

**Avis 27/2025 concernant le projet de décision d'exécution
de la Commission européenne, rendu conformément à la
directive (UE) 2016/680, constatant le niveau de protection
adéquat des données à caractère personnel assuré par le
Royaume-Uni**

Adopté le 16 octobre 2025

Résumé

Le 22 juillet 2025, la Commission européenne a approuvé son projet de décision d'exécution constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni conformément à la directive en matière de protection des données dans le domaine répressif. Le même jour, dans le cadre de la procédure d'adoption formelle du projet de décision, la Commission européenne a demandé l'avis du comité européen de la protection des données.

Le projet de décision modifie et complète la précédente décision d'adéquation vis-à-vis du Royaume-Uni au titre de la directive en matière de protection des données dans le domaine répressif, qui date de juin 2021. L'évaluation par le comité européen de la protection des données du caractère adéquat du niveau de protection offert au Royaume-Uni s'est fondée sur l'examen du projet de décision et est donc axée sur les nouvelles évolutions de la législation britannique en matière de protection des données et sur les éléments mis en évidence dans la décision d'adéquation précédente.

Le comité européen de la protection des données a utilisé ses critères de référence pour l'adéquation adoptés le 2 février 2021 dans le cadre de la directive en matière de protection des données dans le domaine répressif comme référence principale pour ces travaux, ainsi que les recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance et la jurisprudence pertinente. Le comité se félicite de la poursuite de l'harmonisation entre le cadre de protection des données du Royaume-Uni et celui de l'UE, malgré les évolutions récentes du cadre juridique pertinent du Royaume-Uni. Dans ce contexte, il importe de souligner que le comité européen de la protection des données ne s'attend pas à ce que le cadre juridique du Royaume-Uni reproduise la législation européenne en matière de protection des données, l'objectif du présent avis étant de recenser les aspects spécifiques des modifications et évolutions juridiques intervenues depuis l'adoption de la première décision d'adéquation, qui sont susceptibles d'avoir une incidence sur le niveau de protection, et de soulever des points nécessitant des éclaircissements supplémentaires, une attention et un suivi ou suscitant des préoccupations.

À cet égard, le comité européen de la protection des données souligne les constatations suivantes:

le comité européen de la protection des données observe des modifications des règles régissant le transfert ultérieur de données à caractère personnel vers des pays tiers, notamment la nouvelle liste indicative d'éléments à prendre en considération dans l'analyse du caractère adéquat du niveau de protection, qui n'inclut pas des éléments importants qui figuraient dans la précédente analyse du Royaume-Uni. Le comité européen de la protection des données estime que cet aspect ainsi que le nouveau critère relatif à l'«opportunité de faciliter les transferts de données à caractère personnel à destination et en provenance du Royaume-Uni» doivent être abordés plus en détail et encourage la Commission européenne à approfondir spécifiquement son évaluation et à suivre l'évolution et la mise en œuvre pratique de la nouvelle analyse du caractère adéquat du niveau de protection.

Le comité européen de la protection des données prend note de changements importants concernant la manière dont la prise de décision automatisée est réglementée au Royaume-Uni, notamment l'introduction d'une approche plus permissive et l'attribution de nouveaux pouvoirs au secrétaire d'État. L'étendue et le pouvoir discrétionnaire de ces pouvoirs pourraient susciter

des inquiétudes notables, par exemple en raison de leur ampleur, en particulier dans le contexte de l'évolution rapide de l'environnement réglementaire et des progrès des technologies automatisées. Le comité européen de la protection des données invite la Commission européenne à analyser ces pouvoirs et à suivre toute évolution à cet égard. Le comité européen de la protection des données rappelle également l'importance d'un examen humain significatif en vue de veiller au respect des garanties dans la prise de décision automatisée et invite donc instamment la Commission européenne à détailler les exemptions possibles au droit de la personne concernée d'obtenir une intervention humaine dans sa décision finale d'adéquation et à surveiller la mise en œuvre de ces changements dans la pratique.

Le comité estime qu'il est essentiel d'évaluer les exemptions étendues en matière de sécurité nationale dans le cadre répressif et reste particulièrement vigilant à l'égard de toute exemption au principe de proportionnalité, ainsi qu'à l'égard de l'obligation de traiter les données à caractère personnel à des fins légitimes. De même, toute exemption aux pouvoirs de l'autorité de contrôle doit être abordée avec prudence. Toute limitation de l'exercice des droits et libertés reconnus par la charte des droits fondamentaux de l'UE doit respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, ne peut être apportée que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. Le comité européen de la protection des données invite la Commission européenne à compléter son évaluation dans la décision finale d'adéquation et à surveiller spécifiquement l'application pratique des exemptions en matière de sécurité nationale pour les autorités répressives.

Le comité observe que les activités de traitement effectuées par les autorités répressives compétentes peuvent, dans des circonstances particulières, relever des règles normalement applicables au traitement des données à caractère personnel par les autorités nationales de sécurité. Dans ce contexte, il convient de veiller tout particulièrement à ce que le régime de protection des données pour leur traitement à des fins de sécurité nationale ne soit pas étendu à des contextes qui ne sont pas liés à la sécurité nationale. Le comité européen de la protection des données invite la Commission européenne à vérifier dans la pratique si les autorités compétentes qualifiées sont en mesure de maintenir une distinction claire entre les différentes finalités de traitement afin de respecter le cadre juridique correspondant en conséquence.

Bien que le comité européen de la protection des données reconnaisse que le système de surveillance des services répressifs en matière pénale ainsi que les mécanismes de recours restent dans une large mesure inchangés, il réaffirme la nécessité pour la Commission européenne de suivre de près l'application des mesures correctrices et des voies de recours pour les personnes concernées dans le cadre de la protection des données du Royaume-Uni.

Outre la réintroduction d'une clause de suppression automatique et de l'obligation légale de surveillance, le comité européen de la protection des données souligne qu'il importe que la Commission européenne procède au réexamen obligatoire dans le délai légal précisé dans la directive en matière de protection des données dans le domaine répressif, en tenant compte des éléments déjà exposés dans la décision d'exécution (UE) 2021/1773 de la Commission ainsi que de toute autre évolution pertinente.

