Journal officiel
de l'Union européenne

FR
Série L

2025/2571

23.12.2025

DÉCISION D'EXÉCUTION (UE) 2025/2571 DE LA COMMISSION

du 19 décembre 2025

modifiant la décision d'exécution (UE) 2021/1773 de la Commission constatant, conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni

[notifiée sous le numéro C(2025) 8782]

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu la 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 (directive en matière de protection des données dans le domaine répressif) ([1]), et en particulier son article 36, paragraphe 3,

considérant ce qui suit:

1. INTRODUCTION

(1) Dans la décision d'exécution (UE) 2021/1773 ([2]), la Commission conclut que, aux fins de l'article 36 de la directive (UE) 2016/680, le Royaume-Uni assure un niveau de protection adéquat des données à caractère personnel transférées dans le cadre de ladite directive de l'Union européenne vers le Royaume-Uni.

(2) Lorsqu'elle a adopté la décision d'exécution (UE) 2021/1773, la Commission a tenu compte du fait que, à l'issue de la période de transition prévue par l'accord sur le retrait du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de l'Union européenne et de la Communauté européenne de l'énergie atomique ([3]) et dès que la disposition provisoire prévue par l'article 782 de l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part ([4]), aurait cessé de s'appliquer, le Royaume-Uni adopterait, appliquerait et mettrait en œuvre un nouveau régime de protection des données, autre que celui qui était en place lorsqu'il était lié par le droit de l'Union.

(3) Étant donné que cela pouvait donner lieu à des modifications concernant le cadre de protection des données évalué dans la décision d'exécution (UE) 2021/1773, ou à d'autres évolutions pertinentes, il a été jugé approprié de prévoir que ladite décision serait applicable pour une durée de quatre ans à compter de son entrée en vigueur. La décision d'exécution (UE) 2021/1773 devait donc expirer le 27 juin 2025, sauf si elle est prorogée conformément à la procédure visée à l'article 58, paragraphe 2, de la directive (UE) 2016/680.

(4) Pour se prononcer sur une éventuelle prorogation de la décision d'exécution (UE) 2021/1773, la Commission doit procéder à une évaluation afin de déterminer si la conclusion selon laquelle le Royaume-Uni assure un niveau de protection adéquat est toujours justifiée sur les plans factuel et juridique à la lumière de l'évolution de la situation depuis l'adoption de la décision d'exécution (UE) 2021/1773 en ce qui concerne les éléments énumérés à l'article 36, paragraphe 2, de la directive (UE) 2016/680.

(5) En particulier, le 23 octobre 2024, le gouvernement britannique a présenté au Parlement britannique le projet de loi sur les données (utilisation et accès) ([5]), qui contient des propositions de modifications de la loi de 2018 sur la protection des données (loi DPA 2018) évaluée dans la décision d'exécution (UE) 2021/1773. Le 24 juin 2025, la

([1]) JO L 119 du 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.
([2]) Décision d'exécution (UE) 2021/1773 de la Commission du 28 juin 2021 constatant, conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (JO L 360 du 11.10.2021, p. 69, ELI: http://data.europa.eu/eli/dec_impl/2021/1773/oj).
([3]) JO C 384 I du 12.11.2019, p. 1.
([4]) JO L 149 du 30.4.2021, p. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.
([5]) Disponible à l'adresse suivante: https://bills.parliament.uk/bills/3825/news.

Commission a adopté la décision d'exécution (UE) 2025/1225 ([6]), qui a prolongé la validité de la décision d'exécution (UE) 2021/1773 pour une période de six mois, jusqu'au 27 décembre 2025. Cette prorogation technique limitée dans le temps a permis à la Commission de mener à bien son évaluation du caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni en s'appuyant sur un cadre juridique stable, c'est-à-dire après l'achèvement du processus législatif concerné.

(6) Depuis l'adoption de la décision d'exécution (UE) 2021/1773, la Commission suit, de manière permanente, les évolutions pertinentes au Royaume-Uni ([7]). Conformément au considérant 165 de la décision d'exécution (UE) 2021/1773, une attention particulière a été accordée à l'application concrète des règles du Royaume-Uni concernant les transferts des données à caractère personnel aux pays tiers et à l'incidence qu'elle pourrait avoir sur le niveau de protection des données transférées en vertu de la décision d'exécution (UE) 2021/1773, et à l'exercice effectif des droits individuels, y compris toute évolution pertinente de la législation et de la pratique concernant les exceptions ou restrictions à ces droits. Entre autres éléments, l'évolution de la jurisprudence et le contrôle exercé par le Bureau du commissaire à l'information (ICO) et par d'autres organismes indépendants ont alimenté le suivi assuré par la Commission.

(7) Sur la base de l'évaluation de ces évolutions, y compris les modifications apportées à la loi DPA 2018 par la loi sur les données (utilisation et accès), la Commission conclut que le Royaume-Uni continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées dans le cadre de la directive (UE) 2016/680 de l'Union européenne vers le Royaume-Uni.

2. ÉVOLUTIONS PERTINENTES CONCERNANT LES RÈGLES APPLICABLES AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

2.1. Le cadre de protection des données du Royaume-Uni

(8) Lorsque la décision d'exécution (UE) 2021/1773 a été adoptée, le cadre juridique britannique régissant le 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, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces, était constitué des parties pertinentes de la loi DPA 2018 ([8]), telle que modifiée par les règlements de 2019 relatifs à la protection des données, à la vie privée et aux communications électroniques (amendements, etc.) (retrait de l'Union européenne) ([9]), et en particulier de la partie 3 de cette loi.

(9) Bien que cette loi, qui reflétait étroitement les règles correspondantes applicables au sein de l'Union européenne, continue de constituer la législation du Royaume-Uni en matière de protection des données pour les activités de traitement concernées, elle a depuis lors fait l'objet de modifications limitées, traduisant le fait que le Royaume-Uni n'est plus soumis au droit de l'Union européenne.

(10) Premièrement, la loi de 2023 sur le droit de l'Union conservé (réforme et révocation) (loi REUL) ([10]) a précisé que les principes généraux du droit de l'Union ne feraient plus partie du droit national britannique après la fin de l'année 2023 ([11]). En outre, les juridictions du Royaume-Uni ne sont plus tenues d'interpréter le «droit assimilé» qui reste inchangé, qui était précédemment appelé «droit de l'Union conservé», conformément aux principes généraux du

([6]) Décision d'exécution (UE) 2025/1225 de la Commission du 24 juin 2025 modifiant la décision d'exécution (UE) 2021/1773 constatant, conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (JO L, 2025/1225, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1225/oj).

([7]) Article 36, paragraphe 4, de la directive (UE) 2016/680.

([8]) Data Protection Act 2018, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2018/12/contents. Avant le retrait du Royaume-Uni de l'Union européenne et pendant la période de transition, la loi DPA 2018 établissait des règles nationales, lorsque le règlement (UE) 2016/679 le permettait, précisant et limitant l'application des règles du règlement (UE) 2016/679 et de la directive transposée (UE) 2016/680.

([9]) Règlements de 2019 relatifs à la protection des données, à la vie privée et aux communications électroniques (amendements, etc.) (retrait de l'Union européenne), disponibles à l'adresse suivante: https://www.legislation.gov.uk/uksi/2019/419/contents/made, tels que modifiés par la réglementation DPPEC de 2020, disponible à l'adresse suivante: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. La réglementation DPPEC modifie le règlement (UE) 2016/679, tel qu'il a été intégré dans le droit britannique par la loi de 2018 sur l'Union européenne (notification de retrait), la loi DPA 2018 et d'autres législations en matière de protection des données afin de les adapter au contexte national.

([10]) Loi de 2023 sur le droit de l'Union conservé (réforme et révocation), disponible à l'adresse suivante: https://www.legislation.gov.uk/ukpga/2023/28.

([11]) Article 5 de la loi de 2018 sur l'Union européenne (notification de retrait), telle que modifiée par la loi REUL.

droit de l'Union; ledit droit doit plutôt être interprété de manière compatible avec le droit national britannique ([12]). Toutefois, le droit assimilé qui reste inchangé doit toujours être interprété par les juridictions compétentes du Royaume-Uni conformément à la jurisprudence pertinente de la Cour de justice de l'Union européenne rendue avant la fin de la période de transition ([13]), comme indiqué également au considérant 12 de la décision d'exécution (UE) 2021/1773. La loi DPA 2018 a été modifiée par la loi sur les données (utilisation et accès) afin de préciser les effets de la loi REUL sur la législation britannique en matière de protection des données. Par exemple, l'article 183A, paragraphe 1, de la loi DPA 2018 prévoit comme règle générale que toute nouvelle législation (adoptée le 20 août 2025 ou après cette date) qui introduit de nouvelles obligations ou de nouveaux pouvoirs en matière de traitement des données à caractère personnel est présumée être soumise à la législation britannique en matière de protection des données. Cela signifie que le cadre britannique de protection des données continue de prévaloir sur d'autres législations. Conformément à l'article 183A, paragraphe 2, point b), de la loi DPA 2018, cette présomption peut être écartée si le Parlement britannique décide délibérément de le faire expressément dans la législation, en préservant la souveraineté parlementaire. Par ailleurs, l'article 186, paragraphe 2A, de la loi DPA 2018 précise que les limitations des droits des personnes concernées énumérées à l'article 186, paragraphe 3, de la loi DPA 2018 ne sont pas supplantées par l'article 186, paragraphe 1, de la loi DPA 2018, qui prévoit que les actes législatifs interdisant ou limitant la divulgation d'informations ne prévalent pas sur certains droits en matière de protection des données. Cela garantit, par exemple, que les limitations des droits des personnes concernées prévues par la loi DPA 2018 ne sont pas elles-mêmes visées par la «dérogation générale à la protection des données» prévue à l'article 186, paragraphe 1, de la loi DPA 2018.

