Déclaration

Déclaration 1/2025 sur le contrôle de l'âge en ligne

Adoptée le 11 février 2025[1]

Le comité européen de la protection des données a adopté la déclaration suivante :

1. CONTEXTE ET FINALITÉ DE LA PRÉSENTE DÉCLARATION

1. Le cadre réglementaire européen appelle à une protection accrue des enfants dans l'espace numérique. Ainsi, la directive « Services de médias audiovisuels »[2], que les États membres ont transposée dans leur législation nationale, souligne la possibilité de mettre en œuvre des mesures de vérification de l'âge (articles 6 *bis* et 28 *ter*), le RGPD introduit des conditions d'âge minimal pour le consentement au traitement de données à caractère personnel dans le cadre des services de la société de l'information (article 8), le règlement sur les services numériques[3] fait de la vérification de l'âge une mesure d'atténuation des risques (article 35, paragraphe 1), et un certain nombre d'États membres ont intégré dans leur législation nationale des conditions d'âge minimal pour exécuter des actes juridiques, exercer certains droits ou accéder à certains biens et services.

2. En outre, différentes initiatives nationales et européennes, telles que la stratégie pour un internet mieux adapté aux enfants (BIK +), voient dans le contrôle de l'âge une solution pour améliorer le bien-être des enfants en ligne grâce à un environnement numérique sûr et adapté à l'âge, conformément aux droits et principes numériques européens[4].

[1] Des corrections mineures ont été apportées à la mise en forme du présent document le 24 février 2025. D'autres corrections mineures ont été apportées au paragraphe 16 et au paragraphe 22, point b), le 1er avril 2025.

[2] Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «Services de médias audiovisuels»), compte tenu de l'évolution des réalités du marché, https://eur-lex.europa.eu/eli/dir/2018/1808/oj.

[3] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

[4] Better Internet for Kids, Guide to age assurance, https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest.

3. Sur la base de la définition fournie dans le rapport de recherche intitulé « *Mapping age assurance typologies and requirements* »[5] (Cartographie des typologies et des exigences en matière de contrôle de l'âge), le « contrôle de l'âge » est utilisé dans le présent document au sens d'un « *terme générique désignant les méthodes utilisées pour déterminer l'âge ou la tranche d'âge d'un individu à différents niveaux de confiance ou de certitude* ». Le même rapport mentionne trois grandes catégories de contrôle de l'âge : l'estimation de l'âge, la vérification de l'âge et l'autodéclaration.

4. Le contrôle de l'âge présente des risques spécifiques pour la protection des données. Un tel contrôle est ainsi susceptible d'avoir une incidence négative non seulement sur le droit des personnes physiques à la protection de leurs données à caractère personnel, mais aussi sur d'autres droits et libertés[6] tels que le droit à la non-discrimination, le droit à l'intégrité de la personne, le droit à la liberté et à la sûreté, et le droit à la liberté d'expression et d'information.

5. Reconnaissant l'importance d'une approche cohérente au niveau de l'Union sur le thème du contrôle de l'âge, le Comité européen de la protection des données (CEPD) souhaite fournir, sur la base du RGPD, des orientations spécifiques et des principes de haut niveau qui devraient être pris en considération lorsque des données à caractère personnel sont traitées dans le cadre du contrôle de l'âge.

6. Les principes proposés visent à concilier la protection des enfants et la protection des données à caractère personnel dans le contexte du contrôle de l'âge.

7. La priorité est de satisfaire aux exigences relatives aux grands principes énoncés à l'article 5 du RGPD (licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, confidentialité, intégrité et responsabilité) et de veiller à ce que ces principes de protection des données soient correctement mis en œuvre et restent solides au fil du temps, comme le prévoient l'article 25 du RGPD, « Protection des données dès la conception et protection des données par défaut », et l'article 32 du RGPD, « Sécurité du traitement ».

8. La présente déclaration est axée sur les principes applicables aux différents cas d'utilisation en ligne, y compris lorsqu'un âge minimal est prescrit par la loi ou d'une autre manière pour l'achat de produits, pour l'utilisation de services susceptibles de nuire aux enfants ou pour l'accomplissement d'actes juridiques, ainsi que lorsqu'il existe un devoir de protection des enfants (par exemple, veiller à ce que les services soient conçus ou proposés d'une manière adaptée à leur âge).

[5] Raiz Shaffique, M., et van der Hof, S., *Mapping age assurance typologies and requirements.*, 2024. Rapport de recherche s'inscrivant dans le cadre du projet « Un internet mieux adapté aux enfants » coordonné par le réseau scolaire européen (EUN) et commandé par la Commission européenne.

[6] En ce qui concerne l'incidence potentielle du contrôle de l'âge sur les droits et les libertés, voir, par exemple: *Roadmap for age verification* (Australian eSafety Commissionner, 2023), https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf?v=1731644498261, *A safe internet by default for children and the role of age verification* (AEPD, 2024), https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf ou *Trustworthy Age Assurance?*, une étude commandée par le cluster économie verte et sociale du groupe Les Verts/ALE au Parlement européen (2024), https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance.