Table des matières

1	INTRODUCTION	5
1.1	Commentaires généraux	5
1.2	Portée du présent avis du comité européen de la protection des données	7
1.3	Évolutions pertinentes du cadre juridique britannique	7
2	ÉVOLUTIONS PERTINENTES CONCERNANT LES RÈGLES APPLICABLES AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL	8
2.1	Garanties, droits et obligations	8
2.1.1	Utilisation du consentement dans le contexte répressif	8
2.1.2	Transferts ultérieurs	8
2.1.3	Prise de décision automatisée	10
2.1.4	Exigences en matière de journalisation	12
2.1.5	Exemptions concernant la sécurité nationale pour les autorités répressives	12
2.1.6	Responsabilité conjointe du traitement entre les services de renseignement et les autorités répressives du Royaume-Uni	15
2.1.7	Droit d'accès	15
2.1.8	Surveillance et voies de recours	16
3	Réexamen, durée et renouvellement de la décision	18

Le comité européen de la protection des données

vu l'article 51, paragraphe 1, point g), de 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 [ci-après la «directive en matière de protection des données dans le domaine répressif»],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ L'AVIS SUIVANT:

INTRODUCTION

Commentaires généraux

1. Le 22 juillet 2025, la Commission européenne a approuvé son projet de décision d'exécution concernant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni conformément à la directive en matière de protection des données dans le domaine répressif (ci-après le «projet de décision»). Le même jour, dans le cadre de la procédure d'adoption formelle du projet de décision, la Commission européenne a demandé l'avis du comité européen de la protection des données. Le comité européen de la protection des données observe que le projet de décision prolonge la validité de la décision d'adéquation existante du Royaume-Uni¹ pour une période de six ans, jusqu'au 27 décembre 2031. Le comité européen de la protection des données rappelle que la décision initiale d'adéquation devait expirer le 27 juin 2025 et que, par conséquent, elle avait déjà fait l'objet d'une prolongation technique et limitée dans le temps² afin de permettre au Royaume-Uni d'achever ses réformes en matière de protection des données³. L'analyse que la Commission a appliquée à cette évaluation vise à «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 précédente décision d'adéquation du Royaume-Uni»⁴. En conséquence, la Commission a concentré son évaluation sur la nouvelle législation en matière

¹ 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 caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni [notifiée sous le numéro C(2021) 4801].

² 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 caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni [notifiée sous le numéro C(2025) 3898].

³ Avis 6/2025 concernant la prorogation des décisions d'exécution de la Commission européenne constatant le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni, adoptées au titre du règlement général sur la protection des données et de la directive en matière de protection des données dans le domaine répressif (Opinion 06/2025 regarding the extension of the European Commission Implementing Decisions under the GDPR and the LED on the adequate protection of personal data in the United Kingdom), adopté le 5 mai 2025, disponible, en anglais uniquement, à l'adresse suivante:

https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202506-uk-adequacyextension-gdpr-led_en.pdf.

⁴ Considérant 4 du projet de décision.

de protection des données, la loi sur les données (utilisation et accès) (ci-après la «DUAA»), qui est entrée en vigueur le 20 août 2025. La Commission a spécifiquement examiné les éléments énumérés au considérant 165 de la précédente décision d'adéquation du Royaume-Uni, qui figurent tous dans le projet de décision, à savoir:

«les règles 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 présente décision; 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 l'ICO et par d'autres organismes indépendants alimenteront le suivi assuré par la Commission.»⁵

2. La Commission conclut que, sur la base de cette évaluation, le Royaume-Uni continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne vers le Royaume-Uni dans le cadre du champ d'application de la directive (UE) 2016/680.
3. Le comité européen de la protection des données convient que l'évaluation devrait être principalement axée sur les nouvelles évolutions de la législation britannique en matière de protection des données et sur les éléments mis en évidence dans la précédente décision d'adéquation. Le comité européen de la protection des données croit comprendre que la Commission a évalué tous les éléments énumérés à l'article 36, paragraphe 2, de la directive en matière de protection des données dans le domaine répressif et toutes les évolutions pertinentes du cadre juridique global du Royaume-Uni au-delà de la DUAA lorsqu'elle a conclu que le cadre juridique global du Royaume-Uni continue d'assurer un niveau adéquat de protection des données à caractère personnel transférées de l'Union européenne vers le Royaume-Uni dans le cadre de la directive en matière de protection des données dans le domaine répressif. Néanmoins, le comité européen de la protection des données souhaiterait une clarification explicite à cet égard dans la décision d'adéquation finale. Le comité européen de la protection des données souhaiterait également que la Commission précise qu'elle continuera d'évaluer ces éléments de manière permanente dans le cadre de son rôle de suivi.
4. Étant donné que certaines modifications législatives, exigences juridiques et garanties s'appliquent de la même manière au titre du régime d'accès des pouvoirs publics et du cadre de la directive en matière de protection des données dans le domaine répressif, les évaluations correspondantes du comité européen de la protection des données seront intégrées à la fois dans le présent avis et dans l'avis 26/2025 afin de garantir la cohérence et l'exhaustivité.
5. Le comité européen de la protection des données observe également que, conformément aux articles 47 et 94 du règlement (UE) 2018/1725⁶, les institutions, organes et organismes de l'Union européenne peuvent transférer des données à caractère personnel vers un pays tiers, un territoire, un secteur ou une organisation internationale reconnus par la Commission en vertu de l'article 36, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif comme assurant un niveau de protection adéquat, à condition que le transfert serve uniquement à l'exécution de missions relevant de la compétence du responsable du traitement,

⁵ Considérant 6 du projet de décision.

⁶ 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 (RPDUE), JO L 295 du 21.11.2018, p. 39.

sans qu'une autorisation supplémentaire soit nécessaire. Compte tenu de la coopération existante entre les services répressifs de l'Union, tels qu'Europol et Eurojust, et leurs homologues britanniques, le comité européen de la protection des données invite la Commission à rappeler cette possibilité juridique dans les considérants du projet de décision.

Portée du présent avis du comité européen de la protection des données

6. Conformément à l'article 51, paragraphe 1, point g), de la directive en matière de protection des données dans le domaine répressif, le comité européen de la protection des données est tenu de rendre à la Commission un avis indépendant en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers. En raison de la situation particulière du Royaume-Uni, le projet de décision complète la décision d'adéquation de 2021 qui reste valable pour les parties qui ne sont pas spécifiquement abordées dans le projet de décision. De même, dans le présent avis, le comité européen de la protection des données s'appuie sur son avis précédent et le développe⁷. Par conséquent, l'analyse et les observations du comité européen de la protection des données qui y figurent continuent généralement de s'appliquer.
7. Compte tenu de ce qui précède, et en raison du délai limité accordé au comité européen de la protection des données pour adopter le présent avis, le comité européen de la protection des données a concentré ses observations et son analyse sur certains points présentés dans le projet de décision, en particulier lorsque des éclaircissements supplémentaires, d'autres informations ou un suivi futur par la Commission sont nécessaires.

