
# Lignes directrices 4/2019 relatives à l'article 25

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

## Version 2.0

## Adoptées le 20 octobre 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

## Historique des versions

| | | |
|---|---|---|
| Version 1.0 | 13 novembre 2019 | Adoption des lignes directrices pour consultation publique |
| Version 2.0 | 20 octobre 2020 | Adoption des lignes directrices par le comité européen de la protection des données après consultation publique |

# Table des matières

## Le comité européen de la protection des données

vu l'article 70, paragraphe 1, point e), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord EEE et en particulier son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018,

vu les articles 12 et 22 de son règlement intérieur,

**A ADOPTE LES LIGNES DIRECTRICES SUIVANTES**

**Synthèse**

Dans un monde de plus en plus numérique, le respect des exigences relatives à la protection des données dès la conception et à la protection des données par défaut joue un rôle essentiel dans la promotion de la protection de la vie privée et des données au sein de la société. Il est par conséquent essentiel que les responsables du traitement accordent toute l'attention nécessaire à cette responsabilité et mettent en œuvre les obligations du RGPD lors de la conception des opérations de traitement.

Ces lignes directrices fournissent des orientations sur l'obligation de protection des données dès la conception et de protection des données par défaut, telle qu'exposée à l'article 25 du RGPD. La protection des données dès la conception et la protection des données par défaut constituent une obligation pour tous les responsables du traitement, indépendamment de la taille et du degré de complexité du traitement. Pour pouvoir mettre en œuvre les exigences relatives à la protection des données dès la conception et à la protection des données par défaut, il est fondamental que le responsable du traitement comprenne les principes relatifs à la protection des données ainsi que les droits et libertés de la personne concernée.

L'obligation essentielle consiste en la mise en œuvre des mesures *appropriées* et des garanties nécessaires pour assurer, *dès la conception et par défaut, la mise en œuvre effective* des *principes de protection des données* et, par conséquent, des *droits et libertés des personnes concernées*. L'article 25 définit à la fois les éléments dès la conception et les éléments par défaut à prendre en compte. Ces éléments sont précisés dans les présentes lignes directrices.

L'article 25, paragraphe 1, dispose que, lorsqu'ils planifient un nouveau traitement, les responsables du traitement doivent tenir compte, dès un stade précoce, de la protection des données dès la conception et de la protection des données par défaut. Les responsables du traitement mettent en œuvre la protection des données dès la conception et la protection des données par défaut *avant* le traitement, et *de manière continue* pendant celui-ci, en examinant régulièrement l'effectivité des mesures et des garanties choisies. La protection des données dès la conception et la protection des données par défaut s'appliquent également aux systèmes existants qui traitent des données à caractère personnel.

Les lignes directrices contiennent également des orientations sur la manière de mettre en œuvre de façon effective les principes relatifs à la protection des données énoncés à l'article 5; elles énumèrent les éléments clés pour la protection des données dès la conception et la protection des données par défaut et présentent des cas concrets à titre d'illustration. Le responsable du traitement devrait évaluer le caractère approprié des mesures proposées dans le cadre du traitement particulier concerné.

Le comité européen de la protection des données formule des recommandations sur la manière dont les responsables du traitement, les sous-traitants et les producteurs peuvent coopérer pour mettre en œuvre la protection des données dès la conception et la protection des données par défaut. Le comité encourage les responsables du traitement du secteur industriel, les sous-traitants et les producteurs à utiliser la protection des données dès la conception et la protection des données par défaut comme moyen d'obtenir un avantage concurrentiel lors de la commercialisation de leurs produits auprès de responsables du traitement et de personnes concernées. Il incite également tous les responsables du traitement à avoir recours aux certifications et aux codes de conduite.

# 1 CHAMP D'APPLICATION

1. Les lignes directrices sont axées sur la mise en œuvre, par les responsables du traitement, de la protection des données dès la conception et de la protection des données par défaut sur la base de l'obligation prévue à l'article 25 du RGPD.[1] D'autres acteurs, tels que les sous-traitants, les fabricants de produits, les prestataires de services ou les producteurs d'applications (ci-après les «producteurs»), qui ne sont pas directement visés par l'article 25, peuvent également trouver ces lignes directrices utiles pour créer des produits et des services conformes au RGPD, qui permettent aux responsables du traitement de s'acquitter des obligations qui leur incombent en matière de protection des données.[2] Le considérant 78 du RGPD précise que la protection des données dès la conception et la protection des données par défaut devraient être prises en considération dans le cadre des marchés publics. Bien que tous les responsables du traitement aient l'obligation d'intégrer la protection des données dès la conception et la protection des données par défaut dans leurs activités de traitement, cette disposition favorise l'adoption des principes relatifs à la protection des données, pour lesquels les administrations publiques devraient montrer l'exemple. Le responsable du traitement est responsable du respect des obligations relatives à la protection des données dès la conception et à la protection des données par défaut, dans le cadre du traitement effectué par ses sous-traitants et sous-traitants ultérieurs. Par conséquent, il devrait tenir compte de cette obligation dans les contrats qu'il passe avec ces parties.

2. L'article 25 impose l'obligation pour les responsables du traitement de s'assurer que la protection des données est intégrée comme paramètre par défaut dans le traitement des données à caractère personnel. Cette obligation s'applique à toutes les étapes du traitement. La protection des données dès la conception et la protection des données par défaut constituent également une obligation pour

[1] Les interprétations qui sont formulées dans le présent document s'appliquent également à l'article 20 de la directive (UE) 2016/680 et à l'article 27 du règlement (UE) 2018/1725.

[2] Le considérant 78 du RGPD précise clairement cette nécessité: «*Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en considération le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données*».

les systèmes de traitement préexistant à l'entrée en vigueur du RGPD. Les responsables du traitement doivent veiller à ce que le traitement soit constamment mis à jour conformément au RGPD. Pour de plus amples informations sur la manière de maintenir un système existant en conformité avec les principes relatifs à la protection des données dès la conception et à la protection des données par défaut, voir le sous-chapitre 2.1.4 des présentes lignes directrices. L'élément central de cette disposition est d'assurer une protection *appropriée* et *effective* des données, *dès la conception* et *par défaut*, ce qui signifie que les responsables du traitement devraient être en mesure de démontrer qu'ils ont mis en place les mesures et les garanties appropriées, dans le cadre du traitement, pour garantir l'effectivité des principes relatifs à la protection des données et des droits et libertés des personnes concernées.

3. Le chapitre deux des lignes directrices est axé sur l'interprétation des exigences énoncées à l'article 25 et examine les obligations juridiques instaurées par la disposition. Des exemples de la manière d'appliquer la protection des données dès la conception et la protection des données par défaut, dans le cadre des principes spécifiques relatifs à la protection des données, sont fournis au chapitre 3.

4. Les lignes directrices traitent, au chapitre 4, de la possibilité de mettre en place un mécanisme de certification pour démontrer le respect de l'article 25, et, au chapitre 5, de la manière dont les autorités de contrôle peuvent faire appliquer cet article. Enfin, les lignes directrices fournissent aux parties prenantes des recommandations sur la manière de mener à bien la mise en œuvre de la protection des données dès la conception et de la protection des données par défaut. Le comité européen de la protection des données, qui est conscient des défis que doivent relever les petites et moyennes entreprises (ci-après les «PME») pour s'acquitter pleinement de leurs obligations en matière de protection des données dès la conception et de protection des données par défaut, fournit au chapitre 6 des recommandations supplémentaires spécialement destinées aux PME.

# 2 ANALYSE DE L'ARTICLE 25, PARAGRAPHES 1 ET 2, PROTECTION DES DONNEES DES LA CONCEPTION ET PROTECTION DES DONNEES PAR DEFAUT

5. L'objectif de ce chapitre est d'examiner et de fournir des orientations respectivement sur les exigences en matière de protection des données dès la conception énoncées à l'article 25, paragraphe 1, du RGPD et en matière de protection des données par défaut énoncées à l'article 25, paragraphe 2, du RGPD. La protection des données dès la conception et la protection des données par défaut sont des notions complémentaires qui se renforcent mutuellement. Les personnes concernées bénéficieront d'une meilleure protection des données par défaut si la protection des données dès la conception est mise en œuvre simultanément, et vice versa.

6. La protection des données dès la conception et la protection des données par défaut sont obligatoires pour tous les responsables du traitement, qu'il s'agisse de petites entreprises ou de multinationales. Cela étant dit, la complexité de la mise en œuvre de la protection des données dès la conception et de la protection des données par défaut peut varier en fonction de l'opération de traitement concernée. Toutefois, la mise en œuvre de la protection des données dès la conception et de la protection des données par défaut peut, dans tous les cas, avoir des effets positifs pour le responsable du traitement comme pour la personne concernée, indépendamment de leur taille.

## 2.1 Article 25, paragraphe 1: Protection des données dès la conception

### 2.1.1 Obligation du responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées, ainsi que les garanties nécessaires, dans le cadre du traitement

7. Conformément à l'article 25, paragraphe 1, le responsable du traitement met en œuvre des *mesures* techniques et organisationnelles *appropriées,* qui sont destinées à mettre en œuvre les principes relatifs à la protection des données et à assortir le traitement des *garanties nécessaires* pour répondre aux exigences et protéger les droits et libertés des personnes concernées. Tant les mesures appropriées que les garanties nécessaires contribuent à la réalisation du même objectif, à savoir protéger les droits des personnes concernées et veiller à ce que la protection des données à caractère personnel les concernant soit intégrée au traitement.