9. Le comité européen de la protection des données pourra également publier, le cas échéant et dans d'autres documents, des orientations supplémentaires sur des cas d'utilisation spécifiques.

2. PRINCIPES DE CONCEPTION D'UNE ÉVALUATION DE L'ÂGE CONFORME AU RGPD

2.1 Jouissance pleine et effective des droits et libertés

Le contrôle de l'âge doit respecter l'ensemble des droits et libertés fondamentaux des personnes physiques[7], et l'intérêt supérieur de l'enfant devrait être une considération primordiale pour toutes les parties concernées par le processus.

10. Lorsqu'ils mettent en œuvre un contrôle de l'âge, les fournisseurs de services devraient veiller à prendre en considération non seulement son incidence sur le droit à la protection des données à caractère personnel, mais aussi sur tous les droits fondamentaux des personnes physiques.

11. Dans le cas particulier des enfants, l'intérêt supérieur de l'enfant[8] devrait être une considération primordiale pour toutes les parties concernées par le contrôle de l'âge. Il est important de noter qu'il n'existe pas de hiérarchie dans la prise en considération de l'intérêt supérieur de l'enfant, et qu'il convient de tenir compte de tous les droits des enfants[9], y compris leur droit à la protection des données à caractère personnel et à la protection contre la violence et toute autre forme d'exploitation, ainsi que leur droit d'accéder à des informations provenant de diverses sources et de voir leurs opinions dûment prises en considération.

2.2 Évaluation fondée sur les risques de la proportionnalité du contrôle de l'âge

Il convient de toujours mettre en œuvre un contrôle de l'âge d'une manière proportionnée et fondée sur les risques, qui soit compatible avec les droits et libertés des personnes physiques.

12. Les prestataires de services devraient adopter une démarche fondée sur les risques lors de la conception et de l'exploitation de leurs services. La nécessité et la proportionnalité du recours à des mesures de sécurité telles que le contrôle de l'âge devraient être démontrées, en tenant compte des risques associés. La nécessité pourrait être démontrée en procédant à une évaluation[10] visant à recenser et à évaluer les risques qu'un service particulier présente pour les enfants[11], comme l'exposition à des contacts ou à des contenus préjudiciables. Dans le

[7] En particulier, la Déclaration universelle des droits de l'homme, la Convention européenne des droits de l'homme, la Charte des droits fondamentaux de l'Union européenne et la Convention des Nations unies relative aux droits de l'enfant.

[8] Le Comité des droits de l'enfant des Nations unies a précisé que le principe de l'intérêt supérieur « *vise à assurer tant la réalisation complète et effective de tous les droits reconnus dans la Convention que le développement global de l'enfant* ». Observation générale nº 14 (2013) sur le droit de l'enfant à ce que son intérêt supérieur soit une considération primordiale (article 3, paragraphe 1), https://digitallibrary.un.org/record/778523/files/CRC_C_GC_14-FR.pdf.

[9] Observation générale nº 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique, CRC, mars 2021.

[10] Par exemple, une analyse d'impact sur les droits de l'enfant (ci-après « AIDE »), qui peut faire partie ou non d'une AIPD.

[11] Les experts dans le domaine des droits de l'enfant ont souligné les avantages de l'utilisation des analyses d'impact sur les droits de l'enfant (AIDE) comme un outil efficace *«pour traduire la convention [relative aux droits de l'enfant] et son article 3 dans la pratique, de manière concrète et structurée, en accordant la priorité à l'intérêt supérieur de l'enfant»* (in: Mukherjee, S., Pothong, K.,et Livingstone, S., *Child Rights Impact Assessment: A tool to realise child rights in the digital environment.* Londres: 5Rights Foundation, 2021). En outre, le Comité des

cadre de cette évaluation, les fournisseurs de services peuvent également tenir compte des droits des enfants, des possibilités offertes par l'environnement numérique, des points de vue des enfants ainsi que de l'évolution de leurs capacités afin de garantir une participation adaptée à l'âge[12].

13. Les fournisseurs de services doivent également respecter les droits et libertés de leurs utilisateurs, y compris le droit à la protection de leurs données à caractère personnel, en les conciliant avec la nécessité de mesures de sécurité qui devraient toujours être les moins intrusives parmi celles disponibles et qui devraient toujours être efficaces. Dans de nombreux cas, le contrôle de l'âge présente un risque élevé pour les droits et libertés des personnes concernées, ce qui nécessiterait donc qu'une analyse d'impact relative à la protection des données (« AIPD », article 35 du RGPD) soit effectuée avant le traitement, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement. L'AIPD devrait comprendre une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement. Elle devrait également inclure une évaluation de la nécessité et de la proportionnalité du traitement, recenser les risques découlant du traitement de données à caractère personnel aux fins du contrôle de l'âge et détailler les mesures visant à atténuer ces risques[13].