(11) Deuxièmement, depuis l'adoption de la décision d'exécution (UE) 2021/1773, la législation du Royaume-Uni en matière de protection des données a été modifiée par la réglementation de 2023 relative à la protection des données (libertés et droits fondamentaux) (modification) ([14]). Cette réglementation définit les références aux droits fondamentaux ou aux libertés fondamentales contenues dans la loi DPA 2018 [qui étaient précédemment définies comme des références aux droits fondamentaux et aux libertés fondamentales prévus par le droit de l'Union ([15])] comme des références aux droits consacrés par la convention européenne des droits de l'homme, qui ont été mis en œuvre dans le droit national britannique par la loi de 1998 sur les droits de l'homme ([16]). La loi de 1998 sur les droits de l'homme intègre dans le droit britannique les droits contenus dans la convention européenne des droits de l'homme. La loi sur les droits de l'homme confère à toute personne les libertés et droits fondamentaux prévus aux articles 2 à 12 et 14 de la convention européenne des droits de l'homme, aux articles 1er, 2 et 3 de son premier protocole et à l'article 1er de son treizième protocole, lus en combinaison avec les articles 16, 17 et 18 de ladite convention. Ces droits comprennent le droit au respect de la vie privée et familiale (et à la protection des données à caractère personnel, qui fait partie dudit droit) et le droit à un procès équitable ([17]).

(12) Enfin, la loi DPA 2018 a fait l'objet de réformes ciblées prévues par les parties 5 et 6 de la loi sur les données (utilisation et accès). Bien que le champ d'application de la loi sur les données (utilisation et accès) aille bien au-delà de la protection des données à caractère personnel, cette loi apporte des modifications limitées à plusieurs aspects du régime de protection des données, tels que, notamment, les modalités d'exercice des droits des personnes concernées, les conditions régissant la prise de décision automatisée et la portée de certaines exigences en matière de responsabilité. En outre, la loi sur les données (utilisation et accès) apporte des modifications à la structure de gouvernance de l'ICO. Une fois mises en œuvre, ces mesures remplaceront l'ICO par une nouvelle entité, la commission de l'information. Le rôle et les fonctions de l'autorité de régulation en tant qu'autorité indépendante chargée de veiller à la protection des données au Royaume-Uni resteront inchangés. La loi investit également l'autorité de régulation de nouveaux pouvoirs d'exécution.

(13) La présente décision évalue les évolutions législatives, réglementaires et autres qui sont pertinentes pour la conclusion relative au niveau de protection assuré par le Royaume-Uni qui est formulée dans la décision d'exécution (UE) 2021/1773. L'évaluation effectuée dans la décision d'exécution (UE) 2021/1773 reste valable pour les aspects du cadre de protection des données du Royaume-Uni qui n'ont pas été modifiés ou concernés par d'autres évolutions depuis l'adoption de la décision d'exécution (UE) 2021/1773.

([12]) Article 5, paragraphe A2, de la loi de 2018 sur l'Union européenne (notification de retrait), telle que modifiée par la loi REUL.
([13]) Article 6, paragraphes 3 et 7, de la loi de 2018 sur l'Union européenne (notification de retrait), telle que modifiée par la loi REUL.
([14]) Disponible à l'adresse suivante: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.
([15]) Les droits fondamentaux et les libertés fondamentales prévus par le droit de l'Union avaient été conservés dans le droit britannique en vertu de l'article 4 de la loi de 2018 sur l'Union européenne (notification de retrait), qui a été abrogé à la fin de 2023 par la loi REUL.
([16]) Article 2, paragraphe 3, de la réglementation de 2023 relative à la protection des données (libertés et droits fondamentaux) (modification).
([17]) Articles 6, 8, 10 et 13 de la CEDH (voir, également, annexe 1 de la loi de 1998 sur les droits de l'homme), disponibles à l'adresse suivante: https://www.legislation.gov.uk/ukpga/1998/42/contents).

(14) Les évolutions législatives, réglementaires et autres qui sont pertinentes sont analysées en détail dans les sections suivantes sur la base du principe d'adéquation, selon lequel la Commission doit déterminer si le pays tiers en question assure un niveau de protection «essentiellement équivalent» à celui qui est garanti dans l'Union européenne ([18]). Comme l'a précisé la Cour de justice de l'Union européenne, il n'est pas nécessaire de constater un niveau de protection identique ([19]). En particulier, les moyens auxquels ce pays tiers a recours aux fins de la protection des données à caractère personnel peuvent être différents de ceux mis en œuvre au sein de l'Union, pour autant qu'ils s'avèrent, en pratique, effectifs afin d'assurer un niveau de protection adéquat ([20]). Le principe d'adéquation n'exige donc pas que l'on reproduise à l'identique les règles de l'Union. Il s'agit plutôt de déterminer si le système juridique étranger offre, dans son ensemble, par l'essence de ses droits en matière de protection des données et leur mise en œuvre effective, leur opposabilité et le contrôle de leur application, le niveau requis de protection ([21]).

2.1.1. *Définitions*

(15) Les notions de base en matière de protection des données qui correspondent à la terminologie de la directive (UE) 2016/680 continuent de s'appliquer dans le régime de protection des données du Royaume-Uni. Ces notions ont été évaluées aux considérants 26 et 27 de la décision d'exécution (UE) 2021/1773.

(16) En particulier, en introduisant une définition plus précise du «consentement» et en précisant les conditions d'obtention d'un tel consentement, la loi sur les données (utilisation et accès) confirme le cadre juridique qui régit l'utilisation du consentement en tant que base licite pour le traitement des données à caractère personnel ([22]). Les dispositions actualisées reproduisent le libellé du RGPD britannique, renforçant ainsi la cohérence entre les régimes de protection des données du Royaume-Uni. Cet alignement permet aux autorités compétentes d'interpréter de manière plus claire les conditions dans lesquelles le consentement peut servir de base juridique pour le traitement des données.

(17) Premièrement, l'article 69 de la loi sur les données (accès et utilisation) insère à l'article 33 de la loi DPA 2018 un nouveau paragraphe (le paragraphe 1A), où le «consentement» est défini comme une manifestation de volonté libre, spécifique, éclairée et univoque de la personne concernée. Cette manifestation de volonté doit prendre la forme d'une déclaration ou d'un acte positif clair et doit signifier que la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

(18) Deuxièmement, le même article insère dans la loi DPA 2018 un article 40A qui énonce les conditions à respecter lors de l'invocation du consentement. Le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné un consentement valable. Si le consentement est obtenu par écrit dans le cadre d'un document plus large, il doit être présenté d'une manière qui le distingue clairement des autres questions, en étant formulé en des termes accessibles, compréhensibles et simples. Aucune disposition du document qui ne respecte pas ces normes ne sera contraignante ([23]).

(19) Les responsables du traitement ou les sous-traitants doivent également informer la personne concernée, avant d'obtenir son consentement, de son droit de retirer son consentement. Le processus pour retirer son consentement doit être aussi simple que celui pour le donner. Cela garantit que la personne concernée conserve à tout moment un véritable contrôle sur l'utilisation des données à caractère personnel la concernant ([24]).

(20) Enfin, la loi sur les données (utilisation et accès) précise que, au moment de déterminer si le consentement est «donné librement», il est nécessaire d'examiner si la fourniture d'un service a été subordonnée à l'acceptation par la personne concernée du traitement de données à caractère personnel qui n'est pas requis pour la fourniture dudit service. Si tel est le cas, cela peut compromettre la validité du consentement ([25]).

([18]) Considérant 67 de la directive (UE) 2016/680.
([19]) Arrêt de la Cour dans l'affaire C-362/14, Schrems (ci-après l'«arrêt Schrems I»), ECLI:EU:C:2015:650, point 73.
([20]) Arrêt Schrems I, point 74.
([21]) Voir communication de la Commission au Parlement européen et au Conseil intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation» [COM(2017) 7 du 10.1.2017], section 3.1, p. 6 et 7, disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52017DC0007.
([22]) Articles 33 et 40A de la loi DPA 2018, tels qu'insérés par l'article 69, paragraphes 1, 2 et 4, de la loi sur les données (utilisation et accès).
([23]) Article 40A, paragraphes 2 et 3, de la loi DPA 2018, tels qu'insérés par l'article 69, paragraphe 4, de la loi sur les données (utilisation et accès).
([24]) Article 40A, paragraphes 5 et 6, de la loi DPA 2018, tels qu'insérés par l'article 69, paragraphe 4, de la loi sur les données (utilisation et accès).
([25]) Article 40A, paragraphe 7, de la loi DPA 2018, tel qu'inséré par l'article 69, paragraphe 4, de la loi sur les données (utilisation et accès).

(21) Il est important de noter que, en vertu de la partie 3 révisée de la loi DPA 2018, le consentement ne constitue toujours pas une base juridique pertinente pour les opérations de traitement relevant du champ d'application de la présente décision, comme expliqué au considérant 35 de la décision d'exécution (UE) 2021/1773. En outre, comme indiqué au considérant 36 de la décision d'exécution (UE) 2021/1773, le traitement dans un contexte répressif continue de ne pas être possible sur la base du consentement seul, puisqu'une autorité compétente doit toujours disposer d'un pouvoir sous-jacent qui lui permet de traiter les données. Plus précisément, à l'instar de ce qui est autorisé en vertu de la directive (UE) 2016/680 ([26]), cela signifie que le consentement fait office de condition supplémentaire pour permettre certaines opérations de traitement limitées et spécifiques qui pourraient autrement ne pas être effectuées, par exemple, la collecte et le traitement d'un échantillon ADN d'une personne qui n'est pas suspectée.

2.2. **Garanties, droits et obligations**

2.2.1. *Traitement des données à caractère personnel sensibles*

(22) Le cadre de protection des données du Royaume-Uni continue de prévoir des garanties spécifiques pour le traitement portant sur des catégories particulières de données, lesquelles ont été évaluées aux considérants 38 à 42 de la décision d'exécution (UE) 2021/1773.