8. *Les mesures techniques et organisationnelles appropriées* et les *garanties* nécessaires peuvent s'entendre au sens large comme toute méthode ou tout moyen qu'un responsable du traitement peut employer dans le cadre du traitement. *Approprié* signifie que les mesures et les garanties nécessaires doivent être adaptées pour atteindre le but visé, c'est-à-dire qu'elles doivent mettre en œuvre les principes de protection des données *de façon effective*[3]. Ainsi, l'exigence du caractère approprié est étroitement liée à l'exigence d'effectivité.

9. On entend par «mesure technique ou organisationnelle et garantie» diverses mesures pouvant aller de l'utilisation de solutions techniques avancées à la formation de base du personnel. Parmi les exemples de mesures et de garanties adéquates, on peut citer, selon le contexte et les risques associés au traitement concerné, la pseudonymisation des données à caractère personnel[4], la conservation des données à caractère personnel disponibles dans un format structuré, couramment utilisé et lisible par machine, la possibilité pour les personnes concernées d'intervenir dans le traitement, la fourniture d'informations sur la conservation des données à caractère personnel, la mise en place de systèmes de détection des logiciels malveillants, la formation des salariés aux principes de base de la «cyberhygiène», la mise en place de systèmes de gestion de la protection de la vie privée et de la sécurité des informations, l'obligation contractuelle pour les sous-traitants de mettre en œuvre des pratiques spécifiques de minimisation des données, etc.

10. Les normes, les bonnes pratiques et les codes de conduite reconnus par les associations et autres organismes représentant les différentes catégories de responsables du traitement peuvent être utiles pour déterminer les mesures appropriées. Toutefois, le responsable du traitement doit vérifier le caractère approprié des mesures pour le traitement particulier concerné.

### 2.1.2 Conçues pour mettre en œuvre les principes relatifs à la protection des données de façon effective et protéger les droits et libertés des personnes concernées

11. Les *principes relatifs à la protection des données* figurent à l'article 5 (ci-après «les principes»). Les *droits et libertés des personnes concernées* sont les droits et libertés fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel, protection qui est définie, à l'article premier, paragraphe 2, comme l'objectif du RGPD (ci-après «les droits»)[5]. La formulation précise de ces droits et libertés figure dans la Charte des droits fondamentaux de l'UE. Il

[3] L'«effectivité» est abordée ci-après au sous-chapitre 2.1.2.
[4] Définie à l'article 4, paragraphe 5, du RGPD.
[5] Voir considérant 4 du RGPD.

est essentiel que le responsable du traitement comprenne la signification des *principes* et des *droits*, qui constituent la base de la protection conférée par le RGPD, et plus particulièrement par l'obligation de protection des données dès la conception et de protection des données par défaut.

12. Lors de la mise en œuvre des mesures techniques et organisationnelles appropriées, les garanties et mesures devraient être *conçues* dans l'optique de la mise en œuvre effective de chacun des principes susmentionnés et de la protection des droits qui s'ensuit.

**Garantir l'effectivité**

13. L'effectivité est au centre de la notion de protection des données dès la conception. L'obligation de mettre en œuvre les principes de façon effective signifie que les responsables du traitement doivent mettre en œuvre les mesures et les garanties nécessaires pour protéger ces principes, afin de garantir les droits des personnes concernées. Chaque mesure mise en œuvre devrait produire les résultats escomptés pour le traitement prévu par le responsable du traitement. Il découle deux conséquences de cette observation.

14. Premièrement, si l'article 25 n'impose pas la mise en œuvre de mesures techniques et organisationnelles spécifiques, il exige que les mesures et garanties choisies soient propres à la mise en œuvre des principes de protection des données dans le cadre du traitement particulier concerné. À cet égard, les mesures et garanties devraient être conçues de manière robuste et le responsable du traitement devrait être à même de mettre en œuvre des mesures supplémentaires pour s'adapter à une éventuelle augmentation du risque[6]. L'effectivité ou non des mesures dépendra donc du contexte du traitement concerné et d'une évaluation de certains éléments qui devraient être pris en considération lors de la détermination des moyens du traitement. Les éléments susmentionnés seront examinés ci-dessous au sous-chapitre 2.1.3.

15. En outre, les responsables du traitement devraient être en mesure de démontrer que les principes ont été maintenus.

16. Les mesures et les garanties mises en œuvre devraient produire l'effet escompté en termes de protection des données, et le responsable du traitement devrait documenter les mesures techniques et organisationnelles mises en place[7]. Pour ce faire, le responsable du traitement peut définir des indicateurs clés de performance (ICP) appropriés pour démontrer l'effectivité des mesures. Un ICP est une valeur mesurable choisie par le responsable du traitement, qui démontre l'efficacité avec laquelle ce dernier remplit son objectif de protection des données. Les ICP peuvent être *quantitatifs*, tels que le pourcentage de faux positifs ou de faux négatifs, la réduction des plaintes, la réduction du temps de réponse lorsque les personnes concernées exercent leurs droits, ou *qualitatifs*, tels que les évaluations de performances, le recours à des grilles de classement ou les évaluations d'experts. En lieu et place

[6] Les principes fondamentaux applicables aux responsables du traitement (légitimité, minimisation des données, limitation de la finalité, transparence, intégrité des données, exactitude des données) doivent rester identiques, indépendamment du traitement et des risques pour les personnes concernées. Toutefois, la prise en considération de la nature et de la portée de ce traitement a toujours constitué une partie intégrante de l'application de ces principes, de sorte qu'ils sont modulables par nature. Groupe de travail «Article 29». «Statement on the role of a risk-based approach in data protection legal frameworks» (Déclaration sur le rôle d'une approche fondée sur les risques dans les cadres juridiques de protection des données) WP 218 du 30 mai 2014, p.3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[7] Voir les considérants 74 et 78.

des ICP, les responsables du traitement peuvent démontrer la mise en œuvre effective des principes en fournissant une justification de leur évaluation de l'efficacité des mesures et des garanties choisies.

### 2.1.3 Éléments à prendre en considération

17. L'article 25 énumère les éléments que le responsable du traitement doit prendre en considération pour définir les mesures d'une opération de traitement spécifique. La section qui suit comporte des orientations sur la manière d'appliquer ces éléments lors du processus de conception, et notamment lors de la conception des paramètres par défaut. Ces éléments concourent tous à déterminer si une mesure est appropriée pour mettre en œuvre les principes de façon effective. Ainsi, ces éléments ne sont pas une finalité en soi, mais des facteurs à considérer ensemble pour atteindre l'objectif visé.

#### *2.1.3.1 «État des connaissances»*

18. La notion d'«état des connaissances» figure dans divers textes de l'acquis de l'UE, par exemple en matière de protection de l'environnement et de sécurité des produits. Dans le RGPD, il est fait référence à l'«état des connaissances»[8] non seulement à l'article 32, pour les mesures de sécurité[9] [10], mais aussi à l'article 25, ce qui étend ce critère à toutes les mesures techniques et organisationnelles intégrées au traitement.

19. Dans le cadre de l'article 25, la référence à l'«état des connaissances» impose aux responsables du traitement, lors de la définition des mesures techniques et organisationnelles appropriées, de **prendre en considération le progrès technologique actuel** présent sur le marché. Cette disposition impose l'obligation pour les responsables du traitement d'avoir connaissance et de se tenir informés des progrès technologiques, de la manière dont la technologie peut présenter des risques ou des opportunités, en matière de protection des données, pour l'opération de traitement, et de la manière de mettre en œuvre et de tenir à jour les mesures et garanties qui *assurent une mise en œuvre effective* des principes et des droits des personnes concernées dans un contexte technologique en constante évolution.

20. L'«état des connaissances» est une notion dynamique qui ne peut se définir de manière statique à un moment précis, mais qui doit être évaluée en continu au regard des progrès technologiques. Compte tenu des avancées technologiques, un responsable du traitement pourrait estimer qu'une mesure a fourni à un moment donné un niveau de protection adéquat, mais que ce n'est plus le cas. Le fait de ne pas se tenir informé des évolutions technologiques pourrait donc entraîner une non-conformité avec l'article 25.

21. Le critère de l'«état des connaissances» ne s'applique pas uniquement aux mesures technologiques, mais aussi aux mesures organisationnelles. L'absence de mesures organisationnelles adéquates peut faire baisser, voire réduire à néant, l'effectivité d'une technologie choisie. Parmi les exemples de mesures organisationnelles, on peut citer l'adoption de politiques internes, la réalisation de formations

[8] Voir la décision «Kalkar» du Tribunal constitutionnel fédéral allemand (1978): https://germanlawarchive.iuscomp.org/?p=67; cette décision peut jeter les bases d'une méthodologie pour une définition objective de la notion. Sur cette base, le niveau technologique correspondant à l'«état des connaissances» se situerait entre le niveau technologique correspondant aux «connaissances scientifiques et à la recherche existantes» et les «règles techniques généralement acceptées» et davantage établies. L'«état des connaissances» peut donc être défini comme le niveau technologique d'un service, d'une technique ou d'un produit qui existe sur le marché et présente l'efficacité maximale pour atteindre les objectifs recensés.
[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security
[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

actualisées sur la technologie, la sécurité et la protection des données, ou encore l'élaboration de politiques de gouvernance et de gestion de la sécurité informatique.