Évolutions pertinentes du cadre juridique britannique

8. Comme expliqué dans le projet de décision⁸, après la fin de la période de mise en œuvre convenue dans l'accord sur le retrait du Royaume-Uni de l'Union européenne⁹ le 31 décembre 2020, le Royaume-Uni avait l'intention d'adopter un nouveau régime de protection des données qui différerait du cadre juridique de l'UE. Depuis lors, le Royaume-Uni a apporté des modifications à son cadre existant en matière de protection des données, principalement par l'intermédiaire de la DUAA, qui apportent des modifications limitées à différents aspects du cadre.
9. Le présent avis porte sur les modifications législatives pertinentes introduites par la DUAA et sur la manière dont ces modifications ont une incidence sur la protection des données du cadre du Royaume-Uni. Bien que la plupart des modifications apportées au cadre de protection des données du Royaume-Uni visent à clarifier et à faciliter le respect de la législation, le comité européen de la protection des données estime que certaines des nouvelles modifications juridiques dont on ne peut encore apprécier les effets, qui peuvent avoir une incidence sur le niveau de protection, en fonction de leur mise en œuvre, devraient être davantage clarifiées et faire l'objet d'un suivi attentif de la part de la Commission. D'après les explications

⁷ Avis 15/2021 concernant le projet de décision d'exécution de la Commission européenne, rendu conformément à la directive (UE) 2016/680, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni, adopté le 13 avril 2021.

⁸ Voir considérant 2 du projet de décision.

⁹ La période de mise en œuvre est une période convenue dans l'accord sur le retrait du Royaume-Uni de l'Union européenne, pendant laquelle le Royaume-Uni ne sera plus membre de l'UE, mais continuera à être soumis aux règles de l'Union et restera membre du marché unique et de l'union douanière. Voir la loi de 2020 sur l'Union européenne (relative à l'accord de retrait).

supplémentaires fournies par la Commission, le comité européen de la protection des données comprend que la Commission a l'intention d'examiner l'évolution de certaines de ces modifications et invite la Commission à mettre en évidence, dans la décision finale, les domaines qu'elle a l'intention de surveiller attentivement.

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

Garanties, droits et obligations

Utilisation du consentement dans le contexte répressif

10. Le comité européen de la protection des données prend note des explications fournies par la Commission en ce qui concerne les modifications techniques apportées à la définition¹⁰, aux conditions d'obtention du consentement¹¹ et à l'alignement global de la notion de consentement dans les deuxième et troisième parties de la loi de 2018 sur la protection des données (ci-après la «loi DPA 2018»), étant donné que les considérants 35 et 36 de la décision d'exécution 2021/1773 restent valables, c'est-à-dire que le consentement ne constitue pas en soi une base juridique pour le traitement, y compris le transfert, de données à caractère personnel dans le contexte de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.
11. Le comité européen de la protection des données se félicite que la Commission, à l'instar de l'évaluation de 2021, ait examiné l'utilisation du consentement dans un contexte répressif. Le comité européen de la protection des données rappelle que «le consentement de la personne concernée ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes»¹². Par conséquent, le comité européen de la protection des données réaffirme la nécessité de procéder à une telle analyse lors de l'évaluation du niveau de protection au titre de l'article 36 de la directive en matière de protection des données dans le domaine répressif¹³.

Transferts ultérieurs

12. Lorsqu'une autorité compétente envisage de partager des données à caractère personnel traitées au titre de la partie 3 de la DPA 2018 avec les autorités répressives d'un pays tiers, des exigences spécifiques s'appliquent. En particulier, ces transferts peuvent avoir lieu lorsqu'ils sont approuvés par des règlements d'adéquation adoptés par le secrétaire d'État ou, en

¹⁰ Voir la section 69, paragraphe 2, point 1A, de la loi de 2025 sur les données (utilisation et accès), qui introduira la définition suivante du consentement: «toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement» qui est formulée comme l'article 4, paragraphe 11, du RGPD britannique de 2018.

¹¹ Voir la section 69, paragraphe 4, de la loi de 2025 sur les données (utilisation et accès) qui définira les conditions du consentement.

¹² Comme le comité européen de la protection des données l'a indiqué au considérant 35 de ses recommandations 01/2021 sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, adoptées le 2 février 2021.

¹³ Voir le considérant 37 de l'avis 15/2021 du comité européen de la protection des données.

l'absence de tels règlements, sur la base des garanties appropriées. Si un transfert ne peut être fondé ni sur un règlement ni sur des garanties appropriées, il ne peut avoir lieu que dans certaines circonstances déterminées, appelées «circonstances spéciales» et correspondant aux situations et conditions pouvant être qualifiées de «dérogations» au titre de l'article 38 de la directive en matière de protection des données dans le domaine répressif.

13. Bien que la Commission observe que «le régime applicable aux transferts internationaux de données à caractère personnel en provenance du Royaume-Uni reste très proche des règles énoncées au chapitre V de la directive (UE) 2016/680», le projet de décision indique également que la norme juridique applicable aux règlements relatifs à l'approbation des transferts, qualifiés de règlements d'adéquation dans l'ancienne section 74A de la loi DPA 2018, ainsi que les garanties appropriées, ont été reformulées. Au lieu de faire référence à un niveau de protection adéquat, le nouveau «critère de la protection des données» énoncé à la section 74AB de la loi DPA 2018 exige que le niveau de protection des personnes concernées assuré dans les pays tiers destinataires ou 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.
14. Dans ce contexte, le comité européen de la protection des données observe que les éléments que le secrétaire d'État doit prendre en considération dans l'évaluation de l'adéquation conformément à la section 74AB, paragraphe 2, de la loi DPA 2018 semblent avoir été réduits par rapport à l'évaluation précédente des règlements d'adéquation¹⁴. Le comité européen de la protection des données souligne la suppression de certains facteurs qui, selon lui, jouent un rôle important afin de déterminer si un pays tiers offre un niveau de protection des données à caractère personnel essentiellement équivalent. Il s'agit, en particulier, i) des règles du pays tiers en ce qui concerne «la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel», ii) de la jurisprudence, iii) de l'évaluation globale du cadre juridique pertinent, y compris en ce qui concerne l'accès des pouvoirs publics aux données, iv) de l'existence de droits effectifs et opposables des personnes concernées, v) et de la référence à une ou plusieurs autorités de contrôle indépendantes dont le fonctionnement est effectif (au lieu de cela, le nouveau critère fait référence à une «autorité chargée de faire respecter la protection des personnes concernées à l'égard du traitement des données à caractère personnel»).
15. S'il est reconnu que les critères de référence pour l'adéquation de la directive en matière de protection des données dans le domaine répressif ne fournissent que des détails limités sur cet aspect, le comité européen de la protection des données rappelle sa déclaration selon laquelle «les transferts ultérieurs de données à caractère personnel par le destinataire initial vers un autre pays tiers ou une organisation internationale ne doivent pas porter atteinte au niveau de protection, prévu dans l'Union, des personnes physiques dont les données sont transférées», qui ne saurait être interprétée comme n'incluant pas la nécessité d'une autorité de contrôle indépendante et de droits effectifs et opposables des personnes concernées. Par conséquent, le comité européen de la protection des données encourage la Commission à examiner spécifiquement ces modifications et à approfondir son évaluation du nouveau critère de protection des données.