(23) Tant la définition des catégories particulières de données à caractère personnel que les règles spécifiques applicables au traitement de ces catégories de données qui sont incluses dans la partie 3 de la loi DPA 2018 restent en place. Dans le même temps, la loi sur les données (utilisation et accès) investit le secrétaire d'État de nouveaux pouvoirs l'habilitant à adopter des règlements pour ajouter de nouvelles catégories particulières de données et adapter, si nécessaire, les conditions applicables à leur utilisation ([27]). Il est important de noter que ces pouvoirs ne permettent pas au secrétaire d'État de supprimer ou de modifier des catégories particulières de données existantes, ni de modifier les conditions régissant le traitement de ces catégories de données ([28]).

(24) Par conséquent, ces modifications n'ont pas d'incidence sur le niveau de protection garanti pour les catégories particulières de données à caractère personnel, qui avait été jugé essentiellement équivalent à la protection assurée au sein de l'Union dans la décision d'exécution (UE) 2021/1773.

2.2.2. *Droits individuels*

(25) En vertu du cadre juridique applicable au Royaume-Uni, les personnes concernées continuent de bénéficier des mêmes droits individuels que ceux que prévoit la directive (UE) 2016/680, et elles peuvent opposer ces droits au responsable du traitement ou au sous-traitant. Il s'agit en particulier du droit d'accès aux données, du droit de s'opposer au traitement et du droit à la rectification et à l'effacement des données, comme indiqué aux considérants 57 à 65 de la décision d'exécution (UE) 2021/1773.

(26) La loi sur les données (utilisation et accès) clarifie certaines modalités d'exercice de ces droits.

(27) Premièrement, en vertu du régime actuel, les responsables du traitement ont le droit de rejeter une demande ou d'exiger le paiement de frais raisonnables si une demande est manifestement infondée ou excessive ([29]). À cet égard, la loi sur les données (utilisation et accès) investit le secrétaire d'État d'un nouveau pouvoir l'habilitant à adopter des règlements pour exiger des responsables du traitement qu'ils produisent et publient des orientations concernant les frais qu'ils exigent dans de telles circonstances. En outre, la loi sur les données (utilisation et accès) clarifie que lorsque les responsables du traitement refusent de donner suite à une demande pour les motifs susmentionnés, ils restent tenus de notifier les motifs du refus à la personne concernée et de l'informer de son droit d'introduire une réclamation auprès du commissaire à l'information. Cette notification doit être effectuée dans les meilleurs délais ([30]).

(28) Deuxièmement, la loi sur les données (utilisation et accès) précise les délais dans lesquels les responsables du traitement doivent répondre aux demandes de la personne concernée. Plus précisément, elle aligne les délais de réponse requis sur ceux que prévoit le RGPD britannique. Les dispositions révisées permettent également de prolonger le délai de réponse d'un maximum de deux mois dans le cas d'une demande complexe ou si plusieurs

([26]) Voir considérants 35 et 37 de la directive (UE) 2016/680.

([27]) Article 74 de la loi sur les données (utilisation et accès). Ces règlements sont soumis à une procédure de ratification, ce qui signifie qu'ils nécessitent l'approbation expresse du Parlement britannique.

([28]) Voir nouvel article 42A de la loi DPA 2018 inséré par l'article 74 de la loi sur les données (utilisation et accès), ainsi que notes explicatives accompagnant le projet de loi sur les données (utilisation et accès), point 577, disponibles à l'adresse suivante: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

([29]) Article 53, paragraphe 1, de la loi DPA 2018. Voir, également, considérant 64 de la décision d'exécution (UE) 2021/1773.

([30]) Paragraphes 4A, 6 et 7 de l'article 53 de la loi DPA 2018, tels qu'insérés par l'article 75 de la loi sur les données (utilisation et accès).

demandes sont reçues. Dans de telles circonstances, le responsable du traitement doit informer la personne concernée de la prorogation du délai et des motifs qui la sous-tendent ([31]). La loi sur les données (utilisation et accès) a par ailleurs introduit un mécanisme permettant aux responsables du traitement de suspendre le délai de réponse à une demande lorsque des informations complémentaires de la part de la personne concernée sont nécessaires pour identifier les données demandées ([32]).

(29) Troisièmement, en ce qui concerne uniquement le droit d'accès aux informations et aux données à caractère personnel, la loi sur les données (utilisation et accès) modifie l'article 45 de la loi DPA 2018 pour intégrer la clarification apportée par la jurisprudence nationale – en s'appuyant sur le principe de proportionnalité du droit de l'Union – qui précise que les responsables du traitement ne doivent effectuer que des recherches raisonnables et proportionnées pour obtenir les informations et les données à caractère personnel demandées ([33]). La nouvelle disposition devrait être interprétée conformément à la jurisprudence existante, qui prévoit que «[…] ce qui est mis en balance dans l'examen de proportionnalité est l'objet final de la recherche, à savoir l'avantage potentiel que la fourniture d'informations pourrait apporter à la personne concernée, par rapport aux moyens par lesquels ces informations sont obtenues. Il s'agira d'évaluer dans chaque cas particulier si des efforts disproportionnés seront nécessaires pour trouver et fournir les informations par rapport aux avantages que cela pourrait apporter à la personne concernée» ([34]).

(30) Par conséquent, si les modalités de réponse aux demandes des personnes concernées sont soumises à des règles plus détaillées, le système en place au Royaume-Uni continue de garantir que les demandes des personnes concernées doivent être traitées dans des délais raisonnables, définis sur la base de facteurs objectifs. En outre, les obligations matérielles qui incombent aux responsables du traitement lorsqu'ils répondent à une demande d'accès sont encadrées par des normes juridiques établies qui tiennent également compte des intérêts de la personne concernée. Enfin, les orientations actuelles de l'ICO précisent déjà qu'un responsable du traitement n'est pas tenu d'effectuer des recherches qui seraient déraisonnables ou disproportionnées par rapport à l'importance de donner accès aux informations ([35]).

(31) Par ailleurs, la loi sur les données (utilisation et accès) a inséré dans la loi DPA 2018 un nouvel article (l'article 45A), qui crée une exemption explicite à l'obligation de fournir un accès ou des informations à la personne concernée lorsque les informations sont protégées par le secret professionnel ([36]). Cette exemption s'applique spécifiquement aux obligations prévues par l'article 44, paragraphe 2, et l'article 45, paragraphe 1, de la loi DPA 2018, qui imposent aux responsables du traitement d'informer la personne concernée du traitement de données à caractère personnel la concernant et de lui donner accès à ces données ([37]). Elle précise que les responsables du traitement ne sont pas tenus de divulguer des informations si, ce faisant, ils enfreignent le secret professionnel. Une exemption similaire existe au titre du RGPD britannique ([38]).

(32) En ce qui concerne les garanties, lorsqu'ils se prévalent de cette exemption, les responsables du traitement doivent informer la personne concernée par écrit, dans les meilleurs délais, de l'application de l'exemption, motiver cette décision et notifier à la personne concernée son droit de demander un réexamen par la commission de l'information ou les voies de recours disponibles ([39]). Afin de garantir la responsabilité, l'article 45A, paragraphe 4, de la loi DPA 2018 exige des responsables du traitement qu'ils conservent une trace de l'origine de leur décision d'appliquer l'exemption et mettent ce registre à la disposition de la commission de l'information, à sa demande ([40]).

([31]) Paragraphes 3A et b3 de l'article 54 de la loi DPA 2018, tels qu'insérés par l'article 76, paragraphe 6, de la loi sur les données (utilisation et accès).

([32]) Paragraphes 3C et 3D de l'article 54 de la loi DPA 2018, tels qu'insérés par l'article 76, paragraphes 5 et 6, de la loi sur les données (utilisation et accès).

([33]) Paragraphe 2A de l'article 45 de la loi DPA 2018, tel qu'inséré par l'article 78 de la loi sur les données (utilisation et accès).

([34]) Dawson-Dammer contre Taylor Wessing LLP [2017] EWCA Civ 74.

([35]) Disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([36]) Article 45A, tels qu'inséré par l'article 79, de la loi sur les données (utilisation et accès). Au Royaume-Uni, le secret professionnel est un droit juridique fondamental qui protège des communications confidentielles spécifiques entre un client et son conseil juridique, ces communications ne pouvant être divulguées sans le consentement du client. Il se décline en deux grandes catégories: la confidentialité des conseils juridiques, qui protège les échanges effectués dans le but d'obtenir ou de fournir des conseils juridiques, et la confidentialité ad litem, qui s'applique aux communications effectuées en préparation ou au cours d'une procédure judiciaire.

([37]) Les autorités compétentes au titre de la partie 3 se sont précédemment appuyées sur d'autres exemptions disponibles au titre de l'article 44, paragraphe 4 (Droit d'être informé), et de l'article 45, paragraphe 4 (Droit d'accès), de la loi DPA 2018.

([38]) Annexe 2, point 19, de la loi DPA 2018.

([39]) Article 45A, paragraphe 2, de la loi DPA 2018, tel qu'inséré par l'article 79 de la loi sur les données (utilisation et accès). Une exception à cette obligation de notification s'applique lorsque la notification porterait atteinte au secret ou à la confidentialité des informations. Dans de telles circonstances, le responsable du traitement n'est pas tenu de révéler que l'exemption a été appliquée ni de fournir d'autres explications.

([40]) Paragraphe 45A de la loi DPA 2018, tel qu'inséré par l'article 79 de la loi sur les données (utilisation et accès).

(33) Enfin, la loi sur les données (utilisation et accès) a modifié et consolidé les exemptions existantes accordées conformément à la partie 3 de la loi DPA 2018 aux autorités compétentes à des fins de sécurité nationale. L'exemption en matière de sécurité nationale permet aux autorités compétentes de ne pas appliquer certaines dispositions de la partie 3 de la loi DPA 2018 si une dérogation à celles-ci est nécessaire aux fins de la sauvegarde de la sécurité nationale ([41]). Il reflète les exemptions en matière de sécurité nationale prévues pour le traitement des données à caractère personnel en vertu du RGPD britannique (article 26 de la loi DPA 2018) et de la partie 4 de la loi DPA 2018 (article 110 de la loi DPA 2018).