22. Les cadres, normes, certifications, codes de conduite, etc., existants et reconnus dans différents domaines, peuvent jouer un rôle dans l'indication de l'«état des connaissances» actuel dans le domaine d'utilisation concerné. Lorsque de telles normes existent et garantissent un niveau élevé de protection de la personne concernée, qui respecte ou va même au-delà des exigences légales, les responsables du traitement devraient tenir compte de ces normes lors de la conception et de la mise en œuvre des mesures de protection des données.

#### *2.1.3.2 «Coûts de mise en œuvre»*

23. Le responsable du traitement peut tenir compte des coûts de mise en œuvre lorsqu'il choisit et applique les mesures techniques et organisationnelles appropriées et les garanties nécessaires concrétisant les principes de façon effective afin de protéger les droits des personnes concernées. Les coûts font référence aux ressources en général, y compris le temps et les ressources humaines.

24. L'élément coût n'oblige pas le responsable du traitement à dépenser une quantité disproportionnée de ressources lorsqu'il existe d'autres mesures moins exigeantes en ressources, mais tout aussi efficaces. Les coûts de mise en œuvre constituent cependant un facteur à prendre en compte pour mettre en œuvre la protection des données dès la conception, et non un motif pour ne pas mettre en œuvre une telle protection.

25. En effet, indépendamment des coûts, les mesures choisies doivent garantir que l'activité de traitement prévue par le responsable du traitement n'englobe pas des données à caractère personnel en violation des principes. Les responsables du traitement devraient être en mesure de gérer les coûts globaux afin de mettre en œuvre tous les principes de façon effective et, par conséquent, de protéger les droits.

#### *2.1.3.3 «Nature, portée, contexte et finalités du traitement»*

26. Les responsables du traitement doivent prendre en considération la nature, la portée, le contexte et la finalité du traitement lorsqu'ils déterminent les mesures nécessaires.

27. Ces facteurs devraient être interprétés en cohérence avec leur rôle dans d'autres dispositions du RGPD, telles que les articles 24, 32 et 35, de manière à intégrer les principes de protection des données dans le traitement.

28. En bref, la notion de **nature** peut s'entendre comme les caractéristiques intrinsèques[11] du traitement. La **portée** fait référence à l'ampleur et à l'étendue du traitement. Le **contexte** a trait aux circonstances du traitement susceptibles d'influencer les attentes de la personne concernée, tandis que les **finalités** concernent les objectifs du traitement.

#### *2.1.3.4 «Risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques»*

29. Le RGPD adopte, dans nombre de ses dispositions (articles 24, 25, 32 et 35), une approche cohérente fondée sur les risques, visant à définir les mesures techniques et organisationnelles appropriées pour

[11] Des exemples en sont des catégories spéciales de données à caractère personnel, la prise de décision automatisée, des relations de pouvoir biaisées, le traitement imprévisible, des difficultés pour les personnes concernées d'exercer les droits, etc.

protéger les personnes et les données à caractère personnel les concernant et pour respecter les exigences prévues par le RGPD. Il s'agit toujours de protéger les mêmes ressources (les personnes, par la protection des données à caractère personnel les concernant), contre les mêmes risques (ceux qui pèsent sur les droits des personnes), en tenant compte des mêmes conditions (la nature, la portée, le contexte et les finalités du traitement).

30. Lorsqu'il effectue l'analyse de risque en conformité avec l'article 25, le responsable du traitement doit identifier les risques que présente une violation des principes pour les droits des personnes concernées, et doit déterminer la probabilité et la gravité de ces risques dans le but de mettre en œuvre des mesures atténuant de façon effective les risques recensés. Lors de l'analyse des risques, il est essentiel de procéder à une évaluation systématique et approfondie du traitement. Par exemple, lorsqu'il n'existe pas d'autre fondement juridique, un responsable du traitement évalue les risques particuliers liés à l'absence de consentement libre, qui constitue une violation du principe de licéité, au cours du traitement des données à caractère personnel d'enfants et de jeunes de moins de 18 ans en tant que groupe vulnérable, et il met en œuvre les mesures appropriées pour faire face aux risques identifiés en lien avec ce groupe de personnes concernées et les atténuer de façon effective.

31. Les «lignes directrices du comité européen de la protection des données concernant l'analyse d'impact relative à la protection des données (AIPD)»[12], qui mettent l'accent sur la manière de déterminer si l'opération de traitement est susceptible d'engendrer un risque élevé, fournissent également des orientations sur la façon d'évaluer les risques liés à la protection des données et de réaliser une analyse de risques relative à la protection des données. Ces lignes directrices peuvent également être utiles lors de l'évaluation des risques telle que prévue dans tous les articles susmentionnés, y compris l'article 25.

32. L'approche fondée sur les risques n'exclut pas le recours aux scénarios de référence, aux bonnes pratiques et aux normes. Ceux-ci pourraient constituer une boîte à outils utile permettant aux responsables du traitement de traiter des risques similaires dans des situations identiques (nature, portée, contexte et finalités du traitement). Toutefois, l'obligation prévue à l'article 25 [ainsi qu'aux articles 24 et 32 et à l'article 35, paragraphe 7, point c), du RGPD] de prendre en considération les «*risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques*» demeure. Par conséquent, les responsables du traitement, même s'ils peuvent s'aider de ces outils, doivent toujours effectuer une évaluation des risques liés à la protection des données, au cas par cas, pour le traitement en question, et vérifier l'effectivité des mesures appropriées et des garanties proposées. Une analyse d'impact relative à la protection des données (AIPD), ou une mise à jour d'une AIPD existante, peut alors être exigée à titre supplémentaire.

### 2.1.4 Aspect temporel

#### *2.1.4.1 Au moment de la détermination des moyens du traitement*

33. La protection des données dès la conception doit être mise en œuvre «*au moment de la détermination des moyens du traitement*».

[12] Groupe de travail «Article 29», Lignes directrices 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. WP 248 rev.01 du 4 octobre 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 - adoptées par le comité.

34. Les «*moyens du traitement*» couvrent tant les éléments généraux que les éléments concrets détaillés de la conception du traitement, notamment l'architecture, les procédures, les protocoles, la présentation et l'apparence.

35. Le «*moment de la détermination des moyens du traitement*» désigne la période pendant laquelle le responsable du traitement décide des modalités de réalisation du traitement et de la manière dont celui-ci aura lieu, ainsi que des mécanismes qui seront utilisés pour effectuer un tel traitement. C'est lorsqu'il prend ces décisions que le responsable du traitement doit évaluer les mesures et garanties appropriées pour mettre en œuvre de façon effective les principes et les droits des personnes concernées lors du traitement et prendre en considération les éléments tels que l'«état des connaissances», les coûts de mise en œuvre, la nature, la portée, le contexte, les finalités et les risques. Cette période comprend le moment d'acquisition et de mise en œuvre des logiciels, du matériel et des services de traitement de données.

36. La prise en compte en amont de la protection des données dès la conception et de la protection des données par défaut est fondamentale pour une bonne mise en œuvre des principes et de la protection des droits des personnes concernées. En outre, du point de vue du rapport coût-bénéfices, les responsables du traitement ont intérêt à prendre en considération la protection des données dès la conception et la protection des données par défaut le plus tôt possible, étant donné qu'il pourrait se révéler difficile et coûteux de modifier ultérieurement des plans qui ont déjà été établis et des opérations de traitement qui ont déjà été conçues.

#### *2.1.4.2 Au moment du traitement lui-même (maintien et examen des exigences en matière de protection des données)*

37. Une fois que le traitement a commencé, le responsable du traitement est tenu de maintenir en permanence la protection des données dès la conception et la protection des données par défaut, c'est-à-dire d'assurer en permanence la mise en œuvre effective des principes afin de protéger les droits, de se tenir informé de l'état des connaissances, de réévaluer le niveau de risque, etc. La nature, la portée et le contexte des opérations de traitement, de même que le risque, peuvent évoluer au cours du traitement, de telle sorte que le responsable du traitement doit réévaluer ses opérations de traitement en procédant à des examens et des évaluations périodiques de l'efficacité des mesures et des garanties choisies.

38. L'obligation de maintenir, d'examiner et de mettre à jour, selon les nécessités, l'opération de traitement s'applique également aux systèmes préexistants. Cela signifie que les systèmes antérieurs, conçus avant l'entrée en vigueur du RGPD, doivent faire l'objet d'examens et d'une maintenance pour garantir la mise en œuvre de mesures et de garanties concrétisant les principes et les droits des personnes concernées de façon effective, comme prévu dans les présentes lignes directrices.

39. Cette obligation s'étend également à tout traitement effectué par l'intermédiaire de sous-traitants. Les opérations des sous-traitants devraient faire l'objet d'une évaluation et d'un examen périodiques de la part des responsables du traitement, afin de s'assurer qu'elles garantissent le respect permanent des principes et de permettre au responsable du traitement de remplir ses obligations en la matière.

## 2.2 Article 25, paragraphe 2: Protection des données par défaut

### 2.2.1 Par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

40. Dans sa définition courante en informatique, le terme «par défaut» fait référence à la valeur préexistante ou présélectionnée d'un paramètre configurable qui est attribuée à une application logicielle, un programme informatique ou un dispositif informatique. Ces paramètres sont également appelés «préréglages» ou «réglages d'usine», en particulier pour les appareils électroniques.