¹⁴ La disposition désormais supprimée de la section 74A, paragraphe 4, de la loi DPA 2018 prévoyait une liste de critères qui était identique à l'article 36, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif.

16. Le comité comprend que les nouvelles règles relatives aux transferts de données à caractère personnel vers des pays tiers visent à offrir davantage de souplesse. Dans le même temps, le comité européen de la protection des données invite la Commission à contrôler l'application pratique de ces règles. Cela est particulièrement pertinent en ce qui concerne le nouveau pouvoir du secrétaire d'État d'établir des règlements qui identifient et approuvent un transfert, sur la base du nouveau critère de protection des données, par quelque moyen que ce soit, y compris par référence à des secteurs géographiques au sein d'un pays; les responsables du traitement et les sous-traitants; les destinataires des données; les types de données; les moyens de transfert; et les instruments juridiques. Il reste difficile de savoir, par exemple, comment un responsable du traitement ou un sous-traitant spécifique établi dans un pays tiers qui n'est pas considéré comme adéquat satisferait au critère en matière de protection des données en ce qui concerne des mécanismes de recours effectifs ou les droits des personnes concernées qui ne sont pas déjà établis dans le cadre juridique de ce pays tiers.
17. En outre, le comité européen de la protection des données invite la Commission à préciser dans sa décision que le critère relatif à l'«opportunité de faciliter les transferts de données à caractère personnel à destination et en provenance du Royaume-Uni» (section 74AA, paragraphe 3, de la loi DPA de 2018) n'est pas un élément du critère de la protection des données, mais simplement un facteur supplémentaire que le secrétaire d'État peut prendre en considération lorsque les conditions du critère sont pleinement remplies, étant donné que cela ne ressort pas clairement du libellé de la loi. À cet égard, le comité européen de la protection des données invite la Commission à surveiller les implications pratiques de la section 74AA, paragraphe 3, de la loi DPA 2018, étant donné qu'il reste à déterminer le rôle que l'«opportunité de faciliter les transferts de données à caractère personnel à destination et en provenance du Royaume-Uni» jouera dans ce contexte.

Prise de décision automatisée

18. Le comité européen de la protection des données prend note de la section 80 de la DUAA, qui introduit des changements importants dans la manière dont la prise de décision automatisée est réglementée au Royaume-Uni. Le comité européen de la protection des données observe que la DUAA adopte une approche plus permissive, ce qui constitue un écart par rapport à l'approche plus restrictive de l'Union. Les personnes perdent généralement le droit de ne pas être soumises à des décisions automatisées, sauf dans les cas impliquant des données sensibles. Avec les nouvelles sections 50A à 50D de la loi DPA 2018, les services répressifs peuvent prendre des décisions importantes en ayant recours à des processus automatisés, quelle que soit la base légale sur laquelle ils s'appuient, à condition de mettre en œuvre les garanties appropriées. Parmi ces garanties figurent la fourniture d'informations à la personne concernée sur les décisions importantes prises par des moyens automatisés et le traitement connexe des données à caractère personnel, à l'instar de l'article 11 et du considérant 38 de la directive en matière de protection des données dans le domaine répressif. En outre, la personne concernée doit avoir la possibilité de formuler des observations concernant de telles décisions, d'obtenir une intervention humaine du responsable du traitement en vue de réexaminer la décision automatisée et de contester une telle décision¹⁵.
19. En conséquence, la législation ne met plus l'accent sur la limitation du recours à la prise de décision automatisée, mais sur la garantie de la transparence, de l'examen humain et des contrôles des risques. Bien que la Commission reconnaisse ce changement au considérant 43

¹⁵ Section 50C, paragraphe 2, de la loi DPA 2018.

et l'analyse au considérant 47, le comité européen de la protection des données invite la Commission à expliquer plus en détail pourquoi elle considère que la nouvelle approche continue d'offrir un niveau de protection suffisant. En conséquence, le comité européen de la protection des données encourage la Commission à intégrer un examen plus détaillé de ce changement substantiel dans la décision d'adéquation finale.

20. Le comité européen de la protection des données prend également note du pouvoir discrétionnaire accordé au secrétaire d'État dans le contexte de la prise de décision automatisée¹⁶. Le comité européen de la protection des données croit comprendre que le secrétaire d'État dispose d'un large pouvoir d'appréciation pour déterminer ce qui peut être qualifié d'«intervention humaine significative» et de «décision déterminante ayant un effet d'importance comparable». L'étendue et la marge d'appréciation de ces pouvoirs pourraient susciter des inquiétudes notables, par exemple en raison de leur ampleur, en particulier dans le contexte de l'évolution rapide de l'environnement réglementaire et des progrès des technologies automatisées, telle que l'IA. Par conséquent, le comité européen de la protection des données invite la Commission à analyser ces nouveaux pouvoirs conférés au secrétaire d'État et à suivre toute évolution à cet égard.
21. Dans ce contexte, le comité européen de la protection des données souligne en particulier le rôle et la pertinence du droit de la personne concernée d'obtenir une intervention humaine. Les critères de référence du comité européen de la protection des données pour l'adéquation qui sont prévus par la directive en matière de protection des données dans le domaine répressif soulignent l'importance de ce droit, en particulier celui d'exprimer son point de vue, de recevoir une explication de la décision prise à l'issue de cette évaluation ou de contester la décision¹⁷. Si le droit d'obtenir une intervention humaine reste généralement l'une des garanties essentielles en cas de prise de décision automatisée, le comité européen de la protection des données observe qu'une nouvelle exemption a été introduite dans le cadre répressif du Royaume-Uni, qui permet aux autorités répressives de ne pas appliquer les garanties énumérées à la section 50C, paragraphe 2, de la loi DPA 2018, par exemple pour éviter l'obstruction d'une enquête¹⁸. Cette exemption exige désormais que la décision automatisée soit réexaminée avec une intervention humaine significative «dès que cela est raisonnablement possible» après que la décision a été prise¹⁹.
22. L'introduction de telles exemptions pourrait présenter un risque pour les droits et libertés des personnes concernées si ces exemptions ne sont pas suivies de près. À cette fin, l'exigence de réexamen en temps utile de l'exemption doit être appliquée minutieusement afin d'éviter les lacunes en matière de surveillance. Si les critères de cette intervention humaine sont interprétés de manière trop vague ou si le réexamen est retardé, cela pourrait conduire à un contrôle inadéquat et à une diminution de la responsabilité. Dans ce contexte, le comité européen de la protection des données rappelle la jurisprudence de la Cour de justice de l'Union européenne (CJUE), en particulier l'arrêt PNR de la Cour, selon lequel un réexamen humain significatif et

¹⁶ Voir considérant 46 du projet de décision.

