la communication d'informations aux personnes concernées et à la limitation de certains de leurs droits dans le contexte du traitement des données à caractère personnel aux fins de la sécurité des systèmes d'information et de communication de la Commission

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 249, paragraphe 1,

considérant ce qui suit:

(1) Dans l'exercice de ses missions, la Commission est tenue de respecter les droits des personnes physiques concernant le traitement des données à caractère personnel qui sont consacrés par l'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne et par l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne. Elle doit également respecter les droits prévus par le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([1]). Parallèlement, la Commission doit traiter les incidents de sécurité informatique conformément aux règles énoncées à l'article 15 de la décision (UE, Euratom) 2017/46 ([2]).

(2) Afin de garantir la sécurité informatique, c'est-à-dire la préservation de la confidentialité, de l'intégrité et de la disponibilité des systèmes de communication et d'information et des ensembles de données qu'ils traitent, en ce qui concerne les personnes, les biens et les informations, la Commission, notamment par l'intermédiaire de sa direction générale de l'informatique, a pris des mesures conformément aux décisions (UE, Euratom) 2017/46 et C(2017) 8841 final ([3]). Ces mesures comprennent le suivi des risques informatiques et les mesures de sécurité informatique mises en œuvre, la demande aux propriétaires de systèmes de prendre des mesures spécifiques afin d'atténuer les risques en matière de sécurité informatique pour les systèmes de communication de la Commission et la gestion des incidents de sécurité informatique.

(3) La direction générale de l'informatique fournit des opérations et des services de sécurité informatique à la Commission et doit traiter plusieurs catégories de données à caractère personnel afin de:

— communiquer des alertes et avertissements concernant des événements et incidents liés à la sécurité informatique,

— réagir face à des événements et incidents et les contenir,

— faciliter l'utilisation des outils et les opérations au moyen d'audits de sécurité, d'évaluations de la sécurité et de la gestion de la vulnérabilité,

— sensibiliser davantage le personnel de la Commission dans le domaine de la cybersécurité,

— suivre, détecter et prévenir les événements et incidents liés à la sécurité informatique,

— contrôler les comptes d'utilisateurs privilégiés.

(4) Des incidents de sécurité informatique susceptibles de menacer la sécurité des systèmes d'information et de communication de la Commission peuvent survenir lors de toute opération de traitement effectuée par la Commission. Ils peuvent concerner n'importe quelle catégorie de données à caractère personnel traitées par la Commission.

([1]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

([2]) Décision (UE, Euratom) 2017/46 de la Commission du 10 janvier 2017 sur la sécurité des systèmes d'information et de communication au sein de la Commission européenne (JO L 6 du 11.1.2017, p. 40).

([3]) Décision C(2017) 8841 de la Commission du 13 décembre 2017 portant modalités d'application des articles 3, 5, 7, 8, 9, 10, 11, 12, 14 et 15 de la décision (UE, Euratom) 2017/46 sur la sécurité des systèmes d'information et de communication au sein de la Commission européenne.

(5) Dans certaines circonstances, il peut s'avérer nécessaire de concilier les droits des personnes concernées prévus par le règlement (UE) 2018/1725 avec la nécessité de garantir que la Commission s'acquitte efficacement de ses tâches consistant à assurer la sécurité informatique des personnes, des biens et des informations au sein de la Commission en application de la décision (UE, Euratom) 2017/46, dans le plein respect des droits fondamentaux et libertés d'autres personnes concernées. À cet effet, l'article 25, paragraphe 1, du règlement (UE) 2018/1725 autorise la Commission à limiter l'application des articles 14 à 17, 19, 20 et 35 de ce règlement, ainsi que du principe de transparence énoncé à l'article 4, paragraphe 1, point a), de ce même règlement, dans la mesure où les dispositions de cet article correspondent aux droits et obligations prévus auxdits articles 14 à 17, 19 et 20.

(6) La présente décision devrait s'appliquer à toutes les opérations de traitement effectuées par la Commission en qualité de responsable du traitement des données aux fins de l'exécution de ses tâches visant à assurer la sécurité informatique des personnes, des biens et des informations au sein de la Commission, en application de la décision (UE, Euratom) 2017/46. Elle devrait donc viser les personnes concernées pour les catégories de données à caractère personnel faisant l'objet de ces opérations de traitement, c'est-à-dire les personnes qui interagissent avec un des systèmes d'information et de communication de la Commission.