(34) L'exemption liée à la sécurité nationale est soumise aux mêmes limitations et garanties que les exemptions prévues par le RGPD britannique et la partie 4 de la loi DPA 2018, telles qu'analysées aux considérants 64 à 67 et 126 de la décision d'exécution (UE) 2021/1772. En particulier, l'exemption ne peut être appliquée que dans la mesure où elle est nécessaire pour garantir la sécurité nationale. Il ne s'agit pas d'une exemption générale. Elle doit être examinée et invoquée par le responsable du traitement au cas par cas ([42]). De plus, toute application de l'exemption doit être conforme aux normes relatives aux droits de l'homme (fondées sur la loi de 1998 sur les droits de l'homme et sur la Convention européenne des droits de l'homme), selon lesquelles toute ingérence dans l'exercice du droit au respect de la vie privée devrait, dans une société démocratique, constituer une mesure nécessaire et proportionnée ([43]). Cela est également confirmé dans les orientations de l'ICO sur l'application des dérogations en matière de sécurité nationale ([44]).

2.2.3. *Limitations concernant les transferts ultérieurs*

(35) Le niveau de protection conféré aux données à caractère personnel qui sont transférées de l'Union européenne vers une autorité répressive au Royaume-Uni continue de ne pas être compromis par le transfert ultérieur de ces mêmes données vers des destinataires se trouvant dans un pays tiers. Le régime applicable aux transferts internationaux de données à caractère personnel depuis le Royaume-Uni reste très proche des règles énoncées au chapitre V de la directive (UE) 2016/680, comme indiqué aux considérants 74 à 87 de la décision d'exécution (UE) 2021/1773.

(36) Bien que la loi sur les données (utilisation et accès) ait modifié le chapitre 5 de la partie 3 de la loi DPA 2018 concernant les transferts de données à caractère personnel vers des autorités compétentes de pays tiers, elle maintient les exigences essentielles selon lesquelles a) le transfert doit être nécessaire à des fins répressives; b) le transfert doit être i) fondé sur des règlements approuvant le transfert (remplaçant les règlements d'adéquation antérieurs), ii) soumis à des garanties appropriées, ou iii) fondé sur des circonstances particulières; et c) le destinataire du transfert doit être: i) une autorité pertinente (c'est-à-dire l'équivalent d'une autorité compétente) dans le pays tiers, ii) une organisation internationale compétente, iii) un sous-traitant traitant des données au nom d'une autorité compétente ou iv) une personne autre qu'une autorité pertinente, mais uniquement lorsque le transfert est strictement nécessaire à l'une des fins répressives ([45]). Ces principes généraux applicables aux transferts de données se reflètent à l'article 73 de la loi DPA 2018, qui précise également que les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale ne sont autorisés que si le transfert est effectué conformément aux autres dispositions de la partie 3 de la loi DPA 2018 ([46]).

(37) En ce qui concerne plus particulièrement les règlements approuvant un transfert, l'article 74AA, paragraphe 2, de la loi DPA 2018 précise que le secrétaire d'État ne peut établir de tels règlements que s'il considère que le critère de la protection des données est rempli. Cela signifie que la possibilité, introduite à l'article 74AA, paragraphe 3, de la loi DPA 2018, pour le secrétaire d'État de tenir compte de l'opportunité de faciliter les flux de données lors de l'adoption de tels règlements est toujours subordonnée à la condition que le critère de la protection des données soit rempli. Le nouvel article 74AB ([47]) de la loi DPA 2018 définit la norme juridique applicable au respect du critère de la protection des données, en exigeant que le niveau de protection des personnes concernées assuré dans les pays destinataires ou par les organisations internationales ne soit pas sensiblement inférieur à la norme prévue pour les personnes concernées par la législation britannique pertinente en matière de protection des données. L'article 74AB

([41]) Article 78A, paragraphe 1, de la loi DPA 2018, tel qu'inséré par l'article 88 de la loi sur les données (utilisation et accès). Conformément à l'article 78A, paragraphes 2 à 4, de la loi DPA 2018, l'exemption permet de ne pas appliquer les principes de protection des données (à l'exception du principe de licéité et des conditions et garanties applicables au traitement des données sensibles), les droits individuels, les obligations des responsables du traitement et des sous-traitants en ce qui concerne les violations de données, certaines parties des règles relatives aux transferts de données à l'échelle internationale et certains pouvoirs conférés au commissaire à l'information en vue de la réalisation d'inspections et de l'adoption de mesures coercitives.

([42]) Voir l'arrêt dans l'affaire Baker/Secretary of State for the Home Department [2001] UKIT NSA2 («Baker/Secretary of State»).

([43]) Voir également l'arrêt dans l'affaire Guriev/Community Safety Development (UK) Ltd [2016] EWHC 643 (QB), point 45, et l'arrêt dans l'affaire Lin/Commissioner of the Police for the Metropolis [2015] EWHC 2484 (QB), point 80.

([44]) Voir les orientations d'ICO sur l'exception en matière de sécurité et de défense nationales, disponibles à l'adresse suivante: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([45]) Article 73 de la loi DPA 2018, tel que modifié par les points 3, 4), et 3, 5), de l'annexe 8 de la loi sur les données (utilisation et accès).

([46]) Article 73 de la loi DPA 2018, tel que modifié par le point 3, 3), de l'annexe 8 de la loi sur les données (utilisation et accès).

([47]) Tel qu'inséré par le point 4, 2), de l'annexe 8 de la loi sur les données (utilisation et accès).

de la loi DPA 2018 dresse ensuite, à son paragraphe 2, une liste non exhaustive d'éléments à prendre en considération pour évaluer si ce critère est rempli, tels que le respect de l'état de droit et des droits de l'homme, l'existence d'une autorité chargée de la protection des données et ses pouvoirs, les modalités de recours juridictionnel ou extrajudiciaire, les règles relatives au transfert de données à caractère personnel du pays ou de l'organisation vers d'autres pays ou organisations internationales, les obligations internationales pertinentes du pays ou de l'organisation, ainsi que la constitution, les traditions et la culture du pays ou de l'organisation. Bien qu'elle reformule la liste des éléments pertinents prévue à l'ancien article 74A de la loi DPA 2018, la nouvelle disposition conserve les éléments essentiels de cette liste et reste donc proche de ce qui est prévu à l'article 36 de la directive (UE) 2016/680. En outre, les autorités britanniques ont confirmé que le secrétaire d'État tiendra compte d'éléments qui ne sont pas énumérés à l'article 74AB, paragraphe 2, tels que les lois et pratiques d'un pays tiers concernant la manière dont les autorités publiques accèdent aux données à caractère personnel à des fins telles que la sécurité nationale ou l'application des lois, dans la mesure où ces éléments ont une incidence sur le niveau global de protection. Par ailleurs, les autorités britanniques considèrent que la jurisprudence pertinente du pays tiers sera un élément essentiel lors de l'examen des questions énumérées de manière non exhaustive à l'article 74AB, paragraphe 2, de la loi DPA 2018.

(38) Les règlements approuvant un transfert continuent d'être soumis aux règles de procédure «générales» prévues à l'article 182 de la loi DPA 2018, comme indiqué au considérant 77 de la décision d'exécution (UE) 2021/1773. Dans le cadre de cette procédure, le secrétaire d'État doit consulter le commissaire à l'information lorsqu'il propose à l'adoption des règlements d'adéquation ([48]). Une fois adoptés par le secrétaire d'État, ces règlements sont présentés au Parlement et sont soumis à la procédure de «résolution négative» dans le cadre de laquelle les deux chambres du Parlement peuvent examiner les règlements et déposer une motion en vue de leur annulation dans un délai de 40 jours ([49]).

(39) En ce qui concerne les garanties appropriées, l'article 75 de la loi DPA 2018, tel que modifié par le point 6 de l'annexe 8 de la loi sur les données (utilisation et accès), prévoit que ces transferts ne peuvent avoir lieu que si: a) un instrument juridique approprié lie le destinataire prévu des données, c'est-à-dire un instrument qui remplit les conditions énoncées au nouveau paragraphe 4, en particulier le fait que chaque autorité compétente du Royaume-Uni partie à l'instrument, agissant de manière raisonnable et proportionnée, considère que le critère de la protection des données est rempli, ou b) si le responsable du traitement, agissant de manière raisonnable et proportionnée, considère que le critère de la protection des données est rempli en ce qui concerne le transfert ou ce type de transfert. Le nouveau paragraphe 5 de l'article 75 de la loi DPA 2018 précise que le critère de la protection des données est rempli si, grâce aux garanties requises, le niveau de protection prévu pour les personnes concernées n'est pas sensiblement inférieur, après le transfert, à la norme prévue par la législation britannique pertinente en matière de protection des données. Cela est similaire aux mesures prévues à l'article 37 de la directive (UE) 2016/680. En conséquence, les mêmes normes juridiques s'appliquent dans l'Union et au Royaume-Uni en ce qui concerne l'approbation d'un transfert sous réserve de garanties appropriées. Selon le nouveau paragraphe 6 de l'article 75 de la loi DPA 2018, ce qui est raisonnable et proportionné doit être déterminé au regard de toutes les circonstances, ou circonstances probables, entourant le transfert ou le type de transfert, notamment la nature et le volume des données à caractère personnel transférées.

(40) En ce qui concerne les transferts fondés sur des circonstances particulières conformément à l'article 76 de la loi DPA 2018, plusieurs modifications techniques sont apportées pour clarifier les conditions dans lesquelles ces transferts peuvent avoir lieu, mais sans avoir d'incidence sur le niveau de protection des données à caractère personnel assuré par le Royaume-Uni ([50]).