¹⁷ Voir également le considérant 66 des recommandations 01/2021 du comité européen de la protection des données sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, adoptées le 2 février 2021.

¹⁸ Article 50C, paragraphe 4, point b), de la DUAA.

¹⁹ Voir également la fiche d'information du ministère de la science, de l'innovation et de la technologie, relative à la loi sur les données (utilisation et accès): RGPD britannique et DPA, publiés le 27 juin 2025, p. 14, <https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa>.

substantiel doit précéder tout résultat exploitable des systèmes automatisés de profilage ou de mise en correspondance²⁰. La position de la CJUE sur le réexamen humain préalable dans le contexte des données PNR fournit des orientations importantes sur la mise en œuvre des garanties concernant la prise de décision automatisée prévues par la directive en matière de protection des données dans le domaine répressif. Étant donné qu'une intervention humaine significative est essentielle pour assurer le respect des garanties dans la prise de décision automatisée, le comité demande instamment à la Commission d'inclure son évaluation de cette exemption nouvellement introduite dans la décision et de surveiller sa mise en œuvre dans la pratique.

Exigences en matière de journalisation

23. Le comité européen de la protection des données a rappelé dans ses recommandations 01/2021 que les mesures prises dans le cadre de protection des données d'un pays tiers permettant à une autorité compétente de démontrer sa conformité «devraient consister en la tenue ou de journaux d'activité de traitement des données pour une période appropriée»²¹. Dans son projet de décision, la Commission reconnaît qu'une telle obligation existe toujours dans le cadre du Royaume-Uni, mais qu'elle a été modifiée par la DUAA, étant donné que le responsable du traitement n'est plus tenu d'enregistrer le motif spécifique de la consultation ou de la divulgation de données à caractère personnel²². La suppression de cette obligation s'écarte des exigences de la directive en matière de protection des données dans le domaine répressif, qui prévoient une journalisation complète afin de garantir la transparence et la responsabilité. La directive en matière de protection des données dans le domaine répressif prévoit des registres détaillés démontrant la que le traitement est licite, y compris la justification de l'accès, afin de faciliter les audits et de prévenir les abus. L'absence de justification obligatoire de la journalisation dans le cadre du nouveau régime pourrait compliquer la vérification de la légalité de l'accès aux données, tant pour le responsable du traitement que pour les autorités de contrôle. Le comité européen de la protection des données invite la Commission à examiner plus avant ces exigences réduites en matière de journalisation dans sa décision finale et à vérifier si cette modification a ou non une incidence négative sur la surveillance et l'exercice des droits par les personnes concernées.

Exemptions concernant la sécurité nationale pour les autorités répressives

24. La section 88 de la DUAA met à jour les exemptions existantes concernant la sécurité nationale dans le cadre répressif afin de refléter celles prévues par le RGPD britannique et les régimes des services de renseignement²³. Si les autorités répressives sont déjà en mesure de limiter certaines obligations pour des motifs de protection de la sécurité nationale, telles que celles relatives aux droits des personnes concernées, la section 78A de la loi DPA 2018 inclura²⁴ également la

²⁰ Arrêt du 21 juin 2022, C-817/19, EU:C:2022:491, point 179.

²¹ Voir également le considérant 66 des recommandations 01/2021 du comité européen de la protection des données sur les critères de référence pour l'adéquation dans le cadre de la directive, adoptées le 2 février 2021.

²² Voir considérants 48 et 49 du projet de décision.

²³ Voir également la fiche d'information du Ministère de la science, de l'innovation et de la technologie, relative à la loi sur les données (utilisation et accès): RGPD britannique et DPA, publiés le 27 juin 2025, p. 14, <https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa>.

²⁴ La DUAA sera mise en place progressivement, en plusieurs étapes. Les principales modifications apportées à la législation en matière de protection des données dans la partie 5 de la DUAA prendront effet dans le cadre de la phase 3, environ 6 mois après l'assentiment royal, <https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement>.

majorité des principes de protection des données²⁵ et certaines exigences internationales en matière de transfert de données²⁶ en tant que dispositions qui peuvent être laissées inappliquées si cela est nécessaire aux fins de la protection de la sécurité nationale. En outre, certains des pouvoirs dont dispose le commissaire à l'information pour effectuer des inspections et prendre des mesures répressives²⁷ peuvent ne pas s'appliquer dans de telles circonstances.

25. Ces modifications ne sont mentionnées ni dans le projet de décision ni dans le projet de décision d'adéquation au titre de l'article 45 du RGPD. Toutefois, le comité européen de la protection des données estime qu'il est essentiel d'évaluer ces exemptions étendues au regard des principes de nécessité et de proportionnalité. Dans ce contexte, le comité européen de la protection des données rappelle la deuxième des quatre «garanties essentielles européennes»: toute limitation de l'exercice des droits et libertés reconnus par la charte doit respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, ne peut être apportée que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui²⁸. Le comité fait part de son inquiétude quant à ces exemptions concernant des principes fondamentaux de la protection des données, des exigences en matière de transferts internationaux et des pouvoirs dont dispose le commissaire à l'information.
26. En vertu de la règle révisée, cinq des six principes de protection des données peuvent être laissés inappliqués lorsque cela est nécessaire pour protéger la sécurité nationale²⁹. Ces principes disposent, entre autres, que la finalité répressive pour laquelle les données à caractère personnel sont collectées doit être déterminée, explicite et légitime, et que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard de cette finalité. Ils précisent également que les données à caractère personnel doivent être exactes et n'être conservées que pendant le temps nécessaire. Comme indiqué ci-dessus, les futures exemptions englobent en outre certaines des exigences en matière de transferts internationaux, telles que la deuxième condition relative aux transferts internationaux énoncée à la section 73, paragraphe 3, de la loi DPA 2018. Cette condition exige que les transferts soient fondés soit sur des règlements d'adéquation, soit sur des garanties appropriées, soit, en l'absence de tels règlements ou garanties, sur des circonstances spéciales. Les exemptions ont également une incidence sur les pouvoirs du commissaire à l'information, par exemple le pouvoir de publier des avis d'information et d'exécution³⁰.