14. L'AIPD devrait guider la conception et la mise en œuvre de mesures techniques et organisationnelles appropriées pour assurer le respect de la protection des données. Cette approche fondée sur les risques est essentielle pour trouver un juste équilibre entre l'atteinte potentielle aux droits et libertés des personnes physiques et l'objectif visé dans ce contexte particulier, à savoir la sécurité des enfants. La portée, l'étendue et l'intensité de cette atteinte, au sens d'incidence sur les droits et libertés, doivent toujours être soigneusement évaluées[14]. Par exemple, un fournisseur de services traitant des données à caractère personnel pour vérifier l'âge de tous ses utilisateurs lorsqu'ils accèdent à l'ensemble de ses contenus ou services, même lorsque ces contenus ou services conviennent à tous les publics et sont dépourvus de tout risque, ne satisferait pas aux critères de nécessité et de proportionnalité.

2.3 Prévention des risques en matière de protection des données

Le contrôle de l'âge ne devrait pas entraîner de risques inutiles en matière de protection des données pour les personnes physiques. En particulier, le contrôle de l'âge ne devrait pas fournir aux prestataires de services des moyens supplémentaires d'identifier, de localiser, de profiler ou de pister les personnes physiques.

Nations unies a invité les États à imposer le recours aux AIDE afin d'intégrer les droits de l'enfant dans la réglementation et la conception de l'environnement numérique.

[12] Observation générale nº 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique, CRC, mars 2021.

[13] Lignes directrices du comité européen de la protection des données concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, https://ec.europa.eu/newsroom/article29/items/611236/en.

[14] Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_fr.

15. Les prestataires de services et tout tiers participant au contrôle de l'âge devraient mettre en œuvre des mesures et des garanties efficaces pour éviter que ce processus ne crée des risques inutiles pour la protection des données, tels que ceux résultant de l'identification, de la localisation, du profilage ou du pistage des personnes physiques. Le traitement de données à caractère personnel aux fins du contrôle de l'âge ne devrait pas fournir de moyens supplémentaires pour atteindre des finalités sans rapport avec le contrôle de l'âge proprement dit. Cela nécessite de sélectionner des méthodes permettant de s'assurer de l'âge des utilisateurs qui respectent pleinement le principe de protection des données dès la conception et par défaut (voir la section 2.8) et de mettre en œuvre des mesures qui garantissent le principe de loyauté, en veillant à ce que les données à caractère personnel ne soient pas traitées d'une manière qui soit préjudiciable de manière injustifiée, illégalement discriminatoire, inattendue ou trompeuse pour les personnes concernées.

16. Par exemple, une personne physique tenue de valider son âge pour accéder à un contenu pour adultes ne s'attend pas à ce que le prestataire de services utilise le contrôle de l'âge pour l'identifier ou pour déterminer sa localisation géographique précise ou pour surveiller, évaluer ou déduire des aspects personnels de son identité. Ce point est particulièrement pertinent pour le respect des principes de protection des données énoncés à l'article 5, paragraphe 1, du RGPD, dont la loyauté, la transparence et la limitation des finalités, ainsi que des règles de l'article 6, paragraphe 4 du RGPD, relatives aux utilisations à d'autres fins des données à caractère personnel. De même, conformément aux principes de limitation des finalités et de minimisation des données énoncés à l'article 5, paragraphe 1 du RGPD, le processus de contrôle de l'âge ne devrait pas permettre de cibler ou de profiler davantage les utilisateurs, notamment à des fins de ciblage commercial (par exemple, les publicités personnalisées) et malveillant (par exemple, le pédopiégeage, l'intimidation, la cyberprédation ou le harcèlement). Le Comité européen de la protection des données rappelle qu'en vertu du considérant 75 du RGPD, il peut exister des risques particuliers pour les droits en matière de protection des données lorsque les données à caractère personnel concernent des personnes physiques vulnérables, en particulier les enfants. D'une manière générale, il ne devrait pas être possible d'en apprendre plus qu'il n'est nécessaire au sujet d'une personne physique et de ses actions en établissant un profilage de cette personne sur la base des informations utilisées dans le cadre du processus de contrôle de l'âge. Ce principe devrait également être assuré, dans toute la mesure du possible, en cas de violation de données.