(41) En ce qui concerne la mise en œuvre des règles britanniques applicables aux transferts internationaux, plusieurs évolutions ont eu lieu depuis l'adoption de la décision d'exécution (UE) 2021/1773.

(42) Premièrement, à la suite de la conclusion entre le ministère de l'intérieur et l'ICO, en 2022, d'un protocole d'accord définissant leur rôle respectif dans la réalisation d'évaluations de l'adéquation de la protection des données dans le domaine répressif ([51]), le Royaume-Uni a évalué les cadres de protection des données dans les bailliages de Jersey et de

([48]) Voir le protocole d'accord entre le secrétaire d'État au ministère du numérique, de la culture, des médias et du sport (Department for Digital, Culture, Media and Sport) et le bureau du commissaire à l'information sur le rôle de l'ICO dans le cadre de la nouvelle évaluation de l'adéquation au Royaume-Uni, disponible à l'adresse suivante: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([49]) Si une telle motion est adoptée, les règlements cesseront à terme de produire tout autre effet juridique.

([50]) Point 7) de l'annexe 8 de la loi sur les données (utilisation et accès).

([51]) Disponible à l'adresse suivante: https://ico.org.uk/media2/about-the-ico/mou/4025752/ico-ho-mou.pdf.

Guernesey, ainsi que dans l'île de Man. À la suite de ce processus, le Royaume-Uni a adopté des règlements d'adéquation pour Guernesey en juillet 2023 ([52]), pour Jersey en novembre 2023 ([53]) et pour l'île de Man en janvier 2025 ([54]). Ces règlements confirment que chaque territoire assure un niveau adéquat de protection des données à caractère personnel transférées en vertu de la partie 3 de la loi DPA 2018. Bien que ces règlements aient été initialement adoptés au titre du cadre juridique précédent, l'évaluation qui les sous-tend reste valable dans le cadre actualisé. En conséquence, les règlements continuent de faciliter la coopération internationale dans le domaine répressif.

(43) La Commission a également évalué les cadres de protection des données pour le traitement des données à caractère personnel à des fins répressives, ainsi que les règles relatives à l'accès des autorités publiques aux données à caractère personnel à des fins de sécurité nationale dans les bailliages de Jersey et de Guernesey, ainsi que dans l'île de Man, lors de l'évaluation du fonctionnement des décisions d'adéquation adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE conformément à l'article 97 du règlement (UE) 2016/679. Sur la base, entre autres, de cette évaluation, la Commission a conclu que ces trois pays et territoires continuaient d'assurer un niveau de protection adéquat des données à caractère personnel transférées de l'Union ([55]).

(44) Deuxièmement, en 2022, le Royaume-Uni et les États-Unis ont conclu un accord sur la protection des données et le respect de la vie privée ([56]) qui applique mutatis mutandis les termes de l'accord-cadre Union européenne - États-Unis ([57]), garantissant des protections équivalentes dans le cadre des échanges de données entre le Royaume-Uni et les États-Unis à des fins répressives.

(45) Troisièmement, en 2023 et 2025, l'ICO a mis à jour ses orientations sur les transferts internationaux au titre du chapitre 5 de la partie 3 de la loi DPA 2018 ([58]). La mise à jour de 2023 a clarifié le sens de l'exigence «strictement nécessaire» pour les transferts de données à des destinataires autres que les autorités répressives pertinentes, ce qui offre une plus grande certitude aux responsables du traitement qui évaluent la légalité de ces transferts. En 2025, la liste des pays et territoires adéquats a été mise à jour à la suite des règlements d'adéquation du Royaume-Uni pour l'île de Man.

2.2.4. *Prise de décision automatisée*

(46) Bien qu'elle conserve plusieurs éléments des règles relatives à la prise de décision automatisée évaluées aux considérants 72 et 73 de la décision d'exécution (UE) 2021/1773, la loi sur les données (utilisation et accès) a modifié certains aspects de ces règles.

(47) Premièrement, le nouvel article 50B de la loi DPA 2018 interdit de manière générale les décisions déterminantes fondées entièrement ou partiellement sur le traitement portant sur des catégories particulières de données à caractère personnel. Toutefois, deux exceptions à cette interdiction sont prévues: la personne concernée a donné son consentement explicite à ce traitement; ou la décision est nécessaire ou autorisée par la loi ([59]).

(48) Deuxièmement, le nouvel article 50C de la loi DPA 2018 prévoit que les responsables du traitement mettent en œuvre des garanties pour toute décision déterminante fondée entièrement ou partiellement sur des données à caractère personnel et fondée exclusivement sur un traitement automatisé. Ces garanties doivent comprendre la

([52]) Disponible à l'adresse suivante: https://www.legislation.gov.uk/uksi/2023/1221/contents/made.
([53]) Disponible à l'adresse suivante: https://www.legislation.gov.uk/uksi/2023/744/made.
([54]) Disponible à l'adresse suivante: https://www.legislation.gov.uk/uksi/2025/89/contents/made.
([55]) Rapport de la Commission au Parlement européen et au Conseil sur le premier réexamen du fonctionnement des décisions d'adéquation adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE du 15 janvier 2024, disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52024DC0007; et rapports par pays sur le fonctionnement des décisions d'adéquation adoptées en vertu de la directive 95/46/CE accompagnant le rapport de la Commission au Parlement européen et au Conseil sur le premier réexamen du fonctionnement des décisions d'adéquation adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE, disponible à l'adresse suivante: https://commission.europa.eu/document/download/f8229eb2-1a36-4cf5-a099-1cd001664bff_en?filename=JUST_template_comingsoon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf.
([56]) Disponible à l'adresse suivante: https://www.gov.uk/government/publications/ukusa-exchange-of-notes-on-the-protection-of-personal-information-relating-to-prevention-investigation-detection-and-prosecution-of-criminal-offe.
([57]) Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière (JO L 336 du 10.12.2016, p. 3), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:22016A1210(01)&from=FR.
([58]) Disponible à l'adresse suivante: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/international-transfers/.
([59]) Article 50B de la loi DPA 2018, tel qu'inséré par l'article 80, paragraphe 3, de la loi sur les données (utilisation et accès).

fourniture d'informations à la personne concernée sur le processus décisionnel, la possibilité pour la personne concernée de contester la décision ou de formuler des observations, et le droit pour la personne concernée de demander une intervention humaine dans le processus décisionnel ([60]). Bien que l'article 50C, paragraphe 4, de la loi DPA 2018 prévoie une exemption de l'application de ces garanties si cette exemption est nécessaire pour éviter de gêner une enquête, une recherche ou une procédure officielle ou judiciaire, pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière ou à l'exécution de sanctions pénales, pour protéger la sécurité publique, ou pour protéger la sécurité nationale ou protéger les droits et libertés d'autrui, l'application de ces garanties n'est suspendue que temporairement, étant donné que le responsable du traitement est tenu de revoir la décision dès que cela est raisonnablement possible et que le réexamen de la décision nécessite une intervention humaine significative ([61]).

(49) En outre, le nouvel article 50A de la loi DPA 2018 clarifie la définition d'une décision qui est «fondée exclusivement sur un traitement automatisé» en prévoyant qu'il s'agit d'une décision qui ne nécessite aucune intervention humaine significative dans le processus décisionnel. Il est important de noter que les responsables du traitement sont tenus d'évaluer la mesure dans laquelle le profilage contribue à une décision afin de déterminer si l'intervention humaine a été significative. L'article 50A de la loi DPA 2018 précise également qu'une «décision déterminante» est une décision qui produit des effets juridiques préjudiciables pour la personne concernée ou des effets d'une importance similaire ([62]). Cette limitation aux décisions qui ont un effet préjudiciable sur la personne concernée reflète le fait que, contrairement au traitement en vertu du RGPD britannique, il est peu probable que les autorités compétentes prennent des décisions considérées comme positives par les personnes concernées.

(50) Enfin, le nouvel article 50D de la loi DPA 2018 investit le secrétaire d'État du pouvoir d'adopter des actes de droit dérivé afin de décrire ce qui constitue, et ce qui ne constitue pas, une intervention humaine significative et quelles décisions sont, et ne sont pas, considérées comme produisant des effets préjudiciables d'une importance similaire sur les personnes concernées. Il permet aussi au secrétaire d'État d'adopter des actes de droit dérivé afin i) d'ajouter de nouvelles garanties; ii) d'imposer des exigences complétant les garanties existantes; et iii) de définir les mesures qui ne satisfont pas aux garanties ([63]). Il est important de noter qu'avant d'adopter des règlements conformément à l'article 50D de la loi DPA 2018, le secrétaire d'État doit consulter l'ICO ([64]), et que les règlements sont soumis à la procédure de résolution positive ([65]), ce qui signifie qu'ils doivent être approuvés par les deux chambres du Parlement britannique avant de pouvoir être adoptés.

(51) Bien que la loi sur les données (utilisation et accès) ait donc modifié le cadre régissant la prise de décision automatisée, il importe de noter que le cadre juridique du Royaume-Uni continue de prévoir que la prise de décision automatisée est soumise à la garantie essentielle exigeant le droit d'obtenir une intervention humaine dans tous les cas de prise de décision automatisée, c'est-à-dire pour le traitement de données à caractère personnel sensibles comme non sensibles ([66]).

2.2.5. *Obligation de rendre compte*

(52) Le cadre juridique du Royaume-Uni continue d'appliquer le principe de responsabilité consacré par la directive (UE) 2016/680, en vertu duquel les autorités publiques sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir et démontrer le respect des obligations en matière de protection des données, comme indiqué aux considérants 88 à 92 de la décision d'exécution (UE) 2021/1773.