²⁵ Section 78A, paragraphe 1, paragraphe 2, point a) et paragraphe 3, de la loi de 2018 sur la protection des données, telle qu'introduite par la section 88 de la DUAA.

²⁶ Section 78A, paragraphe 1, paragraphe 2, point d), et paragraphe 4, de la loi de 2018 sur la protection des données, telle qu'introduite par l'article 88 de la DUAA.

²⁷ Section 78A, paragraphe 1, paragraphe 2, points e), f) et g) de la loi de 2018 sur la protection des données, telle qu'introduite par l'article 88 de la DUAA.

²⁸ Recommandations 02/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020, p. 10.

²⁹ Conformément à la section 78A, paragraphes 2 et 3, de la loi de 2018 sur la protection des données, le chapitre 2 de la partie 3 de cette loi ne s'applique pas si cela est nécessaire aux fins de la protection de la sécurité nationale, à l'exception de la section 35, paragraphe 1, point a), (premier principe de protection des données) dans la mesure où il exige que le traitement des données à caractère personnel soit licite; b) la section 35, paragraphes 2 à 5 (licéité du traitement et limitations du traitement des données sensibles); c) la section 42 (garanties: traitement de données sensibles); et d) l'annexe 8 (conditions pour le traitement de données sensibles).

³⁰ Les avis d'information exigent d'un responsable du traitement ou d'un sous-traitant qu'ils fournissent au commissaire les informations raisonnablement nécessaires à l'exercice de ses fonctions. Les avis d'exécution habilite le commissaire à exiger d'une personne qu'elle prenne (ou s'abstienne de prendre) des mesures spécifiques, et ce lorsque le commissaire est convaincu que la personne ne respecte pas certaines obligations en matière de protection des données.

27. Le comité européen de la protection des données observe que, si les exemptions s'écartent clairement de la directive en matière de protection des données dans le domaine répressif, elles sont très semblables aux exceptions et restrictions pour la sécurité nationale prévues à l'article 11 de la convention modernisée 108 du Conseil de l'Europe (ci-après la «convention 108+»)³¹ que le Royaume-Uni a signée le 10 octobre 2018 mais qui, à la date du présent avis, n'a pas été ratifiée par le Royaume-Uni ou n'est pas encore entrée en vigueur³². À cet égard, le comité européen de la protection des données rappelle que le comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) a récemment publié des lignes directrices sur les principes généraux de l'article 11 de la convention 108+³³.
28. Dans ses lignes directrices, le Conseil de l'Europe souligne explicitement qu'aucune exception n'est applicable, entre autres, en ce qui concerne les principes de proportionnalité et de légitimité de la finalité du traitement. Cela implique que la proportionnalité du traitement des données doit être assurée, ainsi que l'obligation de traiter les données à caractère personnel à des fins légitimes. Conformément aux orientations du comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, le comité reste particulièrement vigilant en ce qui concerne toute exemption au principe de proportionnalité, ainsi qu'à l'obligation de traiter des données à caractère personnel à des fins légitimes. De même, selon le comité européen de la protection des données, toute exemption aux pouvoirs de l'autorité de contrôle doit être abordée avec prudence. Bien que des exigences spécifiques applicables aux activités de contrôle, telles que les habilitations de sécurité, puissent être appropriées dans le cadre du traitement lié à la sécurité nationale, il est essentiel d'assurer un contrôle efficace afin d'éviter de créer un vide en la matière. Dans le même esprit, l'article 11, paragraphe 3, de la convention 108+ prévoit que les exemptions à l'article 15³⁴ sont «sans préjudice de l'exigence que les activités de traitement à des fins de sécurité nationale et de défense fassent l'objet d'un contrôle et d'une supervision indépendants effectifs selon la législation nationale» des parties à la convention. En outre, toute exemption devrait être interprétée de la manière la plus restrictive possible. Le fait que des données à caractère personnel soient traitées à des fins de sécurité nationale ne devrait pas suffire à lui seul pour qu'une exemption puisse être invoquée. Il convient de préciser qu'une exemption au régime de protection des données doit être appliquée au cas par cas et uniquement si cela est nécessaire et proportionné³⁵.
29. Étant donné que les projets de décisions d'adéquation n'abordent pas ce point, le comité européen de la protection des données invite la Commission à compléter son évaluation dans le

³¹ Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223).

³² <https://www.coe.int/fr-FR/web/conventions/full-list?module=signatures-by-treaty&treatynum=223>.

³³ <https://rm.coe.int/t-pd-2021-7rev13-interpretation-of-general-principles-article-11-c108-/488028cf84>.

³⁴ L'article 15 de la convention 108+ précise la manière dont les parties à la convention, en prévoyant une ou plusieurs autorités de contrôle, veillent au respect des dispositions de la convention.

³⁵ Voir également l'article 11 de la convention 108+ qui précise que les exceptions doivent être prévues par la loi, respecter l'essence des droits et libertés fondamentales et constituer une mesure nécessaire et proportionnée dans une société démocratique. Selon les lignes directrices du comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel sur les principes généraux prévus à l'article 11, cela implique qu'une mise en balance des intérêts en présence entre la nécessité de prévoir des exceptions à certaines dispositions de la Convention et le respect des droits de l'homme et des libertés fondamentales des personnes soit opérée et justifiée.

projet de décision ainsi qu'à surveiller spécifiquement l'application pratique des exemptions en matière de sécurité nationale pour les autorités répressives.

Responsabilité conjointe du traitement entre les services de renseignement et les autorités répressives du Royaume-Uni