41. Dès lors, le terme «par défaut», dans le cadre du traitement de données à caractère personnel, désigne le fait de faire des choix concernant les valeurs de configuration ou les options de traitement définies ou prescrites dans un système de traitement, tel qu'une application logicielle, un service ou un dispositif, ou une procédure de traitement manuel, qui affectent la quantité de données à caractère personnel collectées, l'étendue de leur traitement, la durée de leur conservation ainsi que leur accessibilité.

42. Le responsable du traitement devrait choisir et répondre de la mise en œuvre des paramètres et des options de traitement par défaut, de manière à ce que seul le traitement qui est strictement nécessaire pour atteindre la finalité licite prévue soit effectué par défaut. Dans ce contexte, les responsables du traitement doivent s'appuyer sur leur évaluation de la nécessité du traitement au regard des fondements juridiques visés à l'article 6, paragraphe 1. Il s'ensuit que, par défaut, le responsable du traitement ne doit ni collecter plus de données que nécessaire, ni traiter les données collectées plus qu'il n'est nécessaire pour atteindre ses finalités, ni conserver les données plus longtemps que nécessaire. L'exigence fondamentale est que la protection des données soit intégrée par défaut dans le traitement.

43. Le responsable du traitement doit définir à l'avance pour quelles finalités déterminées, explicites et légitimes les données à caractère personnel sont collectées et traitées[13]. Par défaut, les mesures doivent être appropriées pour garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient traitées. Les «lignes directrices du Contrôleur européen de la protection des données (le CEPD) concernant l'évaluation de la nécessité et de la proportionnalité des mesures qui limitent le droit à la protection des données à caractère personnel» peuvent également se révéler utiles pour décider quelles données il est nécessaire de traiter pour atteindre une finalité spécifique[14] [15] [16].

[13] Article 5, paragraphe 1, points b), c), d) et e), du RGPD.
[14] CEPD. «Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection». 25 février 2019 edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.
[15] Voir également CEPD. «Évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel» https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_fr
[16] Pour plus d'informations sur la nécessité, voir Groupe de travail «Article 29». «Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE». WT 217 du 9 avril 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf.

44. Si le responsable du traitement utilise un logiciel tiers ou un logiciel du commerce, il doit procéder à une évaluation des risques du produit et s'assurer que les fonctions qui n'ont pas de base juridique ou qui ne sont pas compatibles avec les finalités prévues du traitement sont désactivées.

45. Les mêmes considérations valent aussi pour les mesures organisationnelles à l'appui du traitement. Elles doivent être conçues pour ne traiter, dès le début, que la quantité minimale de données à caractère personnel nécessaires aux opérations spécifiques. Ce point devrait tout particulièrement être pris en considération lors de l'attribution de l'accès aux données aux membres du personnel ayant des rôles différents et des besoins d'accès différents.

46. Les «mesures techniques et organisationnelles» appropriées dans le contexte de la protection des données par défaut recouvrent donc la même notion que celle qui a été exposée ci-dessus au sous-chapitre 2.1.1, mais appliquée spécifiquement à la mise en œuvre du principe de minimisation des données.

47. L'obligation susmentionnée de ne traiter que les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique s'applique aux éléments ci-après.

### 2.2.2 Portée de l'obligation de minimisation des données

48. L'article 25, paragraphe 2, définit la portée de l'obligation de minimisation des données pour le traitement par défaut, en indiquant que cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation ainsi qu'à leur accessibilité.

#### *2.2.2.1 «La quantité de données à caractère personnel collectées»*

49. Les responsables du traitement doivent tenir compte du volume de données à caractère personnel, ainsi que des types, des catégories et du niveau de détail des données à caractère personnel requises au regard des finalités du traitement. Dans leurs choix de conception, les responsables du traitement devraient tenir compte des risques accrus que la collecte de quantités importantes de données à caractère personnel détaillées fait peser sur les principes d'intégrité et de confidentialité, de minimisation des données et de limitation de la conservation, et devraient comparer ces risques à la réduction des risques qu'entraîne la collecte d'informations moins détaillées et/ou en moins grande quantité au sujet des personnes concernées. En tout état de cause, le paramètre par défaut ne doit pas inclure la collecte de données à caractère personnel qui ne sont pas nécessaires au regard de la finalité spécifique du traitement. En d'autres termes, si certaines catégories de données à caractère personnel ne sont pas nécessaires ou si des données détaillées ne sont pas requises car des données d'une granularité moins fine sont suffisantes, toute donnée à caractère personnel excédentaire ne doit pas être collectée.

50. Les mêmes exigences par défaut s'appliquent aux services, indépendamment de la plateforme ou du dispositif utilisé, et seules les données à caractère personnel nécessaires à la finalité indiquée peuvent être collectées.

#### 2.2.2.2 «L'étendue de leur traitement»

51. Les opérations de traitement[17] réalisées sur les données à caractère personnel doivent se limiter à ce qui est nécessaire. De nombreuses opérations de traitement peuvent contribuer à la réalisation d'une finalité de traitement. Toutefois, le fait que certaines données à caractère personnel sont nécessaires au regard d'une finalité ne signifie pas que ces données puissent faire l'objet de tous les types d'opérations de traitement et être traitées à n'importe quelle fréquence. Les responsables du traitement devraient également veiller à ne pas étendre les limites des «finalités compatibles» visées à l'article 6, paragraphe 4, et à garder à l'esprit le type de traitement auquel les personnes concernées peuvent raisonnablement s'attendre.

#### 2.2.2.3 «Leur durée de conservation»

52. Les données à caractère personnel collectées ne sont pas conservées si elles ne sont pas nécessaires à la finalité du traitement, et s'il n'existe pas d'autre finalité compatible ou fondement juridique conformément à l'article 6, paragraphe 4. Toute conservation de données devrait être objectivement justifiable, le cas échéant, par le responsable du traitement, en conformité avec le principe de responsabilité.

53. Le responsable du traitement limite la période de conservation à la durée nécessaire à la finalité. Si les données à caractère personnel ne sont plus nécessaires aux fins du traitement, elles devront, par défaut, être supprimées ou anonymisées. La durée de conservation dépendra donc de la finalité du traitement en question. Cette obligation est directement liée au principe de limitation de la conservation énoncé à l'article 5, paragraphe 1, point e), et doit être mise en œuvre par défaut, c'est-à-dire que le responsable du traitement devrait prévoir, dans le cadre du traitement, des procédures systématiques pour supprimer ou anonymiser les données.

54. L'anonymisation[18] des données à caractère personnel est une solution de substitution à la suppression, pour autant que tous les éléments contextuels pertinents soient pris en considération et que la probabilité et la gravité du risque, y compris du risque de réidentification, soient régulièrement évaluées[19].

#### 2.2.2.4 «Leur accessibilité»

55. Le responsable du traitement devrait limiter le nombre de personnes ayant accès et les types d'accès aux données à caractère personnel en fonction d'une évaluation de la nécessité, et devrait également veiller à ce que les données à caractère personnel soient effectivement accessibles aux personnes qui en ont besoin lorsque cela est nécessaire, par exemple dans des situations critiques. Des contrôles de l'accès doivent être respectés pour l'ensemble du flux de données pendant le traitement.

---

[17] Conformément à l'article 4, paragraphe 2, du RGPD, ces opérations sont la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

[18] Groupe de travail «Article 29». «Avis 05/2014 sur les techniques d'anonymisation». WP 216 du 10 avril 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf.

[19] Voir l'article 4, paragraphe 1, du RGPD, le considérant 26 du RGPD et l'«avis 05/2014 sur les techniques d'anonymisation» du groupe de travail «Article 29». Voir également la sous-section relative à la «limitation de la conservation» à la section 3 du présent document, qui mentionne la nécessité, pour le responsable du traitement, de garantir l'effectivité de la mise en œuvre de la ou des techniques d'anonymisation.

56. L'article 25, paragraphe 2, précise en outre que les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. Le responsable du traitement doit, par défaut, limiter l'accès et donner à la personne concernée la possibilité d'intervenir avant de publier ou de mettre à la disposition d'un nombre indéterminé de personnes physiques des données à caractère personnel la concernant.

57. La mise à disposition des données à caractère personnel à un nombre indéterminé de personnes peut entraîner une diffusion des données encore plus importante que celle envisagée initialement. Cela est particulièrement vrai dans le contexte de l'Internet et des moteurs de recherche. En conséquence, les responsables du traitement devraient, par défaut, donner aux personnes concernées la possibilité d'intervenir avant que des données à caractère personnel les concernant ne soient mises à disposition sur l'Internet ouvert. Cela est particulièrement important en ce qui concerne les enfants et les groupes vulnérables.

58. En fonction des fondements juridiques du traitement, la possibilité d'intervenir pourrait varier selon le contexte du traitement. Par exemple, demander le consentement pour rendre les données à caractère personnel accessibles au public, ou disposer de paramètres de confidentialité permettant aux personnes concernées de contrôler elles-mêmes l'accès public.

59. Même dans le cas où les données à caractère personnel sont rendues publiques avec l'autorisation éclairée d'une personne concernée, cela ne signifie pas que tout autre responsable du traitement ayant accès aux données à caractère personnel puisse les traiter librement lui-même, pour ses propres finalités; il doit disposer à cet effet d'une base juridique distincte[20].