17. Il convient d'éviter les situations de déséquilibre de pouvoir afin d'empêcher les fournisseurs de services de contraindre des personnes à faire face à des risques inutiles en matière de protection des données du fait qu'ils ne sont pas en mesure d'agir[15]. Lorsque cela n'est pas possible, ces déséquilibres devraient être reconnus et pris en compte dans le cadre de contre-mesures appropriées[16]. Par exemple, des solutions viables pour prouver leur âge devraient

[15] Par exemple, lorsque les personnes concernées sont confrontées à une prise de décision automatisée sans mécanismes de recours appropriés ou lorsque le consentement ne peut être donné librement. Le concept de «déséquilibre de pouvoir» est examiné dans l'avis 08/2024 du comité européen de la protection des données sur la validité du consentement dans le cadre des modèles «consentir ou payer» mis en place par les grandes plateformes en ligne (section 4.2.1.3), https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_fr.pdf.

[16] Voir *EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them* (section 2.3), version 2.0, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

être proposées aux utilisateurs qui ne peuvent pas ou ne souhaitent pas utiliser une méthode spécifique de contrôle de l'âge. En outre, les fournisseurs de services devraient évaluer régulièrement si les méthodes et technologies retenues, y compris celles fournies par des tiers, fonctionnent conformément à leurs finalités et les adapter pour garantir la loyauté du traitement. Les tiers participant au contrôle de l'âge devraient également chercher à aider les prestataires de services à s'acquitter de leurs obligations, en n'introduisant pas de risques inutiles en matière de protection des données et en notifiant en temps utile toute modification pertinente de leurs politiques, de leurs conceptions, de leurs services, etc.

2.4 Limitation des finalités et minimisation des données

Les prestataires de services et tout tiers participant au contrôle de l'âge ne devraient traiter que les attributs liés à l'âge qui sont strictement nécessaires à leur finalité spécifique, explicite et légitime.

18. Dans la plupart des cas, le contrôle de l'âge a pour but de prendre des décisions de contrôle d'accès liées à l'âge, de prévenir les préjudices en ligne pour les enfants, d'offrir une expérience utilisateur appropriée en fonction de l'âge, etc. Quel que soit le cas d'utilisation, la finalité du traitement des données à caractère personnel devrait être spécifique et explicite (article 5, paragraphe 1, point b), du RGPD). Lorsque des données à caractère personnel ont été collectées, elles ne peuvent pas être traitées à d'autres fins, ni combinées à des données supplémentaires d'une manière incompatible avec ces finalités. Des mesures techniques telles que les technologies renforçant la protection de la vie privée (« PETs ») devraient être utilisées afin de limiter la possibilité de réaffectation des données à caractère personnel. Des mesures organisationnelles, telles que des politiques et des obligations contractuelles, qui limitent la réutilisation des données à caractère personnel[17], devraient également être déployées.

19. Est considéré comme un attribut lié à l'âge tout attribut indiquant qu'une personne physique a un certain âge, a plus ou moins qu'un certain âge ou se situe à l'intérieur d'une tranche d'âge. La spécification de la finalité déterminera les attributs liés à l'âge pertinents et nécessaires à collecter. Cela permettra également au responsable du traitement d'évaluer la proportionnalité du processus de contrôle de l'âge. Les avantages découlant de ce processus ne devraient pas être inférieurs aux inconvénients liés à l'exercice des droits fondamentaux[18] (voir section 2.2 ci-dessus).

20. Le responsable du traitement ne devrait donc collecter que les données à caractère personnel qui sont nécessaires, adéquates et pertinentes au regard des finalités auxquelles elles sont destinées. De cette manière, la minimisation des données contribue à étayer et à mettre en œuvre les principes de nécessité[19] et de proportionnalité. Par exemple, le prestataire de services peut seulement avoir besoin de savoir si l'âge de l'utilisateur est supérieur ou

[17] Voir les lignes directrices 4/2019 du comité européen de la protection des données relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut, version 2.0, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf.

[18] Voir les lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_fr.

[19] Voir le guide du CEPD pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.

inférieur à un seuil donné. Cette détermination pourrait être mise en œuvre par une approche par jeton reposant sur la participation d'un prestataire tiers, dans laquelle le prestataire de services ne voit que le résultat fonctionnel du processus de contrôle de l'âge (par exemple, « âge supérieur » ou « âge inférieur » au seuil défini)[20]. Différentes méthodes peuvent être pertinentes lorsque le prestataire de services doit savoir si l'utilisateur se situe dans une tranche d'âge donnée ou est né au cours d'une année donnée.

2.5 Efficacité du contrôle de l'âge

Il convient de démontrer que le contrôle de l'âge atteint un niveau d'efficacité adapté à la finalité pour laquelle elle est effectuée.

21. Les moyens par lesquels le contrôle de l'âge est effectué devraient être adéquats pour atteindre la finalité du traitement. En particulier, l'efficacité de toute mesure de contrôle de l'âge imposée par la loi devrait être considérée comme une condition préalable au respect des principes de nécessité[21] et de proportionnalité[22].