(7) Les données à caractère personnel sont conservées dans un environnement électronique sécurisé afin d'empêcher tout accès illicite par des personnes extérieures à la Commission. Des durées de conservation des données différentes s'appliquent aux différentes opérations de traitement en fonction du type de données à caractère personnel en cause. La conservation des dossiers au sein de la Commission est régie par la liste commune de conservation des dossiers au niveau de la Commission européenne [SEC(2019) 900], un document à valeur réglementaire qui se présente sous la forme d'un tableau de gestion fixant les périodes de conservation pour les différents types de dossiers de la Commission européenne, afin de limiter la conservation des données à ce qui est nécessaire.

(8) La Commission pourrait être amenée à limiter l'application des droits des personnes concernées afin de préserver sa sécurité intérieure conformément à l'article 25, paragraphe 1, point d), du règlement (UE) 2018/1725 (c'est-à-dire de préserver la confidentialité, l'intégrité et la disponibilité de ses systèmes de communication et d'information et des ensembles de données qu'ils traitent, de ses biens et de ses informations). En particulier, la Commission pourrait être amenée à agir ainsi pour:

— communiquer des alertes et avertissements concernant des événements et incidents liés à la sécurité informatique,

— réagir face à des événements et incidents et les contenir; faciliter l'utilisation des outils et les opérations au moyen d'audits de sécurité, d'évaluations de la sécurité et de la gestion de la vulnérabilité,

— sensibiliser davantage le personnel de la Commission dans le domaine de la cybersécurité,

— suivre, détecter et prévenir les événements et incidents liés à la sécurité informatique,

— contrôler les comptes d'utilisateurs privilégiés.

(9) Aux fins de la gestion des incidents de sécurité informatique, conformément à l'article 15 de la décision (UE, Euratom) 2017/46, la direction générale de l'informatique peut échanger des informations avec l'équipe de réaction aux cyberattaques de la direction générale chargée des ressources humaines et de la sécurité.

(10) Afin de se conformer aux articles 14, 15 et 16 du règlement (UE) 2018/1725, la Commission devrait informer toutes les personnes des activités qui impliquent le traitement de leurs données à caractère personnel et qui ont une incidence sur leurs droits. Elle devrait le faire de manière transparente et cohérente en publiant sur le site web de la Commission un avis relatif à la protection des données. Le cas échéant, elle devrait appliquer des garanties supplémentaires pour informer individuellement les personnes concernées sous une forme appropriée.

(11) Se conformer aux articles 14, 15 et 16 du règlement (UE) 2018/1725 pourrait révéler l'existence de mesures, vulnérabilités ou incidents de sécurité informatique relevant de l'article 15 de la décision (UE, Euratom) 2017/46. La divulgation de ces mesures, vulnérabilités et incidents de sécurité informatique accroît le risque que la mesure de sécurité informatique ainsi révélée soit contournée, que la vulnérabilité ainsi révélée soit exploitée et que l'analyse en cours des incidents de sécurité informatique puisse être compromise par suite de la manipulation accidentelle ou intentionnelle d'artefacts par un utilisateur ou un acteur malveillant. Cela pourrait nuire gravement à la capacité de la Commission d'assurer sa sécurité informatique et en particulier à l'efficacité future de la gestion des incidents de sécurité informatique.

(12) Aux termes de l'article 25, paragraphe 1, point h), du règlement (UE) 2018/1725, la Commission est également autorisée à limiter l'application des droits des personnes concernées afin de protéger les droits et libertés d'autres personnes liées à des incidents de sécurité informatique qui pourraient compromettre les opérations de sécurité informatique.

(13) La Commission peut également devoir limiter la communication d'informations aux personnes concernées ainsi que l'application d'autres droits des personnes concernées en ce qui concerne les données à caractère personnel reçues de pays tiers ou d'organisations internationales, afin de s'acquitter de son devoir de coopération avec ces pays ou organisations. Cela s'inscrit dans le cadre du devoir de la Commission de préserver un objectif important d'intérêt public général de l'Union, tel que visé à l'article 25, paragraphe 1, point c), du règlement (UE) 2018/1725. Toutefois, dans certains cas, l'intérêt des droits fondamentaux de la personne concernée peut prévaloir sur l'intérêt de la coopération internationale.

(14) La Commission a donc identifié les motifs énumérés à l'article 25, paragraphe 1, points c), d) et h) du règlement (UE) 2018/1725 comme des motifs de limitations qu'il peut être nécessaire d'invoquer pour les opérations de traitement de données effectués par la direction générale de l'informatique en lien avec la fourniture d'opérations et de services de sécurité informatique à la Commission.

(15) Toute limitation appliquée en vertu de la présente décision devrait être nécessaire et proportionnée, compte tenu des risques qui pèsent sur les droits et libertés des personnes concernées.