# 3 MISE EN ŒUVRE DES PRINCIPES RELATIFS A LA PROTECTION DES DONNEES DANS LE CADRE DU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL EN RECOURANT A LA PROTECTION DES DONNEES DES LA CONCEPTION ET A LA PROTECTION DES DONNEES PAR DEFAUT

60. À tous les stades de la conception des activités de traitement, y compris la passation de marchés, les appels d'offres, l'externalisation, le développement, l'assistance, la maintenance, les essais, le stockage, la suppression, etc., le responsable du traitement devrait prendre en considération et envisager les différents éléments de la protection des données dès la conception et de la protection des données par défaut, qui sont illustrés par les exemples figurant au présent chapitre, dans le contexte de la mise en œuvre des principes[21] [22] [23].

61. Les responsables du traitement doivent mettre en œuvre les principes pour garantir la protection des données dès la conception et la protection des données par défaut. Ces principes sont les suivants: la

[20] Voir l'affaire Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande, nº 931/13.
[21] Pour d'autres exemples, voir le document de l'autorité norvégienne chargée de la protection des données intitulé «Software development with Data Protection by Design and by Default» (Développement logiciel assorti de la protection des données dès la conception et de la protection des données par défaut). 28 novembre 2017 www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729.
[22] https://www.cnil.fr/en/cnil-publishes-RGPD-guide-developers
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

transparence, la licéité, la loyauté, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation, l'intégrité et la confidentialité, ainsi que la responsabilité. Ces principes sont énoncés à l'article 5 et au considérant 39 du RGPD. Pour bien comprendre comment mettre en œuvre la protection des données dès la conception et la protection des données par défaut, il est important de connaître la signification de chacun de ces principes.

62. Lors de la présentation des exemples de mise en œuvre de la protection des données dès la conception et de la protection des données par défaut, nous avons établi, pour chaque principe, une liste d'**éléments clés pour la protection des données dès la conception et la protection des données par défaut**. Les exemples, qui illustrent spécifiquement le principe relatif à la protection des données en question, peuvent également recouper d'autres principes étroitement liés. Le comité européen de la protection des données met l'accent sur le fait que les éléments clés et les exemples présentés ci-dessous ne sont ni exhaustifs, ni contraignants, mais sont destinés à servir d'éléments d'orientation pour chacun des principes. Les responsables du traitement doivent déterminer comment garantir le respect des principes dans le contexte du traitement particulier concerné.

63. Bien que la présente section porte sur la mise en œuvre des principes, le responsable du traitement devrait également mettre en œuvre des moyens *appropriés* et *effectifs* pour protéger les droits des personnes concernées, conformément au chapitre III du RGPD, lorsque cela n'est pas déjà prévu par les principes eux-mêmes.

64. Le principe de responsabilité est primordial: il exige du responsable du traitement qu'il fasse preuve de responsabilité dans le choix des mesures techniques et organisationnelles nécessaires.

## 3.1 Transparence[24]

65. Le responsable du traitement doit faire preuve de clarté et d'ouverture à l'égard de la personne concernée et lui expliquer comment il entend collecter, utiliser et partager les données à caractère personnel la concernant. La transparence vise à permettre aux personnes concernées de comprendre leurs droits établis aux articles 15 à 22 et, si nécessaire, d'en faire usage. Le principe est intégré dans les articles 12, 13, 14 et 34. Les mesures et garanties mises en place à l'appui du principe de transparence devraient également étayer la mise en œuvre de ces articles.

66. En ce qui concerne le principe de transparence, on peut citer parmi les éléments clés de protection des données dès la conception et par défaut:

- Clarté - Les informations doivent être formulées en des termes clairs et simples, concis et compréhensibles.
- Sémantique - La communication doit avoir une signification claire pour le public concerné.
- Accessibilité - Les informations doivent être aisément accessibles pour la personne concernée.
- Contextualité - Les informations doivent être fournies au moment opportun et sous la forme appropriée.
- Pertinence - Les informations doivent être pertinentes et applicables à la personne concernée spécifique.

[24] Des explications sur la manière de comprendre la notion de transparence figurent dans le document du groupe de travail «Article 29» intitulé «Lignes directrices sur la transparence au sens du règlement (UE) 2016/679» WP 260 rev.01 du 11 avril 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 - adopté par le comité.

- Conception universelle – Les informations doivent être accessibles à toutes les personnes concernées et inclure l'utilisation de langages lisibles par machine pour faciliter et automatiser la lisibilité et la clarté.
- Compréhensibilité - Les personnes concernées doivent avoir une juste compréhension de ce qu'elles peuvent attendre en ce qui concerne le traitement de leurs données à caractère personnel, en particulier lorsqu'il s'agit d'enfants ou d'autres groupes vulnérables.
- Canaux multiples - Les informations devraient être fournies par différents canaux et médias, au-delà du texte, afin d'accroître la probabilité que les informations parviennent effectivement à la personne concernée.
- Structuration par couches – Les informations devraient être structurées par couches de manière à résoudre la tension entre l'exhaustivité et la compréhension, tout en tenant compte des attentes raisonnables des personnes concernées.

Exemple[25]

Un responsable du traitement élabore une politique de protection de la vie privée sur son site web pour respecter les exigences en matière de transparence. La politique de protection de la vie privée ne devrait pas contenir une grande quantité d'informations difficiles à comprendre et à assimiler pour la personne concernée moyenne. Elle devrait être rédigée dans un langage clair et concis et permettre à l'utilisateur du site web de comprendre facilement comment les données à caractère personnel le concernant sont traitées. Le responsable du traitement fournit donc des informations à plusieurs niveaux, où les points essentiels sont mis en évidence. Des informations plus détaillées sont facilement accessibles. Des menus déroulants et des liens vers d'autres pages sont fournis pour des explications plus détaillées des différents éléments et notions figurant dans la politique. Le responsable du traitement veille également à ce que les informations soient transmises par des canaux multiples, en fournissant des vidéogrammes pour expliquer les principaux points de l'information écrite. La synergie entre les différentes pages est essentielle pour faire en sorte que l'approche par couches n'accentue pas la confusion, mais au contraire la réduise.

La politique de protection de la vie privée ne devrait pas être difficile d'accès pour les personnes concernées. Elle est donc mise à disposition et visible sur toutes les pages web internes du site en question, pour que la personne concernée puisse accéder en un seul clic à l'information. Les informations fournies sont également conçues conformément aux bonnes pratiques et aux normes en matière de conception universelle afin qu'elles soient accessibles à tous.

En outre, les informations nécessaires doivent également être fournies dans le contexte approprié, au moment opportun. Étant donné que le responsable du traitement effectue de nombreux traitements à l'aide des données collectées sur le site web, une politique générale de protection de la vie privée sur le site web ne suffit pas, à elle seule, pour que le responsable du traitement réponde aux exigences de transparence. Celui-ci conçoit donc un flux d'informations, en présentant des informations pertinentes à la personne concernée dans les contextes appropriés, par exemple au moyen d'extraits d'information ou de fenêtres contextuelles. Par exemple, lorsqu'il demande à la personne concernée d'introduire des données à caractère personnel, le responsable du traitement informe cette dernière de la manière dont ces données seront traitées et des raisons pour lesquelles elles sont nécessaires au traitement.

[25] L'autorité française de protection des données a publié plusieurs exemples illustrant les meilleures pratiques en matière d'information des utilisateurs, ainsi que d'autres principes concernant la transparence: https://design.cnil.fr/

## 3.2 Licéité

67. Le responsable du traitement doit définir une base juridique valable pour le traitement des données à caractère personnel. Les mesures et garanties devraient soutenir l'obligation de veiller à ce que l'ensemble du cycle de vie du traitement soit conforme aux fondements juridiques pertinents du traitement.

68. En ce qui concerne la licéité, on peut citer parmi les éléments clés pour la protection dès la conception et la protection par défaut:

- Pertinence - Le traitement doit reposer sur la base juridique appropriée.
- Différenciation[26] – La base juridique utilisée pour chaque activité de traitement doit être différenciée.
- Finalité déterminée - La base juridique appropriée doit être clairement liée à la finalité spécifique du traitement[27].
- Nécessité – Le traitement doit être nécessaire et inconditionnel pour que la finalité soit licite.
- Autonomie – La personne concernée devrait jouir du plus haut degré d'autonomie possible en ce qui concerne le contrôle de ses données à caractère personnel dans le cadre du fondement juridique.
- Obtention du consentement – Le consentement doit être manifesté de façon libre et doit être spécifique, éclairé et univoque[28]. Il convient d'accorder une attention particulière à la capacité des enfants et des jeunes à donner un consentement éclairé.
- Retrait du consentement – Lorsque le consentement constitue la base juridique, le traitement devrait faciliter le retrait du consentement. Il doit être aussi simple de retirer que de donner son consentement. Dans le cas contraire, le mécanisme de consentement du responsable du traitement n'est pas conforme au RGPD[29].
- Mise en balance des intérêts – Lorsque des intérêts légitimes constituent la base juridique, le responsable du traitement doit procéder à une mise en balance pondérée des intérêts, en accordant une attention particulière au déséquilibre de pouvoir, notamment pour les enfants de moins de 18 ans et les autres groupes vulnérables. Des mesures et des garanties sont prévues pour atténuer l'impact négatif sur les personnes concernées.
- Prédétermination - La base juridique doit être établie avant que le traitement ne soit effectué.
- Cessation - Si la base juridique cesse d'être applicable, le traitement doit prendre fin en conséquence.
- Ajustement - Si un changement valable de la base juridique du traitement intervient, le traitement doit être adapté en fonction de la nouvelle base juridique[30].
- Répartition des responsabilités – Si une coresponsabilité du traitement est envisagée, les parties doivent répartir de manière claire et transparente leurs responsabilités respectives à

[26] Comité. «Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées» Version 2.0 du 8 octobre 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

[27] Voir la section relative à la limitation des finalités ci-dessous.