22. L'efficacité du contrôle de l'âge devrait être évaluée sur plusieurs points, et notamment :

a) Accessibilité. Le contrôle de l'âge devrait être largement accessible aux personnes physiques afin de valider leur âge ou de prouver qu'elles satisfont à une exigence liée à l'âge. Lorsque certaines catégories de personnes risquent d'être victimes de discrimination du fait d'une méthode spécifique de contrôle de l'âge, par exemple parce qu'elles ne sont pas en possession d'un document d'identité ou d'un téléphone portable approprié ou en raison d'un handicap, d'autres méthodes de contrôle de l'âge doivent être mises à disposition, lorsque cela est raisonnablement possible, avec des niveaux adéquats de respect de la vie privée, de sûreté et de sécurité. Les solutions de contrôle de l'âge doivent également être conformes à toute législation applicable en matière d'accessibilité[23] ;
b) Fiabilité. Conformément au principe d'exactitude (article 5, paragraphe 1, point d) du RGPD), toute méthode visant à déterminer si une personne physique satisfait à une exigence liée à l'âge devrait fournir un niveau de précision adéquat et cohérent pour déterminer si elle satisfait ou non à cette exigence. Des mécanismes de recours appropriés devraient être mis à disposition, notamment lorsque les utilisateurs peuvent être affectés de manière significative par une prise de décision automatisée, par exemple lorsque leurs attributs liés à l'âge n'ont pas été correctement établis (voir section 2.7 ci-dessous) ;

[20] Un prestataire tiers effectue une vérification de l'âge et fournit à l'utilisateur un «jeton d'identification d'âge» que l'utilisateur peut présenter au prestataire de services sans avoir besoin de prouver à nouveau son âge. Ce jeton peut contenir différentes caractéristiques relatives à l'utilisateur et indiquer quand, où ou comment le contrôle de l'âge a été effectué.

[21] Guide du CEPD pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.

[22] Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_fr.

[23] Par exemple, l'accessibilité des sites internet et des applications mobiles du secteur public et l'accessibilité des produits et services sont prévues respectivement par la directive sur l'accessibilité du web (DAW) et l'acte législatif européen sur l'accessibilité (AEA). Il doit être garanti que les solutions de contrôle de l'âge confirment ces législations, en satisfaisant aux exigences de la norme européenne harmonisée relative aux exigences en matière d'accessibilité applicables aux produits et services TIC, EN 301 549 v3.2.1.

c) Robustesse. Le contrôle de l'âge devrait être en mesure de faire face à des situations imprévues et de résister aux tentatives raisonnablement probables de fraude ou de contournement du système. Il convient de noter que la robustesse a peu de sens dans le contexte de l'autodéclaration d'un attribut lié à l'âge, étant donné que la fiabilité de cette méthode dépend principalement de la bonne foi de l'utilisateur[24].

En outre, les prestataires de services qui mettent en œuvre le contrôle de l'âge et les tiers participant au processus devraient être en mesure de démontrer son efficacité et être transparents quant aux moyens par lesquels ils atteignent des niveaux appropriés d'accessibilité, de fiabilité et de robustesse (voir section 2.10).

2.6 Licéité, loyauté et transparence

Les prestataires de services et tout tiers participant au contrôle de l'âge devraient veiller à ce que le traitement de toute donnée à caractère personnel à des fins de contrôle de l'âge soit licite, loyal et transparent pour les utilisateurs.

23. Les fournisseurs de services doivent veiller à disposer d'une base juridique applicable en vertu de l'article 6 du RGPD (et, le cas échéant, de l'exception applicable prévue à l'article 9, paragraphe 2) pour traiter des données à caractère personnel dans le cadre du contrôle de l'âge. Par exemple, ils peuvent devoir déployer un contrôle de l'âge pour se conformer à une obligation légale (article 6, paragraphe 1, point c), du RGPD), en tenant compte du fait que ce contrôle doit être proportionnée à l'objectif légitime poursuivi et aux exigences énoncées à l'article 6, paragraphe 3 du RGPD.

24. En outre, les fournisseurs de services doivent faire preuve de transparence auprès des utilisateurs quant à la manière exacte dont leurs données à caractère personnel sont utilisées et par qui. Ce point est particulièrement important lorsque plusieurs parties participent au processus de contrôle de l'âge. Avant que des données à caractère personnel ne soient traitées à des fins de contrôle de l'âge, il convient d'informer les utilisateurs (conformément aux articles 12, 13 et 14 du RGPD) afin qu'ils sachent, entre autres[25] :

- quelles données à caractère personnel seront traitées et comment ;
- si des tiers seront associés au processus et, dans l'affirmative, qui ils sont et qui sont les responsables du traitement et les sous-traitants dans ce scénario ;
- si leurs données seront partagées avec d'autres personnes ou transférées vers un pays tiers ;
- quelle est la durée de conservation de leurs données à caractère personnel ou, si cela n'est pas possible, quels sont les critères utilisés pour déterminer la durée de conservation ;

[24] Le comité européen de la protection des données a précédemment exprimé de sérieux doutes quant à l'efficacité de l'autodéclaration en tant que méthode de vérification de l'âge dans le contexte du traitement à haut risque dans la décision contraignante 2/2023 concernant le litige soumis par l'autorité de contrôle irlandaise concernant TikTok Technology Limited (article 65 du RGPD), https://www.edpb.europa.eu/system/files/2024-11/edpb_bindingdecision_202302_ie_sa_ttl_children_fr_0.pdf.