(53) L'une des mesures prévues par la loi DPA 2018 pour garantir la responsabilité et permettre aux responsables du traitement et aux sous-traitants d'apporter la preuve qu'ils respectent leurs obligations consiste à obliger les autorités compétentes à tenir des registres de leurs activités de traitement, y compris la collecte, la modification, la consultation, la divulgation, la combinaison et l'effacement de données à caractère personnel ([67]). La loi sur les données (utilisation et accès) modifie les obligations spécifiques qui incombent aux responsables du traitement en vertu de cette disposition en supprimant uniquement, à l'article 62 de la loi DPA 2018, l'obligation pour les responsables du traitement d'enregistrer une justification lorsque des données à caractère personnel sont consultées ou divulguées ([68]). Il est important de noter que l'obligation pour les responsables du traitement de tenir des registres de leurs activités de traitement reste en place en tant que telle, ce qui signifie que le principal mécanisme permettant de garantir la responsabilité est maintenu.

([60]) Article 50C de la loi DPA 2018, tel qu'inséré par l'article 80, paragraphe 3, de la loi sur les données (utilisation et accès).
([61]) Article 50C, paragraphes 3 et 4, de la loi DPA 2018, tels qu'insérés par l'article 80, paragraphe 3, de la loi sur les données (utilisation et accès).
([62]) Article 50A de la loi DPA 2018, tel qu'inséré par l'article 80, paragraphe 3, de la loi sur les données (utilisation et accès).
([63]) Article 50D de la loi DPA 2018, tel qu'inséré par l'article 80, paragraphe 3, de la loi sur les données (utilisation et accès). Tout règlement adopté dans le cadre de ces pouvoirs est soumis à la procédure de ratification, assurant ainsi le contrôle parlementaire. Les règlements ne peuvent modifier les exigences énoncées à l'article 50C.
([64]) Article 182, paragraphe 2, de la loi DPA 2018.
([65]) Article 50D, paragraphe 5, de la loi DPA 2018.
([66]) Article 50C, paragraphe 2, c), de la loi DPA 2018.
([67]) Article 62 de la loi DPA 2018. Voir, également, considérant 90 de la décision d'exécution (UE) 2021/1773.
([68]) Article 82 de la loi sur les données (utilisation et accès).

2.3. **Surveillance et contrôle de l'application des règles**

2.3.1. *Surveillance indépendante*

(54) Au Royaume-Uni, une autorité indépendante chargée de veiller à la protection des données continue de surveiller l'application du cadre de protection des données et de le faire respecter, comme indiqué aux considérants 93 à 99 de la décision d'exécution (UE) 2021/1773. La loi sur les données (utilisation et accès) améliore la structure de gouvernance de cette autorité en créant une personne morale constituée en société, l'*Information Commission* (ci-après la «commission de l'information»), qui remplacera l'ICO, lequel était structuré comme une personne morale individuelle.

(55) Plus précisément, les mesures de gouvernance énoncées dans la loi sur les données (utilisation et accès), une fois mises en œuvre, supprimeront le bureau du commissaire à l'information et transféreront les fonctions, le personnel et les biens de l'ICO à la nouvelle entité, la commission de l'information. La commission de l'information est composée de membres exécutifs et non exécutifs ([69]). En outre, en vertu de la loi, le commissaire à l'information se voit confier le poste de président de la commission de l'information, qui est l'un des membres non exécutifs ([70]). La loi sur les données (utilisation et accès) prévoit en outre que, dans la mesure où cela est approprié en raison du transfert de fonctions, les références au commissaire à l'information dans tous les actes législatifs ou autres documents (lorsqu'ils sont adoptés ou émis) doivent être lues comme des références à la commission de l'information. Dans l'exercice de ses fonctions, la commission peut instituer des comités et déléguer certaines fonctions à un membre, à un employé ou à l'un de ses comités ([71]) et peut prendre des dispositions concernant ses propres procédures et celles que doivent suivre les comités, y compris pour ce qui est du quorum et la prise de décisions à la majorité. Ces procédures doivent être rendues publiques ([72]).

(56) Il convient de noter que l'indépendance de la commission de l'information est soumise aux mêmes garanties, y compris en ce qui concerne les règles relatives à la nomination et à la révocation du président, que celles qui font l'objet d'une appréciation aux considérants 95 à 98 de la décision d'exécution (UE) 2021/1773 ([73]). Des garanties similaires s'appliquent en ce qui concerne les autres membres non exécutifs de la commission de l'information. En particulier, le président de la commission de l'information est nommé par Sa Majesté sur recommandation du secrétaire d'État. Il est sélectionné sur la base de ses compétences à l'issue d'un concours équitable et ouvert ([74]). Les autres membres non exécutifs sont nommés par le secrétaire d'État, après consultation du président. Les candidats ne peuvent être recommandés en vue de leur nomination ou ne peuvent être nommés que s'ils sont sélectionnés sur la base de leurs compétences à l'issue d'un concours équitable et ouvert et que si le secrétaire d'État estime qu'ils ne se trouvent pas dans une situation de conflit d'intérêts ([75]). Les membres exécutifs sont des membres de la commission de l'information soumis aux règles et conditions fixées par les membres non exécutifs ([76]). Le directeur est nommé par le président et les autres membres non exécutifs après consultation du secrétaire d'État. Les membres exécutifs sont également nommés sur la base de leurs compétences à l'issue d'un concours équitable et ouvert ([77]).

(57) Le président ne peut être démis de ses fonctions que par Sa Majesté sur requête des deux chambres du Parlement et uniquement si le secrétaire d'État a présenté à la chambre un rapport dont il ressort que le président a commis une faute grave, qu'il se trouve dans une situation de conflit d'intérêts, qu'il ne s'est pas conformé aux exigences spécifiques en matière d'information quant à l'existence d'éventuels conflits d'intérêts ou qu'il n'est pas à même d'accomplir les fonctions inhérentes à la présidence, qu'il se trouve dans l'incapacité de les accomplir ou qu'il n'est pas disposé à les accomplir ([78]). Les membres non exécutifs ne peuvent être démis de leurs fonctions par le secrétaire d'État que si celui-ci estime que les conditions spécifiques énoncées dans la législation sont réunies. Parmi ces conditions figurent l'existence d'un conflit d'intérêts, le fait d'avoir commis une faute grave ou le fait de ne pas être à même d'accomplir leurs fonctions, de ne pas être disposés à les accomplir ou de se trouver dans l'incapacité de les accomplir. En termes de garanties supplémentaires, le secrétaire d'État est tenu de publier la décision de révocation et de fournir au membre un exposé des motifs de sa révocation ([79]).

([69]) Point 3.1 de l'annexe 12A de la loi DPA 2018.
([70]) Articles 117, 118, 119 et 120, lus en combinaison avec l'annexe 14 de la loi sur les données (utilisation et accès).
([71]) Points 13 et 14 de l'annexe 12A de la loi DPA 2018.
([72]) Point 16 de l'annexe 12A de la loi DPA 2018.
([73]) Article 52 du RGPD britannique, ainsi qu'annexe 12A de la loi DPA 2018, telle qu'insérée par l'article 117 du projet de loi sur les données (utilisation et accès).
([74]) Point 5.1 de l'annexe 12A de la loi DPA 2018.
([75]) Points 3.2, 5 et 6 de l'annexe 12A de la loi DPA 2018.
([76]) Point 11 de l'annexe 12A de la loi DPA 2018.
([77]) Point 5.2 de l'annexe 12A de la loi DPA 2018.
([78]) Points 7.6 et 7.7 de l'annexe 12A de la loi DPA 2018.
([79]) Points 9.6, 9.7, 9.8 et 9.9 de l'annexe 12A de la loi DPA 2018.

(58) La loi sur les données (utilisation et accès) ne modifie pas les principales responsabilités de la commission de l'information, qui continuera d'exercer les fonctions énoncées à l'annexe 13 de la loi DPA 2018. Celle-ci est notamment chargée de surveiller l'application de la partie 3 de la loi DPA 2018 et de la faire respecter, de conseiller le Parlement et le gouvernement, de sensibiliser le public, d'aider les responsables du traitement et les sous-traitants à remplir leurs obligations et d'informer les personnes concernées de leurs droits ([80]). La loi sur les données (utilisation et accès) précise que, dans l'exercice de son obligation de garantir un niveau approprié de protection des données à caractère personnel, la commission de l'information devra tenir compte des intérêts des personnes concernées, des responsables du traitement et de tiers, prendre en considération l'intérêt public au sens large et promouvoir la confiance du public dans le traitement des données à caractère personnel ([81]).

(59) En outre, la loi sur les données (utilisation et accès) précise que la commission de l'information tient compte, dans la mesure où cela est pertinent, de l'opportunité d'encourager l'innovation et la concurrence, de l'importance de la prévention et de la détection des infractions pénales ainsi que des enquêtes et des poursuites en la matière, de la nécessité de préserver la sécurité publique et la sécurité nationale, de même que des besoins spécifiques liés à la protection des enfants dans l'exercice de sa fonction au titre de la législation sur la protection des données ([82]). La législation de l'Union en matière de protection des données reconnaît également la nécessité de mettre en balance la protection des données à caractère personnel et plusieurs autres droits fondamentaux et objectifs, tels que la sécurité et la justice ([83]).

2.3.2. *Contrôle de l'application des règles, y compris les sanctions, et voies de recours*

(60) Les pouvoirs et tâches de la commission de l'information continuent de correspondre à ceux qui incombent aux autorités contrôlant la protection des données dans les États membres en vertu des articles pertinents de la directive (UE) 2016/680 ([84]), comme indiqué aux considérants 100 à 109 de la décision d'exécution (UE) 2021/1773.

(61) La loi sur les données (utilisation et accès) a apporté certaines précisions concernant l'exercice de certains de ces pouvoirs.

(62) L'article 97 de la loi sur les données (utilisation et accès) modifie l'article 142 de la loi DPA 2018 afin de permettre expressément à la commission de l'information d'exiger non seulement des informations, mais aussi des documents spécifiques, améliorant ainsi sa capacité à enquêter et à vérifier le respect des règles.