30. Sur la base des modifications apportées par la DUAA, les activités de traitement effectuées par les autorités répressives compétentes peuvent, dans des circonstances particulières, relever des règles normalement applicables au traitement des données à caractère personnel par les autorités nationales de sécurité³⁶. En d'autres termes, sous réserve des conditions énoncées à la section 89 de la DUAA, le régime de protection des données pour le traitement des données à des fins de sécurité nationale établi dans la partie 4 de la loi DPA 2018 est étendu au traitement des données par les autorités répressives.
31. La Commission souligne que les conditions de la section 89 de la DUAA prévoient des garanties strictes: une autorité compétente doit être désignée comme une «autorité compétente qualifiée» dans des règlements adoptés par le secrétaire d'État, qui, en outre, doit désigner une activité de traitement particulière effectuée par l'autorité compétente qualifiée en tant que responsable conjoint du traitement avec au moins un service de renseignement aux fins de la protection de la sécurité nationale³⁷.
32. Tout en reconnaissant que ces garanties entraînent des restrictions importantes, le comité invite la Commission à suivre la mise en œuvre pratique de ces règles. Il convient de veiller tout particulièrement à ce que la partie 4 de la loi DPA 2018 soit appliquée strictement aux opérations de traitement à des fins de sécurité nationale, sans être étendue à d'autres contextes. Bien que les États disposent d'une large marge d'appréciation en matière de sécurité nationale, comme l'a également reconnu la Cour européenne des droits de l'homme³⁸, le comité européen de la protection des données estime que les menaces pour la sécurité nationale doivent pouvoir être distinguées, par leur nature, leur gravité et les circonstances spécifiques, des risques généraux pour la sécurité publique ou des infractions pénales graves. Ce n'est que dans ces cas que l'action des autorités répressives dans le cadre du régime de protection des données des services de renseignement est compatible avec les principes de nécessité et de proportionnalité³⁹. En outre, le comité estime qu'il est nécessaire de vérifier si les autorités compétentes qualifiées sont en mesure dans la pratique de maintenir une distinction claire entre les différentes finalités de traitement afin de respecter le cadre juridique correspondant en conséquence.

Droit d'accès

33. La DUAA précise que les personnes concernées n'ont droit aux informations pertinentes que dans la mesure où le responsable du traitement est à même de les lui fournir sur la base d'une

³⁶ Voir le considérant 72 du projet de décision d'exécution de la Commission en vertu du règlement (UE) 2016/679, qui est tout aussi pertinent pour les deux avis du comité à cet égard (voir également la section 4 ci-dessus).

³⁷ Voir le considérant 73 du projet de décision d'exécution de la Commission en vertu du règlement (UE) 2016/679, qui est tout aussi pertinent pour les deux avis du comité à cet égard (voir également la section 4 ci-dessus).

³⁸ Arrêt de la Cour européenne des droits de l'homme du 25 mai 2021 dans l'affaire Big Brother Watch et autres c. Royaume-Uni, point 350.

³⁹ Il ressort de la jurisprudence de la CJUE que, lorsqu'on applique le critère de la nécessité et de la proportionnalité à la législation des États membres autorisant la conservation des données à caractère personnel et l'accès à celles-ci par les autorités publiques, des objectifs légitimes, tels que la sécurité nationale ou la lutte contre la criminalité grave sont des objectifs différents et, par conséquent, peuvent justifier différents types d'ingérence. Voir CJUE, affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., 6 octobre 2020.

recherche raisonnable et proportionnée. Cette modification est introduite à la fois dans le régime d'application de la loi et dans celui relatif à la sécurité nationale⁴⁰.

34. La Commission explique qu'il s'agit d'une précision conforme aux normes établies dans la jurisprudence nationale, lesquelles tiennent également compte des intérêts de la personne concernée. Néanmoins, le comité européen de la protection des données aurait apprécié des informations plus détaillées sur la manière d'interpréter la notion de «recherche raisonnable et proportionnée», d'autant plus que l'article 14 de la directive en matière de protection des données dans le domaine répressif ne comporte pas un tel élément. Le comité reconnaît qu'il peut effectivement exister des situations dans lesquelles les efforts déployés par un responsable du traitement pour identifier et localiser des informations sur la personne concernée pourraient être considérés comme déraisonnables et disproportionnés sans pour autant compromettre le niveau «essentiellement équivalent»⁴¹. Néanmoins, il est important de définir de manière adéquate la notion de «recherche raisonnable et proportionnée», qui, de l'avis du comité européen de la protection des données, devrait être interprétée de manière restrictive et suffisamment uniforme. Les autorités compétentes devraient avoir une compréhension cohérente de ce qui est «raisonnable et proportionné», qu'elle soit fondée sur la jurisprudence ou sur les orientations d'une autorité de contrôle, car l'application de cette notion pourrait potentiellement conduire à des normes différentes en matière de respect du droit d'accès, en particulier en fonction du niveau des mesures techniques et organisationnelles mises en place par le responsable du traitement pour traiter les demandes d'accès. Le comité européen de la protection des données invite la Commission à veiller à ce que le droit d'accès ne soit pas indûment limité.

Surveillance et voies de recours

35. Le comité européen de la protection des données observe que le système de surveillance des services répressifs en matière pénale en vertu de la loi DPA 2018 et de la loi de 2016 sur les pouvoirs d'enquête, ainsi que les mécanismes de recours, disponibles au titre de la partie 3 de la loi DPA 2018, de la loi de 2016 sur les pouvoirs d'enquête et de la loi de 1998 sur les droits de l'homme, restent dans une large mesure inchangés. En particulier, au Royaume-Uni, la surveillance continue d'être assurée, outre par le bureau du commissaire à l'information (Information Commissioner's Office, ci-après l'«ICO»), par une combinaison de différents commissaires, à savoir le commissaire aux pouvoirs d'enquête (Investigatory Powers Commissioner, ci-après l'«IPC»), assisté d'autres commissaires judiciaires, ainsi que le commissaire au matériel biométrique et aux caméras de surveillance.
36. Comme la Commission l'a expliqué au considérant 97 du projet de décision, la loi modificative de 2024 sur les pouvoirs d'enquête n'a apporté que des modifications limitées, notamment par l'introduction d'IPC adjoints auxquels l'IPC peut déléguer des pouvoirs spécifiques lorsqu'il n'est pas en mesure d'exercer ses fonctions ou n'est pas disponible à cette fin. Ces IPC adjoints doivent être des commissaires judiciaires et sont nommés par l'IPC.
37. Le comité observe avec satisfaction que les idées antérieures figurant dans le projet de loi sur la protection des données et les informations numériques, qui a précédé la DUUA, visant à supprimer le poste de commissaire au matériel biométrique et aux caméras de surveillance et à

⁴⁰ Section 78, paragraphes 3 et 4 de la DUAA, modifiant les sections 45 et 94 de la loi de 2018 sur la protection des données.

⁴¹ Par exemple, on pourrait faire valoir que tel est le cas pour la recherche de dispositifs saisis qui n'ont pas encore été analysés ou déchiffrés.

transférer ses fonctions à l'IPC, ont été abandonnées⁴². À cet égard, le comité invite la Commission à accorder une attention accrue au rôle du commissaire au matériel biométrique et aux caméras de surveillance et à en fournir une évaluation plus détaillée dans le système de contrôle au cours de son suivi et de ses futurs examens du projet de décision.