[25] Voir les lignes directrices du groupe de travail «article 29» sur la transparence au sens du règlement (UE) 2016/679, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf.

- quels sont leurs droits en ce qui concerne leurs données à caractère personnel (articles 15 à 22 du RGPD), y compris la manière dont ils peuvent contester une décision erronée prise en raison du contrôle de l'âge.

25. La transparence dans le contexte du contrôle de l'âge est particulièrement importante en ce qui concerne les enfants. Les prestataires de services doivent veiller à transmettre des informations transparentes aux enfants, lorsqu'ils sont concernés, d'une manière claire et facile à comprendre.

26. La notion de transparence est fondamentalement liée à la loyauté. Si les fournisseurs de services ne sont pas clairs et transparents quant à la manière dont ils traitent les informations des personnes physiques afin d'établir leur âge, il est peu probable que ce traitement puisse être considéré comme loyal, et il est dès lors peu probable qu'il soit licite. En particulier, si un fournisseur propose différentes méthodes permettant aux utilisateurs de valider leur âge, il se doit de faire preuve de transparence quant à l'incidence de chaque méthode du point de vue de la protection des données.

2.7 Prise de décision automatisée

Toute prise de décision automatisée dans le cadre du contrôle de l'âge devrait être conforme au RGPD. Le cas échéant, les prestataires de services et tout tiers concerné devraient prévoir des mesures appropriées pour protéger les droits et libertés et les intérêts légitimes des personnes physiques.

27. Le législateur de l'Union a opté pour une définition large de la prise de décision automatisée qui nécessite un examen au cas par cas[26]. Les décisions automatisées peuvent intervenir à différents stades du processus de contrôle de l'âge, soit pour accéder au contenu ou au service, soit dans le cadre des méthodes déployées pour prouver l'âge.

28. Un contrôle de l'âge entièrement automatisé peut produire des effets juridiques sur les personnes physiques concernées – par exemple concernant l'exercice de leur liberté d'expression – ou, a minima, les affecter de façon significative de manière similaire[27]. L'effet du contrôle automatisé de l'âge sur les droits des personnes physiques peut varier en fonction du type de contenu ou de service concerné.

29. Par conséquent, les prestataires de services et tout tiers participant au contrôle de l'âge devraient prévoir des voies et mécanismes de recours appropriés pour les utilisateurs dont les attributs liés à l'âge ne sont pas correctement établis. Il leur faut ainsi identifier les

[26] Affaire C-634/21, SCHUFA Holding (Scoring): Arrêt de la Cour (première chambre) du 7 décembre 2023 (demande de décision préjudicielle du Verwaltungsgericht Wiesbaden – Allemagne) – OQ / Land Hessen [«Renvoi préjudiciel – Protection des personnes physiques à l'égard du traitement des données à caractère personnel – Règlement (UE) 2016/679 – Article 22 – Décision individuelle automatisée – Sociétés fournissant des informations commerciales – Établissement automatisé d'une valeur de probabilité concernant la capacité d'une personne à honorer des engagements de paiement à l'avenir ("scoring") – Utilisation de cette valeur de probabilité par des tiers»)], https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A62021CA0634.

[27] Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, https://ec.europa.eu/newsroom/article29/items/612053/en.

interlocuteurs que les personnes concernées doivent contacter pour l'exercice de leurs droits[28], en fonction de l'architecture du processus de contrôle de l'âge.

30. Les prestataires de services et tout tiers concerné devraient accorder une attention particulière aux enfants. Comme indiqué au considérant 71 du RGPD, « *une décision […] qui est prise sur le seul fondement d'un traitement automatisé et qui produit des effets juridiques […] ou qui, de façon similaire, [...] affecte [la personne concernée] de manière significative, [...] ne devrait pas concerner un enfant* ». Les exceptions à cette règle devraient rester limitées à des circonstances bien balisées, par exemple lorsqu'il est nécessaire de « *protéger [son] bien-être* »[29]. En tout état de cause, les prestataires de services et tout tiers concerné devraient mettre en œuvre des mesures appropriées – par exemple des solutions de remplacement viables, des mécanismes de recours et, si applicable, une intervention humaine – avec des informations adaptées aux enfants, le cas échéant.

2.8 Protection des données dès la conception et protection des données par défaut

Le contrôle de l'âge devrait être conçu, mis en œuvre et évalué en tenant compte des méthodes et technologies disponibles les plus respectueuses de la vie privée afin de satisfaire aux exigences du RGPD et de protéger efficacement les droits des personnes concernées.