(63) L'article 98 de la loi sur les données (utilisation et accès) renforce les pouvoirs de la commission de l'information confiés en vertu de l'article 146 de la loi DPA 2018 en autorisant la commission de l'information à exiger d'un responsable du traitement ou d'un sous-traitant qu'il fasse établir un rapport indépendant sur une question donnée. Le rapport doit être préparé par une «personne agréée», la commission de l'information étant habilitée en dernier chef à approuver la personne proposée ou à désigner une personne si aucune personne appropriée n'est proposée ou si le responsable du traitement n'agit pas ([85]). L'avis d'évaluation peut préciser le format du rapport, son contenu et l'échéance pour laquelle il doit être produit ([86]). Tous les coûts y afférents, y compris les honoraires de la personne agréée, doivent être pris en charge par le responsable du traitement ou le sous-traitant ([87]).

(64) L'article 100 de la loi sur les données (utilisation et accès) établit les avis d'entretien en tant que nouvel outil d'exécution en vertu de l'article 148A de la loi DPA 2018. La commission de l'information peut contraindre une personne à se soumettre à des entretiens, en lui assurant des garanties telles que la protection contre l'auto-incrimination et le secret professionnel ([88]).

(65) L'article 101 de la loi sur les données (utilisation et accès) modifie l'annexe 16 de la loi DPA 2018 afin de donner à la commission de l'information une plus grande souplesse dans l'émission des avis de sanction. Si le délai actuel de six mois pour émettre un avis de sanction définitif à la suite d'un avis d'intention reste la règle générale, cet article permet à la commission de l'information d'émettre un avis de sanction hors délai lorsqu'il n'est pas raisonnablement possible de respecter le délai. Dans ce cas, l'avis doit être émis dès que cela est raisonnablement possible. En outre, lorsque la commission de l'information décide de ne pas émettre un avis de sanction, elle doit en informer la personne concernée par écrit dans un délai de six mois ou dès que cela est raisonnablement possible passé ce délai. Cet article introduit également une nouvelle obligation pour la commission de l'information de publier des orientations sur les circonstances dans lesquelles un délai supérieur à six mois peut être nécessaire pour émettre un avis de sanction.

([80]) Annexe 13 de la loi DPA 2018.
([81]) Article 91 de la loi sur les données (utilisation et accès), insérant un article 120A à la loi DPA 2018.
([82]) Article 91 de la loi sur les données (utilisation et accès), ajoutant un article 120B à la loi DPA 2018.
([83]) Voir, en particulier, considérant 2 de la directive (UE) 2016/680.
([84]) Annexe 13, point 2, de la loi DPA 2018.
([85]) Article 98 de la loi sur les données (utilisation et accès), insérant un article 146A à la loi DPA 2018.
([86]) Article 98 de la loi sur les données (utilisation et accès), insérant un article 3A à l'article 146 de la loi DPA 2018.
([87]) Article 98 de la loi sur les données (utilisation et accès), insérant un article 11A à l'article 146 de la loi DPA 2018.
([88]) Article 98 de la loi sur les données (utilisation et accès), insérant un article 8B à l'article 146 de la loi DPA 2018.

(66) L'article 102 de la loi sur les données (utilisation et accès) crée de nouvelles obligations en matière de rapports pour la commission de l'information. Elle modifie l'article 139 de la loi DPA 2018 et insère dans cette dernière un nouvel article (l'article 161A), qui impose à la commission de l'information de publier un rapport annuel sur son activité réglementaire. Ce rapport doit détailler la manière dont la commission de l'information a exercé les pouvoirs d'enquête et d'exécution qui lui sont conférés par le RGPD britannique et les parties 3 et 4 de la loi DPA 2018. Il doit également divulguer le nombre d'avis de sanction émis au-delà du délai de six mois à compter d'un avis d'intention et justifier les retards. En outre, le rapport doit expliquer comment la commission de l'information a suivi ses propres orientations lors de ses décisions réglementaires.

(67) L'article 103 de la loi sur les données (utilisation et accès) renforce la procédure de réclamation ouverte aux personnes concernées. Il insère de nouveaux articles (les articles 164A et 164B) dans la loi DPA 2018. L'article 164A prévoit que les personnes concernées ont le droit d'introduire des réclamations directement auprès des responsables du traitement si elles estiment que les droits que leur confèrent le RGPD britannique ou la partie 3 de la loi DPA 2018 ont été violés. Les responsables du traitement doivent faciliter ce processus, accuser réception des réclamations dans un délai de 30 jours et y répondre dans les meilleurs délais. Ils doivent également tenir l'auteur de la réclamation informé de l'état d'avancement de son dossier et de son issue. L'article 164B investit le secrétaire d'État du pouvoir d'adopter des règlements obligeant les responsables du traitement à communiquer le nombre de réclamations reçues.

(68) L'article 104 de la loi sur les données (utilisation et accès) insère dans la loi DPA 2018 un nouvel article (l'article 180A) afin de clarifier les pouvoirs des juridictions dans les procédures de demande d'accès des personnes concernées. En vertu de cette disposition, les juridictions peuvent exiger des responsables du traitement qu'ils fournissent aux fins du contrôle juridictionnel les informations litigieuses afin de déterminer si la personne concernée peut y avoir accès. Toutefois, les informations ne peuvent être divulguées à la personne concernée que si la juridiction détermine qu'elle a un droit d'accès à ces informations. Cet article précise que les juridictions ont la possibilité d'examiner les éléments contestés sans les divulguer prématurément à l'auteur de la réclamation, rétablissant ainsi une garantie qui existait auparavant en vertu de la loi de 1998 sur la protection des données.

(69) En ce qui concerne la mise en œuvre de ces pouvoirs, depuis l'adoption de la décision d'exécution (UE) 2021/1773, le commissaire à l'information a traité de nombreuses réclamations ([89]), mené plusieurs enquêtes et pris des mesures d'exécution ayant trait au traitement des données par les autorités répressives. Entre 2021 et 2025, il a diligenté des enquêtes et émis des rappels à l'ordre à l'encontre de divers organes de police pour différents manquements à leurs obligations en matière de protection des données, constatés par exemple lors de la réponse à des demandes d'accès aux données, lors de la mise en place de mesures de sécurité pour les données de vidéosurveillance, lors du traitement de dossiers judiciaires sensibles, lors de la fusion des données de différentes personnes ou lors de la divulgation de données à caractère personnel à des tiers ([90]). Le commissaire à l'information a également publié et actualisé des lignes directrices, des avis et des documents d'orientation, par exemple sur le droit d'accès ou sur la manière de traiter les demandes manifestement infondées ou excessives au titre de la partie 3 de la loi DPA 2018 ([91]), ou a mis à jour des lignes directrices existantes, telles que son guide sur le traitement par les services répressifs ([92]).

3. **CONCLUSION**

(70) La Commission estime que la partie 3 de la loi DPA 2018 continue de garantir un niveau de protection des données à caractère personnel transférées, à des fins répressives, des autorités compétentes de l'Union européenne vers les autorités compétentes du Royaume-Uni qui est essentiellement équivalent à celui garanti par la directive (UE) 2016/680.

([89]) Par exemple, en 2023 et 2024, la commission de l'information a reçu 1 890 réclamations sur la base du RGPD et/ou de la loi DPA 2018 concernant des organisations des sous-secteurs «Autorité de police», «Forces de police» et «Commissaires de police». Voir, également, rapport annuel et états financiers du commissaire à l'information pour la période 2023-2024, disponibles à l'adresse suivante: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([90]) De plus amples informations sont disponibles à l'adresse suivante: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([91]) Disponibles aux adresses suivantes: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ et https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([92]) Disponible à l'adresse suivante: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/.

(71) De plus, la Commission estime que, pris dans leur ensemble, les mécanismes de surveillance et les voies de recours prévus dans le droit du Royaume-Uni continuent de permettre de détecter et de sanctionner en pratique les infractions et d'offrir aux personnes concernées des voies de droit leur permettant d'avoir accès aux données à caractère personnel les concernant et, in fine, d'obtenir leur rectification ou leur effacement.

(72) En conséquence, il convient de décider que le Royaume-Uni continue d'assurer un niveau de protection adéquat au sens de l'article 36, paragraphe 2, de la directive (UE) 2016/680, interprété à la lumière de la charte des droits fondamentaux.

4. EFFETS DE LA PRÉSENTE DÉCISION ET ACTION DES AUTORITÉS DE PROTECTION DES DONNÉES

(73) Les États membres et leurs organes sont tenus de prendre les mesures nécessaires pour se conformer aux actes des institutions de l'Union, car ces derniers jouissent d'une présomption de légalité et produisent, dès lors, des effets juridiques aussi longtemps qu'ils n'ont pas expiré, été retirés, été annulés à la suite d'un recours en annulation ou été déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité.

(74) En conséquence, une décision d'adéquation de la Commission adoptée en vertu de l'article 36, paragraphe 3, de la directive (UE) 2016/680, a un caractère contraignant pour tous les organes des États membres destinataires, y compris leurs autorités de contrôle indépendantes. En particulier, au cours de la période d'application de la décision d'exécution (UE) 2021/1773, modifiée par la présente décision, les transferts d'un responsable du traitement ou d'un sous-traitant situé dans l'Union européenne à des responsables du traitement ou des sous-traitants situés au Royaume-Uni peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autorisation supplémentaire.

(75) Parallèlement, il convient de rappeler que, en vertu de l'article 47, paragraphe 5, de la directive (UE) 2016/680, et ainsi que la Cour de justice l'a expliqué dans l'arrêt Schrems I, lorsqu'une autorité chargée de la protection des données met en cause, notamment après avoir été saisie d'une réclamation, la compatibilité d'une décision d'adéquation de la Commission avec la protection des droits fondamentaux que constituent le respect de la vie privée et la protection des données, le droit national doit prévoir des voies de recours lui permettant de faire valoir ces griefs devant les juridictions nationales, qui pourraient être amenées à procéder à un renvoi préjudiciel devant la Cour de justice ([93]).