[28] Voir les lignes directrices 05/2020 sur le consentement en vertu du règlement 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Voir les lignes directrices 05/2020 sur le consentement en vertu du règlement 2016/679, p. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] Si la base juridique initiale est le consentement, voir les lignes directrices 05/2000 sur le consentement au titre du règlement 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

l'égard de la personne concernée et doivent concevoir les mesures du traitement conformément à cette répartition.

Exemple

Une banque envisage de proposer un service pour améliorer l'efficacité de la gestion des demandes de prêts. L'idée qui sous-tend le service est que la banque, en demandant l'autorisation du client, puisse récupérer des données concernant le client directement auprès des autorités fiscales publiques. Cet exemple ne tient pas compte du traitement de données à caractère personnel provenant d'autres sources.

L'obtention de données personnelles concernant la situation financière de la personne concernée est nécessaire pour prendre les mesures demandées par la personne concernée avant la conclusion d'un contrat de prêt[31]. La collecte de données personnelles directement auprès de l'administration fiscale n'est toutefois pas jugée nécessaire. En effet, le client est en mesure de conclure un contrat en fournissant lui-même les informations provenant de l'administration fiscale. Bien que la banque puisse avoir un intérêt légitime à obtenir la documentation directement auprès des autorités fiscales, par exemple pour garantir l'efficacité du traitement du prêt, le fait d'accorder aux banques un tel accès direct aux données personnelles des demandeurs présente un risque lié à l'utilisation ou à l'abus potentiel des droits d'accès.

Lorsqu'il met en œuvre le principe de licéité, le responsable du traitement constate que, dans ce contexte, il ne peut pas utiliser la base «nécessaire à l'exécution d'un contrat» pour la partie du traitement qui implique la collecte de données à caractère personnel directement auprès des autorités fiscales. Le fait que ce traitement spécifique présente le risque que la personne concernée soit moins impliquée dans le traitement de ses données est également un facteur pertinent pour apprécier la licéité du traitement lui-même. La banque conclut que cette partie du traitement doit s'appuyer sur une autre base juridique. Dans l'État membre concerné où se trouve le responsable du traitement, il existe des lois nationales qui permettent à la banque de collecter des informations directement auprès des autorités fiscales publiques, à condition que la personne concernée donne son consentement préalable.

La banque présente donc les informations relatives au traitement sur la plateforme de demande en ligne de telle sorte qu'il soit facile pour les personnes concernées de comprendre quelle partie du traitement est obligatoire et quelle partie est facultative. Par défaut, les options de traitement ne permettent pas la récupération de données directement à partir d'autres sources que la personne concernée elle-même, et l'option concernant la récupération directe d'informations est présentée d'une manière qui ne dissuade pas la personne concernée de s'abstenir. Tout consentement donné en vue de la collecte directe d'informations auprès d'autres responsables du traitement est un droit d'accès temporaire à un ensemble déterminé d'informations.

Tout consentement donné est traité électroniquement, de manière vérifiable, et les personnes concernées disposent d'un moyen facile de contrôler ce qu'elles ont accepté et de retirer leur consentement.

Le responsable du traitement a préalablement évalué ces exigences en matière de protection des données dès la conception et de protection des données par défaut et inclut tous ces critères dans ses spécifications relatives à l'appel d'offres portant sur la fourniture de la plateforme. Le responsable du

[31] Voir l'article 6, paragraphe 1, point b), du RGPD.

traitement est conscient que, s'il n'inclut pas ces exigences dans l'appel d'offres, il pourrait ensuite être trop tard pour mettre en œuvre la protection des données ou cela pourrait se révéler très coûteux.

## 3.3 Loyauté

69. La loyauté est un principe fondamental selon lequel les données à caractère personnel ne doivent pas être traitées d'une manière injustifiablement préjudiciable ou illégalement discriminatoire, inattendue ou trompeuse pour la personne concernée. Les mesures et garanties mettant en œuvre le principe de loyauté étayent également les droits et libertés des personnes concernées, en particulier le droit à l'information (transparence), le droit d'intervention (accès, effacement, portabilité des données, rectification) et le droit de limiter le traitement (droit de ne pas faire l'objet d'un processus de prise de décision individuelle automatisée et non-discrimination des personnes concernées dans le cadre de ces processus).

70. En ce qui concerne la loyauté, on peut citer parmi les éléments clés pour la protection dès la conception et par défaut:
    - Autonomie – Les personnes concernées devraient se voir accorder le plus degré d'autonomie le plus élevé possible pour déterminer l'utilisation qui est faite des données à caractère personnel les concernant, ainsi que la portée et les conditions de cette utilisation ou de ce traitement.
    - Interaction – Les personnes concernées doivent être en mesure de communiquer et d'exercer leurs droits auprès du responsable du traitement en ce qui concerne les données à caractère personnel traitées par ce dernier.
    - Attentes – Le traitement devrait correspondre aux attentes raisonnables des personnes concernées.
    - Non-discrimination – Le responsable du traitement ne doit pas discriminer injustement les personnes concernées.
    - Non-exploitation - Le responsable du traitement ne doit pas exploiter les besoins ou les vulnérabilités des personnes concernées.
    - Choix du consommateur – Le responsable du traitement ne devrait pas «engager» ses utilisateurs d'une manière déloyale. Lorsqu'un service traitant des données à caractère personnel est exclusif, il peut créer un engagement à l'égard du service qui peut ne pas être loyal s'il entrave la possibilité pour les personnes concernées d'exercer leur droit de portabilité des données visé à l'article 20.
    - Équilibre de pouvoir – L'équilibre de pouvoir devrait être un objectif central de la relation entre le responsable du traitement et la personne concernée. Les déséquilibres de pouvoir devraient être évités. Lorsque cela n'est pas possible, ces déséquilibres devraient être reconnus et pris en compte dans le cadre de contre-mesures appropriées.
    - Absence de transfert des risques – Les responsables du traitement ne devraient pas transférer les risques de l'entreprise aux personnes concernées.
    - Absence de tromperie – Les informations et les options relatives au traitement des données devraient être fournies d'une manière objective et neutre, en évitant tout langage ou toute conception trompeurs ou manipulateurs.
    - Respect des droits – Le responsable du traitement doit respecter les droits fondamentaux des personnes concernées, mettre en œuvre les mesures et garanties appropriées et ne pas empiéter sur ces droits, sauf si la loi le justifie expressément.
    - Éthique - Le responsable du traitement devrait envisager l'incidence au sens large du traitement sur les droits et la dignité des personnes.

- Véracité – Le responsable du traitement doit mettre à disposition des informations sur la manière dont il traite les données à caractère personnel, et il doit agir conformément à ses engagements et ne pas induire les personnes concernées en erreur.
- Intervention humaine - Le responsable du traitement doit prévoir une intervention humaine *qualifiée* capable de remédier aux biais que les machines peuvent créer en ce qui concerne le droit de ne pas faire l'objet d'une prise de décision individuelle automatisée prévue à l'article 22[32].
- Algorithmes loyaux – Vérifier régulièrement si les algorithmes fonctionnent conformément aux finalités et adapter les algorithmes pour atténuer les biais constatés et garantir la loyauté du traitement. Des informations devraient être fournies aux personnes concernées au sujet du fonctionnement du traitement des données à caractère personnel par des algorithmes qui les analysent ou formulent des prévisions à leur égard, par exemple en ce qui concerne le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences personnelles, sa fiabilité ou son comportement, sa localisation ou ses déplacements[33].

Exemple 1

Un responsable du traitement exploite un moteur de recherche qui traite principalement des données à caractère personnel générées par les utilisateurs. Le fait de disposer de grandes quantités de données à caractère personnel et d'être en mesure d'utiliser ces données pour des publicités ciblées constitue un avantage pour le responsable du traitement. Celui-ci souhaite par conséquent amener les personnes concernées à autoriser une collecte et une utilisation plus larges de leurs données à caractère personnel. Le consentement doit être recueilli en présentant les possibilités de traitement à la personne concernée.

Lorsqu'il met en œuvre le principe de loyauté, en tenant compte de la nature, de la portée, du contexte et de la finalité du traitement, le responsable du traitement a conscience qu'il ne peut pas présenter les options d'une manière qui pousserait la personne concernée à l'autoriser à collecter davantage de données à caractère personnel que si les options étaient présentées de manière neutre et égale. Cela signifie qu'il ne peut pas présenter les options de traitement d'une façon qui rende difficile pour les personnes concernées le fait de s'abstenir de partager leurs données, ni rendre difficile pour ces personnes l'adaptation de leurs paramètres de confidentialité et la limitation du traitement. Il s'agit d'exemples d'interfaces truquées, qui sont contraires à l'esprit de l'article 25. Les options de traitement par défaut ne devraient pas être invasives, et le choix concernant un traitement ultérieur devrait être présenté d'une manière qui ne pousse pas la personne concernée à donner son consentement. Par conséquent, le responsable du traitement présente les options de consentement ou d'abstention comme deux choix tout aussi visibles l'un que l'autre, en représentant avec précision les ramifications de chaque choix pour la personne concernée.