31. En vertu de l'article 25 du RGPD, les responsables du traitement concernés par le contrôle de l'âge devraient mettre en œuvre des mesures techniques et organisationnelles appropriées ainsi que les garanties nécessaires pour assurer la mise en œuvre effective de tous les principes de protection des données et, par conséquent, des droits et libertés des personnes concernées. L'obligation pour les responsables du traitement de voir la protection des données prise en compte par défaut au stade de la conception de toute activité de traitement de données à caractère personnel s'applique également aux sous-traitants et tout au long du cycle de vie du traitement.

32. Compte tenu de la diversité et de la gravité des risques associés aux systèmes de contrôle de l'âge, en particulier lorsque des documents d'identité ou des catégories particulières de données à caractère personnel telles que les données biométriques sont traités, il convient de veiller tout particulièrement à éviter tout accès, traitement, partage et stockage inutiles de données à caractère personnel. Les systèmes de contrôle de l'âge et tout instrument juridique ou technique fixant des exigences pour ces systèmes devraient également être régulièrement révisés et mis à jour, si nécessaire, afin de tenir compte de l'évolution rapide du paysage des technologies renforçant la protection de la vie privée dans le domaine de la gestion de l'identité numérique.

[28] Comme indiqué dans les lignes directrices du Comité européen de la protection des données (susmentionnées) : « *ces droits sont opposables au responsable du traitement qui crée le profil et au responsable du traitement qui prend une décision automatisée au sujet d'une personne concernée (avec ou sans intervention humaine), si ces entités ne sont pas les mêmes* ».

[29] Voir les lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 : « *Il peut néanmoins y avoir des circonstances dans lesquelles il est nécessaire que les responsables du traitement prennent des décisions exclusivement automatisées, y compris le profilage, produisant des effets juridiques ou affectant les enfants de manière significative de façon similaire, par exemple pour protéger leur bien-être* ».

33. Comme indiqué dans les lignes directrices du Comité européen de la protection des données en ce qui concerne la protection des données dès la conception et par défaut[30], la référence à l'« état des connaissances» dans le contexte de l'article 25 du RGPD impose aux responsables de traitement l'obligation de tenir compte des progrès technologiques actuels disponibles sur le marché lorsqu'ils déterminent les mesures techniques et organisationnelles appropriées susmentionnées. Les normes, les bonnes pratiques et les codes de conduite reconnus par les parties prenantes concernées peuvent être utiles pour déterminer ces mesures. Toutefois, le caractère approprié de ces mesures devrait être vérifié pour chaque activité de traitement particulière.

34. Par conséquent, le Comité européen de la protection des données recommande que, sur la base de l'état des connaissances en matière de contrôle de l'âge au moment de l'élaboration du présent document, il soit dûment tenu compte des technologies et des architectures favorisant les données détenues par les utilisateurs et le traitement local et sécurisé de ces données (sur le terminal de l'utilisateur), permettant des propriétés telles que la non-reliabilité[31] (du point de vue des différentes parties ainsi qu'en cas de collusions ou de violations de données) et la divulgation sélective[32] de données à caractère personnel sous le contrôle de la personne concernée. En outre, l'utilisation de stratégies telles que celles reposant sur la délivrance de lots[33] d'identifiants à usage unique ou sur des protocoles cryptographiques tels que des preuves à divulgation nulle de connaissance[34] devrait être mise à disposition des personnes dans les cas où le contrôle de l'âge peut entrainer des risques élevés pour leur vie privée.

2.9 Sécurité du contrôle de l'âge

Les prestataires de services et tout tiers participant au contrôle de l'âge devraient mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque.

35. Le RGPD exige des responsables de traitement et de leurs sous-traitants qu'ils mettent en place des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour les données à caractère personnel traitées (considérant 83 et article 32). La nature, la sensibilité et le volume des données à caractère personnel susceptibles d'être utilisées dans le cadre du contrôle de l'âge mettent en évidence l'effet négatif potentiel qu'une violation de données pourrait avoir.

36. Les modèles de confiance sont essentiels pour prévenir les violations de données dans le contexte du contrôle de l'âge, car ils définissent la manière dont les différentes parties

[30] Lignes directrices 4/2019 du comité européen de la protection des données relatives à l'article 25 – Protection des données dès la conception et protection des données par défaut, version 2.0, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf.

[31] La non-associativité signifie qu'il est impossible d'associer ou de corréler différentes données, actions ou transactions à une personne concernée spécifique.

[32] La divulgation sélective est une caractéristique des jetons, des identifiants et des attestations qui permet aux personnes concernées de ne partager que les informations qu'elles souhaitent avec des parties spécifiques, au cas par cas.

[33] La délivrance par lots repose sur la réponse à une demande de justificatif émanant de la personne concernée, accompagnée d'un ensemble ou d'un groupe d'identifiants produits en même temps.