5. SUIVI

(76) Conformément à l'article 36, paragraphe 4, de la directive (UE) 2016/680, la Commission doit suivre, de manière permanente, les évolutions pertinentes au Royaume-Uni afin de déterminer si ce pays continue d'assurer un niveau de protection essentiellement équivalent. Ce suivi est d'autant plus important que le Royaume-Uni appliquera et mettra en œuvre un régime modifié de protection des données. En outre, le cadre de protection des données modifié du Royaume-Uni confère au secrétaire d'État le pouvoir de préciser davantage le cadre au moyen du droit dérivé. À cet égard, il convient d'accorder une attention particulière à de telles spécifications supplémentaires, ainsi qu'à l'application concrète des règles modifiées du Royaume-Uni concernant les transferts des données à caractère personnel aux pays tiers, à l'exercice effectif des droits individuels, y compris toute évolution pertinente de la législation et de la pratique concernant les exceptions ou restrictions à ces droits nouvellement introduites, au fonctionnement de l'ICO restructuré, y compris en ce qui concerne le traitement des plaintes et l'application des mesures correctives. Parmi d'autres éléments, la Commission devrait fonder son suivi sur les évolutions de la jurisprudence et sur la surveillance exercée par l'ICO et par d'autres organismes indépendants.

(77) Afin de faciliter ce suivi, les autorités du Royaume-Uni sont invitées à informer sans délai et régulièrement la Commission de toute modification de fond apportée à l'ordre juridique britannique ayant une incidence sur le cadre juridique qui fait l'objet de la décision d'exécution (UE) 2021/1773, telle que modifiée par la présente décision, ainsi que de toute évolution des pratiques relatives au traitement des données à caractère personnel évaluées dans la décision d'exécution (UE) 2021/1773, telle que modifiée par la présente décision, en particulier pour ce qui est des éléments mentionnés au considérant 39.

(78) En outre, afin de permettre à la Commission d'accomplir efficacement sa mission de suivi, les États membres devraient l'informer de toute mesure pertinente prise par les autorités nationales chargées de la protection des données, en particulier en ce qui concerne les questions ou les plaintes des personnes concernées de l'Union européenne au sujet du transfert de données à caractère personnel des autorités compétentes de l'Union vers les autorités compétentes du Royaume-Uni. La Commission devrait également être informée de tout élément indiquant que les actions des autorités publiques du Royaume-Uni compétentes pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière, y compris de tout organisme de surveillance, n'assurent pas le niveau de protection requis.

([93]) Arrêt Schrems I, point 65.

(79) Lorsque des informations disponibles, en particulier les informations résultant du suivi de la présente décision ou fournies par les autorités du Royaume-Uni ou des États membres, révèlent que le niveau de protection assuré par le Royaume-Uni pourrait ne plus être adéquat, la Commission devrait en informer sans délai les autorités compétentes du Royaume-Uni et demander que des mesures appropriées soient prises dans un délai bien défini, qui ne peut excéder trois mois. Ce délai peut au besoin être prorogé pour une durée déterminée, compte tenu de la nature de la question en cause et/ou des mesures à prendre.

(80) Si, à l'expiration de ce délai défini, les autorités compétentes du Royaume-Uni échouent à prendre ces mesures ou à démontrer autrement de manière satisfaisante que la présente décision reste fondée sur un niveau de protection adéquat, la Commission lancera la procédure visée à l'article 58, paragraphe 2, de la directive (UE) 2016/680, en vue de suspendre partiellement ou complètement ou d'abroger la présente décision.

(81) À défaut, la Commission lancera cette procédure en vue de modifier la décision d'exécution (UE) 2021/1773, telle que modifiée par la présente décision, notamment en soumettant les transferts de données à des conditions supplémentaires ou en limitant le constat d'adéquation aux seuls transferts de données pour lesquels un niveau de protection adéquat continue d'être assuré.

(82) Pour des raisons d'urgence impérieuses dûment justifiées, la Commission recourra à la possibilité d'adopter des actes d'exécution suspendant, abrogeant ou amendant la présente décision, qui seraient immédiatement applicables, conformément à la procédure visée à l'article 58, paragraphe 3, de la directive (UE) 2016/680.

6. RÉEXAMEN, DURÉE ET RENOUVELLEMENT DE LA PRÉSENTE DÉCISION

(83) En application de l'article 36, paragraphe 3, de la directive (UE) 2016/680, et au regard du fait que le niveau de protection assuré par le cadre juridique du Royaume-Uni est susceptible d'évoluer, la Commission, après l'adoption de la présente décision, devrait vérifier de manière périodique si les conclusions relatives au niveau adéquat de la protection assurée par le Royaume-Uni sont toujours justifiées en fait et en droit. Ces évaluations devraient avoir lieu au moins une fois tous les quatre ans et couvrir tous les aspects relatifs au fonctionnement de la présente décision, y compris le fonctionnement des mécanismes de surveillance et d'application pertinents.

(84) Aux fins de cet examen, la Commission devrait rencontrer les représentants permanents des autorités du Royaume-Uni, y compris la commission de l'information. La participation à cette réunion devrait être ouverte aux représentants des membres du comité européen de la protection des données. Dans le cadre de l'examen, la Commission devrait demander au Royaume-Uni de fournir des informations exhaustives sur tous les aspects pertinents pour le constat d'adéquation. La Commission devrait également demander des explications sur toute information reçue présentant de l'intérêt pour la présente décision, notamment de la part de l'EDPB, de diverses autorités de protection des données ou de groupes de la société civile, des informations publiques ou relayés par les médias, ou toute autre source d'informations disponible.

(85) Sur la base de l'examen, la Commission devrait élaborer un rapport public qui sera présenté au Parlement européen et au Conseil.

(86) La Commission doit également tenir compte du fait que le cadre de protection des données évalué dans la présente décision et dans la décision d'exécution (UE) 2021/1773 peut encore évoluer.

(87) Il convient donc de disposer que la présente décision est applicable pour une durée de six ans à compter de son entrée en vigueur.

(88) Plus particulièrement, si les informations issues du suivi de la présente décision révèlent que les constatations relatives à l'adéquation du niveau de protection assuré au Royaume-Uni sont toujours justifiées sur les plans factuel et juridique, la Commission devrait, au moins six mois avant l'expiration de la présente décision, lancer la procédure de modification de la présente décision en prorogeant sa portée dans le temps, en principe, d'une durée supplémentaire de quatre ans. Un tel acte d'exécution modifiant ainsi la présente décision doit être adopté conformément à la procédure visée à l'article 58, paragraphe 2, de la directive (UE) 2016/680.

7. CONSIDÉRATIONS FINALES

(89) Le comité européen de la protection des données a publié un avis ([94]), dont il a été tenu compte dans l'élaboration de la présente décision.

(90) La mesure prévue dans la présente décision est conforme à l'avis du comité institué par l'article 58 de la directive (UE) 2016/680.

(91) Conformément à l'article 6 *bis* du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande n'est pas liée par les règles fixées dans la directive (UE) 2016/680, et donc dans la présente décision d'exécution, concernant le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne, lorsque l'Irlande n'est pas liée par les règles qui régissent des formes de coopération judiciaire en matière pénale ou de coopération policière dans le cadre desquelles les dispositions fixées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne doivent être respectées. Néanmoins, en vertu de la décision d'exécution (UE) 2020/1745 du Conseil ([95]), la directive (UE) 2016/680 sera mise en œuvre et appliquée provisoirement en Irlande à partir du 1er janvier 2021. L'Irlande est donc liée par la présente décision, dans les mêmes conditions que celles relatives à l'application de la directive (UE) 2016/680 en Irlande, énoncées dans la décision d'exécution (UE) 2020/1745, en ce qui concerne la partie de l'acquis de Schengen à laquelle elle participe.

(92) Conformément aux articles 2 et 2 *bis* du protocole n° 22 sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'est pas lié par les règles fixées dans la directive (UE) 2016/680, et donc dans la présente décision d'exécution, ni soumis à leur application, lorsqu'elles concernent le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne. Toutefois, étant donné que la directive (UE) 2016/680 développe l'acquis de Schengen, le Danemark, conformément à l'article 4 de ce protocole, a notifié le 26 octobre 2016 sa décision de mettre la directive (UE) 2016/680 en œuvre. Le Danemark est donc tenu, en application du droit international, de mettre en œuvre la présente décision.

(93) En ce qui concerne l'Islande et la Norvège, la présente décision constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([96]).

(94) En ce qui concerne la Suisse, la présente décision constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([97]).

(95) En ce qui concerne le Liechtenstein, la présente décision constitue un développement des dispositions de l'acquis de Schengen au sens du protocole signé entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ([98]).

(96) Il y a donc lieu de modifier la décision d'exécution (UE) 2021/1773 en conséquence,

([94]) Avis 27/2025 concernant le projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni, disponible à l'adresse suivante: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_en.

([95]) Décision d'exécution (UE) 2020/1745 du Conseil du 18 novembre 2020 relative à la mise en œuvre des dispositions de l'acquis de Schengen dans le domaine de la protection des données et à la mise en œuvre à titre provisoire de certaines dispositions de l'acquis de Schengen en Irlande (JO L 393 du 23.11.2020, p. 3, ELI: http://data.europa.eu/eli/dec_impl/2020/1745/oj).

([96]) Accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen [JO L 176 du 10.7.1999, p. 36, ELI: http://data.europa.eu/eli/agree_internation/1999/439(1)/oj].

([97]) JO L 53 du 27.2.2008, p. 52.

([98]) JO L 160 du 18.6.2011, p. 21.

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

L'article 4 de la décision d'exécution (UE) 2021/1773 est remplacé par le texte suivant:

«*Article 4*

La présente décision expire le 27 décembre 2031, à moins qu'elle ne soit prolongée conformément à la procédure prévue à l'article 58, paragraphe 2, de la directive (UE) 2016/680.».

Article 2

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 19 décembre 2025.

Par la Commission
Michael MCGRATH
Membre de la Commission