[32] Voir les lignes directrices sur la prise de décision et le profilage automatisés au titre du règlement 2016/679. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] Voir le considérant 71 du RGPD.

Exemple 2

Un autre responsable du traitement traite des données à caractère personnel pour la fourniture d'un service de diffusion en continu pour lequel les utilisateurs peuvent choisir entre un abonnement classique de qualité standard et un abonnement premium de plus haute qualité. Dans le cadre de l'abonnement premium, les abonnés bénéficient d'un service à la clientèle prioritaire.

En ce qui concerne le principe de loyauté, le service à la clientèle prioritaire offert aux abonnés premium ne peut pas établir de discrimination concernant l'accès des abonnés normaux à l'exercice de leurs droits conformément à l'article 12 du RGPD. En d'autres termes, même si les abonnés premium bénéficient d'un service prioritaire, ce traitement prioritaire ne peut pas se traduire par l'absence de mesures appropriées destinées à répondre aux demandes des abonnés classiques dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception des demandes.

Certes, les abonnés premium paient pour obtenir un service amélioré, mais toutes les personnes concernées doivent bénéficier d'un accès égal et indiscriminé aux moyens leur permettant de faire valoir leurs droits et libertés comme l'exige l'article 12.

## 3.4 Limitation des finalités[34]

71. Le responsable du traitement doit collecter les données pour des finalités déterminées, explicites et légitimes, et ne pas les traiter ultérieurement d'une manière incompatible avec les finalités pour lesquelles elles ont été collectées[35]. La conception du traitement doit donc être définie par ce qui est nécessaire au regard des finalités. En cas de traitement ultérieur, le responsable du traitement doit d'abord veiller à ce que les finalités de ce traitement ultérieur soient compatibles avec les finalités originales et concevoir celui-ci en conséquence. La compatibilité ou non d'une nouvelle finalité doit être appréciée au regard des critères énoncés à l'article 6, paragraphe 4.

72. En ce qui concerne la limitation des finalités, on peut citer parmi les éléments clés pour la protection dès la conception et par défaut:

- Prédétermination - Les finalités légitimes doivent être déterminées avant la conception du traitement.
- Spécificité – Les finalités doivent être précisées et doivent expliquer clairement la raison pour laquelle les données à caractère personnel sont traitées.
- Orientation en fonction des finalités - La finalité du traitement devrait guider la conception du traitement et fixer les limites de ce dernier.
- Nécessité - La finalité détermine quelles données à caractère personnel sont nécessaires au traitement.
- Compatibilité - Toute nouvelle finalité doit être compatible avec la finalité initiale pour laquelle les données ont été collectées et guider les changements dans la conception.

[34] Le groupe de travail «Article 29» a fourni des orientations sur l'interprétation du principe de limitation des finalités dans le cadre de la directive 95/46/CE. Bien que cet avis n'ait pas été adopté par le comité, il peut néanmoins conserver sa pertinence, étant donné que le principe est libellé de la même manière dans le RGPD. Groupe de travail «Article 29». «Opinion 03/2013 on purpose limitation». WP 203 du 2 avril 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[35] Article 5, paragraphe 1, point b), du RGPD.

- Limitation du traitement ultérieur - Le responsable du traitement ne devrait pas établir de liens entre les ensembles de données ni effectuer de traitement ultérieur pour de nouvelles finalités incompatibles.
- Limitations de la réutilisation – Le responsable du traitement devrait utiliser des mesures techniques, notamment le hachage et le chiffrement, afin de limiter la possibilité d'utiliser les données à caractère personnel pour d'autres finalités. Le responsable du traitement devrait également disposer de mesures organisationnelles, telles que des politiques et des obligations contractuelles, qui limitent la réutilisation des données à caractère personnel.
- Réexamen - Le responsable du traitement doit examiner régulièrement si le traitement est nécessaire au regard des finalités pour lesquelles les données ont été collectées et vérifier si la conception est compatible avec la limitation des finalités.

Exemple

Le responsable du traitement traite des données à caractère personnel concernant ses clients. Ce traitement a pour finalité l'exécution d'un contrat, à savoir pouvoir livrer des biens à la bonne adresse et en obtenir le paiement. Les données à caractère personnel stockées sont l'historique des achats, le nom, l'adresse, l'adresse électronique et le numéro de téléphone.

Le responsable du traitement envisage d'acheter un produit de gestion de la relation client (CRM) qui regroupe en un seul endroit toutes les données relatives au client, telles que les données relatives aux ventes, au marketing et au service à la clientèle. Le produit offre la possibilité de stocker l'ensemble des appels téléphoniques, activités, documents, courriers électroniques et campagnes de marketing pour obtenir une vue à 360 degrés du client. En outre, le système CRM est capable d'analyser automatiquement le pouvoir d'achat des clients en utilisant des informations publiques. Cette analyse a pour objet de mieux cibler les activités publicitaires. Ces activités ne font pas partie de la finalité licite initiale du traitement.

Pour respecter le principe de limitation des finalités, le responsable du traitement demande au fournisseur du produit d'établir la correspondance entre les différentes activités de traitement utilisant des données à caractère personnel et les finalités pertinentes pour le responsable du traitement.

Après avoir reçu les résultats de la mise en correspondance, le responsable du traitement vérifie si la nouvelle finalité commerciale et la finalité publicitaire ciblée sont compatibles avec les finalités initiales, définies lors de la collecte des données, et s'il existe une base juridique suffisante pour le traitement concerné. Si cette évaluation ne débouche pas sur une réponse positive, le responsable du traitement ne procède pas à l'utilisation des fonctionnalités respectives. Le responsable du traitement pourrait également choisir de renoncer à l'évaluation et simplement de ne pas utiliser les fonctionnalités décrites du produit.

## 3.5 Minimisation des données

73. Seules les données à caractère personnel qui sont adéquates, pertinentes et limitées à ce qui est **nécessaire** au regard des finalités peuvent être traitées[36]. En conséquence, le responsable du

[36] Article 5, paragraphe 1, point c), du RGPD.

traitement doit déterminer à l'avance les caractéristiques et paramètres des systèmes de traitement et de leurs fonctions d'appui qui sont admissibles. La minimisation des données étaye et concrétise le principe de nécessité. Lors du traitement ultérieur, le responsable du traitement devrait examiner périodiquement si les données à caractère personnel traitées sont toujours adéquates, pertinentes et nécessaires, ou si elles doivent être supprimées ou anonymisées.

74. Les responsables du traitement doivent tout d'abord déterminer s'il est même nécessaire de traiter des données à caractère personnel au regard des finalités qui sont les leurs. Le responsable du traitement devrait vérifier si les finalités pertinentes peuvent être atteintes en traitant moins de données à caractère personnel, ou en disposant de données à caractère personnel moins détaillées ou moins agrégées, voire sans avoir à traiter de données à caractère personnel du tout[37]. Cette vérification devrait avoir lieu avant tout traitement, mais elle peut également être effectuée à tout moment pendant la durée du traitement. Ce point est également cohérent avec l'article 11.

75. La minimisation peut également concerner le degré d'identification. Si la finalité du traitement n'exige pas que l'ensemble de données final fasse référence à une personne identifiée ou identifiable (comme dans les statistiques), mais que le traitement initial l'exige (par exemple, avant l'agrégation des données), le responsable du traitement doit anonymiser les données à caractère personnel dès que l'identification n'est plus nécessaire, ou, si le maintien de l'identification est requis pour d'autres activités de traitement, les données à caractère personnel devraient être pseudonymisées afin d'atténuer les risques pour les droits des personnes concernées.

76. En ce qui concerne la minimisation des données, on peut citer parmi les éléments clés pour la protection dès la conception et par défaut:
    - Évitement du recours aux données - Éviter tout traitement de données à caractère personnel si la finalité en question le permet.
    - Limitation - Limiter la quantité de données à caractère personnel collectées à ce qui est nécessaire au regard de la finalité.
    - Limitation de l'accès – Concevoir le traitement de données de manière à ce qu'un nombre minimal de personnes aient besoin d'accéder aux données à caractère personnel pour exercer leurs fonctions, et limiter l'accès en conséquence.
    - Pertinence – Les données à caractère personnel devraient être pertinentes au regard du traitement en question, et le responsable du traitement devrait être en mesure de démontrer cette pertinence.
    - Nécessité - Chaque élément de données à caractère personnel doit être nécessaire au regard des finalités spécifiées et ne doit faire l'objet d'un traitement que s'il n'est pas possible de répondre à ces finalités par d'autres moyens.
    - Agrégation - Utiliser des données agrégées lorsque cela est possible.
    - Pseudonymisation - Pseudonymiser les données à caractère personnel dès qu'il n'est plus nécessaire de disposer de données à caractère personnel directement identifiables, et stocker séparément les clés d'identification.
    - Anonymisation et suppression - Lorsque des données à caractère personnel ne sont pas ou plus nécessaires au regard de la finalité, elles doivent être anonymisées ou supprimées.
    - Flux de données – Le flux de données devrait être rendu suffisamment efficace pour ne pas créer plus de copies que nécessaire.