[34] Une preuve à connaissance nulle est un protocole dans lequel une partie (l'auteur) peut démontrer à une autre partie (le vérificateur) qu'une déclaration donnée est vraie, sans transmettre au vérificateur aucune information allant au-delà de la seule validité de cette déclaration.

peuvent mutuellement vérifier leur identité et leur intégrité. Ils facilitent une communication et un échange de données sécurisés entre des participants n'ayant peut-être pas de relations préalables. En outre, la pseudonymisation et le chiffrement des données à caractère personnel peuvent être des mesures utiles pour atténuer les éventuels effets négatifs des violations de données. Le respect du principe de limitation du stockage et l'utilisation de périodes de rétention courtes peuvent également être essentiels pour garantir la sécurité en ce qui concerne le contrôle de l'âge, car ils réduisent la surface d'exposition. Une politique de non-conservation des journaux peut être considérée comme une garantie précieuse : une fois l'âge de l'utilisateur vérifié, aucun enregistrement des données à caractère personnel utilisées pour le processus de contrôle de l'âge n'est conservé.

37. Dans la pratique, compte tenu de la pression juridique croissante exercée sur la mise en œuvre du contrôle de l'âge et du nombre de fournisseurs susceptibles d'être soumis à de telles règles, il faut s'attendre à ce que des violations de la sécurité se produisent. Il convient de s'assurer que toutes les mesures de protection techniques et organisationnelles appropriées soient mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite, ce qui déterminera si l'obligation de notification s'applique[35]. Un élément clé de toute politique de sécurité des données est la capacité, dans la mesure du possible, de prévenir une violation et, lorsqu'elle se produit, de réagir en temps utile. Par conséquent, la capacité de rétablir rapidement la disponibilité d'un contrôle de l'âge après une violation de la sécurité devrait également être considérée comme essentielle. De même, il est essentiel de garantir la résilience de l'écosystème de contrôle de l'âge, en favorisant l'existence de différentes solutions et d'entités peu couplées entre elles[36] et suffisamment indépendantes les unes des autres pour que la défaillance de l'une d'elles n'entraîne pas d'importantes limitations d'accès.

38. Si les mesures de sécurité sont de la plus haute importance pour les systèmes de contrôle de l'âge, elles ne garantissent pas qu'un accès, autorisé ou non, aux données à caractère personnel n'aura pas d'incidence sur les droits des personnes physiques. Elles ne peuvent se substituer à l'application des principes de nécessité, de proportionnalité ou de protection des données dès la conception et par défaut.

2.10 Principe de responsabilité

Les prestataires de services et tout tiers concerné devraient mettre en œuvre des méthodes de gouvernance qui leur permettent de rendre des comptes concernant leur stratégie de contrôle de l'âge et de démontrer qu'ils respectent la réglementation en matière de protection des données et les autres exigences légales.

39. Compte tenu de l'implication de différentes parties prenantes, la gouvernance du contrôle de l'âge joue un rôle crucial dans l'obligation de rendre des comptes. Le contrôle de l'âge devrait fonctionner dans un cadre de gouvernance de nature à garantir que tous les processus et

[35] Lignes directrices 9/2022 du comité européen de la protection des données sur la notification de violations de données à caractère personnel en vertu du RGPD, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_fr.

[36] Les parties dépendent le moins possible les unes des autres, ce qui réduit l'ampleur de l'incidence en cas de changements ou de défaillances.

systèmes sont conçus, mis en œuvre, révisés, documentés, évalués, utilisés, gérés, testés ou contrôlés d'une manière qui respecte la réglementation en matière de protection des données et les autres exigences légales. Ce cadre devrait inclure, au minimum, les politiques de protection des données (article 24, paragraphe 2 du RGPD) et les processus de hiérarchisation et de prise de décision nécessaires pour atteindre les objectifs de conformité et gérer les risques de manière appropriée tout au long du cycle de vie du contrôle de l'âge.

40. Par exemple, le cadre de gouvernance devrait définir qui est responsable et comment, du point de vue du responsable du traitement/sous-traitant, pour quelles activités ou opérations exactes dans le cadre du traitement. Il devrait également garantir que le contrôle de l'âge peut effectivement être contrôlé par les autorités et les parties prenantes concernées. Le cadre de gouvernance est essentiel pour l'obligation de rendre des comptes, mais aussi pour la transparence et la confiance dans le processus de contrôle de l'âge. Les personnes concernées sont plus susceptibles de faire confiance à des méthodes transparentes concernant leurs activités, leurs processus décisionnels, etc.

41. En outre, une partie du cadre de gouvernance consiste à garantir l'efficacité (section 2.5), la protection des données dès la conception et par défaut (section 2.8) et la sécurité (section 2.9) du contrôle de l'âge.

Pour le comité européen de la protection des données

La présidente

(Anu Talus)