38. Comme l'a déjà souligné le comité européen de la protection des données dans son avis 14/2021, l'ICO est bien doté des pouvoirs nécessaires qui correspondent étroitement aux pouvoirs des autorités de contrôle des États membres de l'UE énoncés à l'article 58 du RGPD. Parallèlement, comme l'a déjà souligné le comité européen de la protection des données, l'existence de sanctions effectives joue un rôle important s'agissant de garantir le respect des règles⁴³.
39. Le comité européen de la protection des données observe avec satisfaction la politique de transparence de l'ICO et la disponibilité de données statistiques et analytiques, y compris des exemples, sur les activités répressives de l'ICO à l'égard des services répressifs⁴⁴. À cet égard, le comité constate que l'autorité britannique de contrôle préfère prononcer des rappels à l'ordre en cas de violation de la législation sur la protection des données par les forces de police. L'avis d'exécution adressé au ministère public en janvier 2024 constitue une exception notable⁴⁵. Le comité européen de la protection des données juge également positif que, depuis l'adoption de la décision d'exécution 2021/1773, l'ICO ait publié de nombreux codes de bonnes pratiques, lignes directrices, avis et autres documents d'orientation à l'intention des parties concernées.
40. Le comité européen de la protection des données observe également qu'avec l'entrée en vigueur de la DUAA, le contrôle indépendant de l'ICO, précédemment structuré en une seule société, évoluera vers une nouvelle structure par l'introduction d'une personne morale, à savoir la commission de l'information (CI)⁴⁶.
41. Le comité européen de la protection des données fournit une première analyse des implications possibles de ce changement dans son avis 26/2025 concernant le projet de décision d'exécution de la Commission conformément au règlement (UE) 2016/679 constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni. Les observations et les recommandations formulées dans cet avis sont également pleinement valables dans le contexte de la surveillance et de la supervision dans le domaine répressif.
42. En particulier, le comité européen de la protection des données invite la Commission à compléter le projet de décision d'adéquation par des détails supplémentaires concernant spécifiquement la structure et l'organisation de la CI, la nomination et la révocation des membres de la CI, en particulier en ce qui concerne la nomination de ses membres non exécutifs par le secrétaire d'État. Le comité estime également que la Commission devrait accorder une attention particulière, dans ses futurs réexamens, à la mise en balance, par la CI, des différentes tâches et des différents intérêts. En outre, le comité européen de la protection des données invite la

⁴² Voir <https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner>.

⁴³ Avis 14/2021 du comité européen de la protection des données, point 112.

⁴⁴ Voir, par exemple, les ensembles détaillés de données relatives aux réclamations en matière de protection des données, disponibles à l'adresse suivante: <https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-protection-complaints/>

⁴⁵ <https://ico.org.uk/action-weve-taken/enforcement/crown-prosecution-service-1/>.

⁴⁶ Voir le nouvel article 114A de la loi DPA 2018 et la section 6 de la DUAA.

Commission à donner suite aux résultats de la consultation publique publiée par l'ICO le 22 août 2025 concernant le traitement des plaintes⁴⁷ et à surveiller les politiques de l'IC qui en résultent.

43. À la lumière de ce qui précède, le comité européen de la protection des données réaffirme la nécessité pour la Commission de suivre de près l'application des mesures correctrices et des voies de recours pour les parties concernées dans le cadre de protection des données du Royaume-Uni.

Réexamen, durée et renouvellement de la décision

44. Le comité européen de la protection des données observe que le présent projet de décision s'applique pendant six ans et que sa date d'expiration est fixée au 27 décembre 2031, et observe que le Royaume-Uni reste le seul pays tiers dont les décisions d'adéquation contiennent une clause de suppression automatique. Le comité européen de la protection des données comprend que le nouveau cadre juridique mérite une attention particulière et invite la Commission à suivre attentivement la mise en œuvre de la DUAA, y compris les domaines prioritaires mis en évidence dans le présent avis et toutes les évolutions pertinentes au Royaume-Uni à cet égard. Le comité européen de la protection des données prend également note du fait que la «clause de suppression automatique» est combinée à l'examen périodique obligatoire prévu à l'article 36, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif, qui devrait avoir lieu au moins tous les quatre ans.
45. Le comité comprend que l'intention de la Commission est de procéder à un réexamen à la fin de la période de quatre ans sur la base de laquelle elle élaborera un rapport public. Le comité accueille favorablement l'intention de procéder au réexamen, qui poursuit un objectif différent de celui de la clause de suppression automatique dans le temps et joue un rôle important dans le suivi du cadre juridique, en particulier en ce qui concerne la responsabilité. Le comité européen de la protection des données demande donc instamment à la Commission de procéder au réexamen dans le délai légal précisé à l'article 36, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif, en tenant également compte des éléments déjà exposés dans la décision d'exécution (UE) 2021/1773⁴⁸ de la Commission ainsi que de toute autre évolution pertinente.
46. En outre, le comité européen de la protection des données croit comprendre que l'analyse figurant dans la décision d'exécution (UE) 2021/1773 de la Commission concernant la suspension et l'abrogation de la décision⁴⁹ est toujours valable. Dans un souci de sécurité juridique, le comité européen de la protection des données estime qu'une telle précision pourrait figurer dans la décision d'adéquation finale.
47. Le comité européen de la protection des données se félicite que le considérant 68 du projet de décision fasse référence à son rôle, ainsi qu'à celui de groupes de la société civile et d'autres parties prenantes dans le mécanisme d'examen périodique, conformément aux recommandations 01/2021 du comité européen de la protection des données⁵⁰. En ce qui concerne l'association concrète du comité européen de la protection des données et de ses

⁴⁷ <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/08/ico-consultation-on-draft-changes-to-how-we-handle-data-protection-complaints/>; <https://ico.org.uk/media2/nrljbhr2/proposed-dpt-framework-20250822.pdf>.

⁴⁸ Voir les considérants 165 à 167 de la décision d'exécution (UE) 2021/1773 de la Commission.

⁴⁹ Voir ibidem, considérants 168 à 171.

⁵⁰ Considérant 19 des recommandations 01/2021 du comité européen de la protection des données sur les critères de référence pour l'adéquation dans le cadre de la directive, adoptées le 2 février 2021.

représentants à la préparation et à la réalisation du futur réexamen, le comité réaffirme que tout document pertinent devrait être communiqué par écrit au comité suffisamment longtemps avant le réexamen.

48. Compte tenu des caractéristiques spécifiques du présent projet de décision, le comité européen de la protection des données invite la Commission à préciser et à clarifier autant que possible les éléments relatifs à la durée, au suivi, à la suspension, à la révocation, à la modification et au renouvellement de la décision.

Pour le comité européen de la protection des données

La présidente

Anu Talus