(16) La Commission devrait traiter toutes les limitations de manière transparente et consigner chaque application d'une limitation dans le registre correspondant.

(17) En vertu de l'article 25, paragraphe 8, du règlement (UE) 2018/1725, les responsables du traitement peuvent différer, omettre ou refuser la communication d'informations sur les motifs de l'application d'une limitation à la personne concernée si cela prive d'effet, de quelque manière que ce soit, la limitation imposée. Cela s'applique en particulier aux limitations des obligations prévues aux articles 16 et 35 du règlement (UE) 2018/1725. La Commission devrait réexaminer à intervalles réguliers les limitations imposées afin de veiller à ce que les droits de la personne concernée à être informée conformément aux articles 16 et 35 du règlement (UE) 2018/1725 ne soient limités qu'aussi longtemps que nécessaire pour permettre à la Commission d'assurer sa sécurité informatique et, notamment, de gérer les incidents de sécurité informatique.

(18) Lorsque la Commission limite l'application des droits des personnes concernées autres que ceux visés aux articles 16 et 35 du règlement (UE) 2018/1725, le responsable du traitement des données devrait évaluer au cas par cas si la communication de la limitation porte atteinte à sa finalité.

(19) Le délégué à la protection des données de la Commission devrait procéder à un examen indépendant de l'application des limitations afin de garantir le respect de la présente décision.

(20) Afin de permettre à la Commission de limiter immédiatement l'application de certains droits et obligations conformément à l'article 25 du règlement (UE) 2018/1725, la présente décision devrait entrer en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

(21) Le contrôleur européen de la protection des données a rendu son avis le 16 septembre 2021,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objet et champ d'application

1. La présente décision établit les règles que la Commission doit suivre pour informer les personnes concernées du fait que leurs données à caractère personnel seront traitées conformément aux articles 14, 15 et 16 du règlement (UE) 2018/1725 lorsqu'elle exerce l'ensemble des tâches qui lui sont confiées en vertu de la décision (UE, Euratom) 2017/46.

Elle fixe également les conditions dans lesquelles la Commission peut limiter l'application des articles 4, 14 à 17, 19, 20 et 35 du règlement (UE) 2018/1725, conformément à l'article 25, paragraphe 1, points c), d) et h), dudit règlement, lorsqu'elle s'acquitte des tâches qui lui incombent en vertu de la décision (UE, Euratom) 2017/46.

2. La présente décision s'applique aux opérations de traitement de données à caractère personnel effectuées par la Commission ou en son nom aux fins des activités qu'elle mène pour assurer la sécurité des personnes, des biens et des informations au sein de la Commission en vertu de la décision (UE, Euratom) 2017/46, ou en relation avec ces activités.

Article 2

Exceptions et limitations applicables

1. Lorsque la Commission exerce ses fonctions en ce qui concerne les droits des personnes concernées en vertu du règlement (UE) 2018/1725, elle examine si l'une des exceptions établies dans ledit règlement s'applique.

2. Sous réserve des articles 3 à 7 de la présente décision, lorsque l'exercice des droits et obligations prévus aux articles 14 à 17, 19, 20 et 35 du règlement (UE) 2018/1725 en ce qui concerne les données à caractère personnel traitées par la Commission compromettrait la finalité de la fourniture d'opérations et de services de sécurité informatique, notamment en révélant les vulnérabilités ainsi que les outils et méthodes d'enquête de la Commission ou nuirait aux droits et libertés ainsi qu'à la sécurité d'autres personnes concernées, en particulier en ce qui concerne le traitement de données à caractère personnel afin de:

— communiquer des alertes et avertissements concernant des événements et incidents liés à la sécurité informatique,

— réagir face à des événements et incidents et les contenir,

— faciliter l'utilisation d'outils et les opérations au moyen d'audits de sécurité, d'évaluations de la sécurité et de la gestion de la vulnérabilité,

— sensibiliser davantage le personnel de la Commission dans le domaine de la cybersécurité,

— suivre, détecter et prévenir les événements et incidents liés à la sécurité informatique,

— contrôler les comptes d'utilisateurs privilégiés,

la Commission peut limiter l'application:

a) des articles 14 à 17, 19, 20 et 35 du règlement (UE) 2018/1725,

b) le principe de transparence énoncé à l'article 4, paragraphe 1, point a), du règlement (UE) 2018/1725, dans la mesure où les dispositions de cet article correspondent aux droits et obligations prévus aux articles 14 à 17, 19 et 20 du règlement (UE) 2018/1725.

La Commission peut agir ainsi conformément à l'article 25, paragraphe 1, points c), d) et h) du règlement (UE) 2018/1725.

3. Sous réserve des articles 3 à 7, la Commission peut limiter les droits et obligations visés au paragraphe 2 du présent article:

a) lorsque l'exercice de ces droits et obligations à l'égard des données à caractère personnel obtenues auprès d'une autre institution, d'un autre organe ou d'un autre organisme de l'Union pourrait être limité par cette autre institution, cet autre organe ou cet autre organisme de l'Union sur la base des actes juridiques prévus à l'article 25 du règlement (UE) 2018/1725, ou en vertu du chapitre IX de ce règlement, ou conformément au règlement (UE) 2016/794 du Parlement européen et du Conseil ([4]) ou au règlement (UE) 2017/1939 du Conseil ([5]);

b) lorsque l'exercice de ces droits et obligations à l'égard des données à caractère personnel obtenues auprès d'une autorité compétente d'un État membre pourrait être limité par les autorités compétentes de cet État membre sur la base des actes visés à l'article 23 du règlement (UE) 2016/679 du Parlement européen et du Conseil ([6]) ou en vertu de mesures nationales transposant l'article 13, paragraphe 3, l'article 15, paragraphe 3, ou l'article 16, paragraphe 3, de la directive (UE) 2016/680 du Parlement européen et du Conseil ([7]);

([4]) Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

([5]) Règlement (UE) 2017/1939 du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen (JO L 283 du 31.10.2017, p. 1).

([6]) 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) (JO L 119 du 4.5.2016, p. 1).

([7]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

c) lorsque l'exercice de ces droits et obligations compromettrait la coopération de la Commission avec des pays tiers ou des organisations internationales sur les menaces communes en matière de cybersécurité.

Avant d'appliquer des limitations dans les circonstances visées au premier alinéa, points a) et b), la Commission consulte les institutions, organes ou organismes de l'Union ou les autorités des États membres concernés au sujet des motifs potentiels justifiant l'imposition de limitations; de la nécessité et de la proportionnalité des limitations concernées, sauf si cela est de nature à porter atteinte aux activités de la Commission et s'il est manifeste pour la Commission que l'application d'une limitation est prévue par l'un des actes visés auxdits points ou que cette consultation est de nature à compromettre la finalité de ses activités au titre de la décision (UE, Euratom) 2017/46.

Le premier alinéa, point c), ne s'applique pas lorsque les intérêts ou les libertés et droits fondamentaux de la personne concernée prévalent sur l'intérêt de la Commission à coopérer avec des pays tiers ou des organisations internationales.

4. Les paragraphes 1, 2 et 3 sont sans préjudice de l'application d'autres décisions de la Commission établissant des règles internes régissant la communication d'informations aux personnes concernées et la limitation de l'application de certains droits en vertu de l'article 25 du règlement (UE) 2018/1725.

5. Toute limitation des droits et obligations visés au paragraphe 2 est nécessaire et proportionnée aux risques qui pèsent sur les droits et libertés des personnes concernées.

6. Un test de nécessité et de proportionnalité est effectué au cas par cas avant l'application de limitations et les limitations correspondent à ce qui est strictement nécessaire pour atteindre l'objectif visé.

Article 3

Communication d'informations aux personnes concernées

1. La Commission publie sur son site internet un avis relatif à la protection des données informant toutes les personnes concernées de ses activités impliquant le traitement de leurs données à caractère personnel aux fins de l'exécution des tâches qui lui incombent en application de la décision (UE, Euratom) 2017/46, avec une description des catégories de données à caractère personnel en cause. Lorsqu'il est possible de le faire sans compromettre la sécurité informatique, la Commission veille à ce que les personnes concernées soient informées individuellement sous une forme appropriée.

2. Lorsque la Commission limite, entièrement ou partiellement, la communication d'informations aux personnes concernées dont elle traite les données à caractère personnel aux fins de l'exécution des tâches qui lui incombent en application de la décision (UE, Euratom) 2017/46, elle enregistre et consigne dans un registre les motifs de la limitation conformément à l'article 6 de la présente décision.

Article 4

Droit d'accès de la personne concernée, droit à l'effacement et droit à la limitation du traitement des données

1. Si la Commission limite, entièrement ou partiellement, le droit d'accès aux données à caractère personnel des personnes concernées, le droit à l'effacement ou le droit à la limitation du traitement des données visées aux articles 17, 19 et 20 du règlement (UE) 2018/1725, elle informe la personne concernée, dans sa réponse à la demande d'accès, d'effacement ou de limitation du traitement des données:

a) de la limitation appliquée et des principaux motifs de celle-ci;

b) de la procédure à suivre pour introduire une réclamation auprès du Contrôleur européen de la protection des données ou pour former un recours juridictionnel devant la Cour de justice de l'Union européenne.

2. La Commission peut différer, omettre ou refuser la communication d'informations sur les motifs de la limitation visée au paragraphe 1, dès lors que cela compromettrait la finalité de la limitation.

3. La Commission enregistre et consigne dans un registre les motifs de la limitation conformément à l'article 6.

4. Lorsque le droit d'accès est entièrement ou partiellement limité, la personne concernée peut exercer son droit d'accès en prenant contact avec le Contrôleur européen de la protection des données, conformément à l'article 25, paragraphes 6, 7 et 8, du règlement (UE) 2018/1725.

Article 5

Communication aux personnes concernées d'une violation de données à caractère personnel

Lorsque la Commission limite la communication à la personne concernée d'une violation de données à caractère personnel, telle que visée à l'article 35 du règlement (UE) 2018/1725, elle enregistre et consigne dans un registre les motifs de la limitation conformément à l'article 6 de la présente décision. La Commission communique le dossier au CEPD au moment de la notification de la violation de données à caractère personnel.

Article 6

Enregistrement des limitations et consignation dans un registre

1. La Commission enregistre les motifs de toute limitation appliquée en vertu de la présente décision, y compris une référence aux motifs juridiques appliqués pour la limitation, ainsi qu'une évaluation de la nécessité et de la proportionnalité de la limitation, en tenant compte des éléments pertinents énumérés à l'article 25, paragraphe 2, du règlement (UE) 2018/1725.

2. L'enregistrement indique de quelle manière l'exercice d'un droit par la personne concernée compromettrait la finalité de la fourniture d'opérations et de services de sécurité informatique à la Commission en application de la décision (UE, Euratom) 2017/46 ou des limitations appliquées en vertu de l'article 2, paragraphe 2 ou 3, de la présente décision, ou porterait atteinte aux droits et libertés d'autres personnes concernées.

3. La Commission conserve ces registres et tous les documents contenant des éléments factuels et juridiques pertinents. Ils sont mis à la disposition du Contrôleur européen de la protection des données sur demande.

Article 7

Durée des limitations

1. Les limitations visées aux articles 3, 4 et 5 continuent de s'appliquer aussi longtemps que les motifs qui les justifient restent valables.

2. Lorsque les motifs d'une limitation visée aux articles 3, 4 et 5 ne sont plus valables, la Commission:

a) lève la limitation;

b) communique à la personne concernée les principaux motifs de la limitation;

c) informe la personne concernée de la procédure à suivre pour déposer une plainte auprès du Contrôleur européen de la protection des données ou pour former un recours juridictionnel devant la Cour de justice de l'Union européenne.

Article 8

Garanties et durées de conservation

1. La Commission réexamine l'application des limitations visées aux articles 3, 4 et 5 tous les six mois à compter de leur adoption et à la clôture de l'opération de sécurité informatique concernée. Par la suite, la Commission réexamine et contrôle chaque année la nécessité de maintenir la limitation.

Le réexamen inclut une évaluation de la nécessité et de la proportionnalité de la limitation, en tenant compte des éléments pertinents énumérés à l'article 25, paragraphe 2, du règlement (UE) 2018/1725.

2. La Commission a adopté des mesures techniques et organisationnelles visant à éviter toute destruction, perte, altération, divulgation non autorisée, d'origine accidentelle ou illicite, de données à caractère personnel transmises, conservées ou traitées de toute autre manière, comme par exemple dans le cadre de la gestion des droits d'accès, d'une politique de sauvegarde ou de toute autre mesure conforme à la décision (UE, Euratom) 2017/46, ou l'accès non autorisé à ces données.

3. La Commission consigne les durées de conservation conformément à la liste commune de conservation des dossiers au niveau de la Commission et met à la disposition des personnes concernées les durées de conservation pour ces activités de traitement dans son avis relatif à la protection des données.

Article 9

Réexamen par le délégué à la protection des données de la Commission

1. Le délégué à la protection des données de la Commission est informé sans délai chaque fois que les droits de personnes concernées sont limités conformément à la présente décision. Il obtient sur demande l'accès à l'enregistrement et à tout document contenant des éléments factuels et juridiques sous-jacents.

2. Il peut demander un réexamen des limitations et est informé du résultat du réexamen demandé.

3. La Commission documente l'intervention du délégué à la protection des données chaque fois que les droits de personnes concernées sont limités conformément à la présente décision.

Article 10

Entrée en vigueur

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 15 décembre 2021.

Par la Commission
La présidente
Ursula VON DER LEYEN