[37] Le considérant 39 du RGPD est libellé comme suit: «...Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens.»

- «État des connaissances» – Le responsable du traitement devrait appliquer des technologies à jour et appropriées aux fins de l'évitement du recours aux données et de la minimisation des données.

Exemple 1

Une librairie souhaite augmenter ses recettes en vendant ses livres en ligne. Le libraire veut mettre au point un formulaire standard pour le processus de commande. Pour veiller à ce que les clients fournissent toutes les informations souhaitées, le libraire rend obligatoires tous les champs du formulaire (si tous les champs ne sont pas remplis, le client ne peut pas passer commande). Il utilise initialement un formulaire de contact standard qui demande des informations telles que la date de naissance, le numéro de téléphone et l'adresse du client. Toutefois, tous les champs du formulaire ne sont pas strictement nécessaires aux fins de l'achat et de la livraison des livres. Dans ce cas particulier, si la personne concernée paie le produit à l'avance, sa date de naissance et son numéro de téléphone ne sont pas nécessaires pour l'achat du produit. Cela signifie que ces champs ne peuvent pas être obligatoires dans le formulaire web de commande du produit, à moins que le responsable du traitement ne puisse clairement démontrer qu'ils sont nécessaires pour d'autres raisons et expliquer pourquoi. En outre, dans certaines situations, une adresse n'est pas non plus nécessaire. Par exemple, lors de la commande d'un livre électronique, le client peut télécharger le produit directement sur son appareil.

Le propriétaire de la boutique en ligne décide par conséquent d'établir deux formulaires: le premier, qui contient un champ pour l'adresse du client, pour les commandes de livres imprimés et le second, sans champ pour l'adresse du client, pour les commandes de livres électroniques.

Exemple 2

Une société de transports publics souhaite collecter des informations statistiques fondées sur les itinéraires des voyageurs. Ces statistiques sont utiles pour permettre à la société d'effectuer des choix adéquats concernant la modification des horaires des transports publics et les itinéraires appropriés des trains. Les passagers doivent passer leur billet dans un lecteur à chaque fois qu'ils montent dans un véhicule ou en descendent. Après avoir procédé à une évaluation des risques que pose la collecte des itinéraires de transport des passagers pour les droits et libertés de ces derniers, le responsable du traitement établit qu'il est possible d'identifier les passagers dans des cas où ils vivent ou travaillent dans des zones peu peuplées, en fonction d'une identification unique de l'itinéraire grâce à l'identifiant du billet. Par conséquent, étant donné que cela n'est pas nécessaire pour optimiser les horaires des transports publics et les itinéraires des trains, le responsable du traitement ne conserve pas l'identifiant du billet. Une fois le voyage terminé, le responsable du traitement ne conserve que les différents itinéraires de transport afin de ne pas être en mesure d'identifier les voyages liés à un billet donné; il ne conserve que les informations sur les itinéraires de transport distincts.

Dans les cas où il peut toujours exister un risque d'identification d'une personne uniquement par son itinéraire de transport public, le responsable du traitement met en œuvre des mesures statistiques pour réduire le risque, par exemple en coupant le début et la fin de l'itinéraire.

Exemple 3

Une entreprise de courrier vise à évaluer l'efficacité de ses livraisons du point de vue des délais de livraison, de la planification de la charge de travail et de la consommation de carburant. Pour atteindre cet objectif, l'entreprise doit traiter un certain nombre de données à caractère personnel relatives à la fois aux salariés (chauffeurs) et aux clients (adresses, objets à livrer, etc.). Ce traitement comporte des risques liés à la fois à la surveillance des salariés, qui exige des garanties juridiques spécifiques, et au suivi des habitudes des clients grâce à la connaissance des produits livrés au fil du temps. Ces risques peuvent être considérablement réduits grâce à une pseudonymisation appropriée des données relatives aux salariés et aux clients. En particulier si les clés de pseudonymisation font l'objet d'une rotation régulière et que des macrozones apparaissent au lieu d'adresses précises, une minimisation effective des données est mise en œuvre, et le responsable du traitement peut se concentrer uniquement sur le processus de livraison et sur l'optimisation des ressources, sans franchir le seuil de la surveillance des comportements des particuliers (clients ou salariés).

Exemple 4

Un hôpital collecte des données sur ses patients dans un système d'information hospitalier (dossier médical électronique). Les personnels hospitaliers ont besoin d'accéder aux dossiers des patients pour éclairer leurs décisions concernant les soins et le traitement des patients, et pour documenter toutes les actions prises en matière de diagnostic, de soins et de traitement. Par défaut, l'accès n'est accordé qu'aux membres du personnel médical qui sont affectés au traitement du patient concerné au sein du service spécialisé dans lequel celui-ci est pris en charge. Le groupe de personnes ayant accès au dossier d'un patient est élargi si d'autres services ou unités de diagnostic interviennent dans le traitement. Après la sortie du patient de l'hôpital et la facturation, l'accès est limité à un petit groupe d'employés par service spécialisé, qui répondent aux demandes d'informations médicales et aux consultations réalisées ou demandées par d'autres prestataires de services médicaux sur autorisation du patient concerné.

### 3.6 Exactitude

77. Les données à caractère personnel doivent être exactes et tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder[38].

78. Les exigences doivent être considérées au regard des risques et des conséquences associés à l'utilisation concrète des données. Des données à caractère personnel inexactes pourraient constituer un risque pour les droits et libertés des personnes concernées, par exemple lorsqu'elles conduisent à un diagnostic erroné ou à un traitement injustifié dans un protocole de santé, ou si l'image incorrecte d'une personne peut donner lieu à des décisions fondées sur une base erronée, que ces décisions soient prises manuellement, par un système de décision automatisé ou par une intelligence artificielle.

79. En ce qui concerne l'exactitude, on peut citer parmi les éléments clés pour la protection dès la conception et par défaut:

[38] Article 5, paragraphe 1, point d), du RGPD.

- Source de données – Les sources de données personnelles devraient être fiables quant à l'exactitude des données.
- Degré d'exactitude - Chaque élément de données à caractère personnel doit être aussi précis que nécessaire aux fins déterminées.
- Précision mesurable – Réduire le nombre de faux positifs/négatifs, par exemple les biais dans les décisions automatisées et l'intelligence artificielle.
- Vérification – Selon la nature des données, en fonction de la fréquence à laquelle elles peuvent changer, le responsable du traitement devrait vérifier l'exactitude des données à caractère personnel avec la personne concernée avant le traitement et à différents stades de celui-ci (par exemple par rapport aux conditions d'âge).
- Effacement/rectification - Le responsable du traitement doit effacer ou rectifier sans délai les données inexactes. Le responsable du traitement doit notamment faciliter cette démarche lorsque les personnes concernées sont (ou étaient) des enfants et qu'elles souhaitent plus tard supprimer ces données à caractère personnel[39].
- Éviter la propagation d'erreurs – Les responsables du traitement devraient atténuer les effets d'une erreur cumulée dans la chaîne de traitement.
- Accès – Les personnes concernées devraient recevoir des informations sur les données à caractère personnel les concernant et se voir accorder un accès effectif à ces données, conformément aux articles 12 à 15 du RGPD, afin de pouvoir en contrôler l'exactitude et de les rectifier, le cas échéant.
- Maintien de l'exactitude - Les données à caractère personnel devraient être exactes à tous les stades du traitement et des tests portant sur l'exactitude devraient être effectués aux étapes critiques.
- Données tenues à jour - Les données à caractère personnel doivent être tenues à jour si les finalités du traitement le nécessitent.
- Conception des données – Utilisation de caractéristiques de conception technologique et organisationnelle pour réduire les inexactitudes, par exemple, présenter des choix prédéterminés concis au lieu de champs de texte libre.

Exemple 1

Une compagnie d'assurance souhaite utiliser l'intelligence artificielle (IA) pour établir le profil des clients qui souscrivent une assurance, afin de leur permettre de prendre des décisions lors du calcul du risque d'assurance. En définissant la manière de développer ses solutions d'IA, elle détermine les moyens du traitement et doit tenir compte de la protection des données dès la conception lorsqu'elle choisit une IA auprès d'un vendeur et décide de la manière d'entraîner l'IA.

Lorsqu'il détermine la manière d'entraîner l'IA, le responsable du traitement doit disposer de données exactes pour atteindre des résultats précis. Par conséquent, il doit veiller à ce que les données utilisées pour entraîner l'IA soient exactes.

Dès lors qu'il dispose d'une base juridique valable pour entraîner l'IA à l'aide de données à caractère personnel provenant d'un sous-ensemble important de clients existants, le responsable du traitement choisit un groupe de clients représentatif de la population afin d'éviter tout biais.

Les données sur les clients sont ensuite collectées à partir du système de traitement de données correspondant, y compris les données sur le type d'assurance, par exemple l'assurance maladie, l'assurance habitation, l'assurance voyage, etc., ainsi que les données des registres publics auxquels il

[39] Voir le considérant 65.

a légalement accès. Toutes les données sont pseudonymisées avant d'être transférées vers le système dédié à la formation du modèle d'IA.

Afin de veiller à ce que les données utilisées pour l'entraînement de l'IA soient aussi précises que possible, le responsable du traitement ne collecte que des données provenant de sources contenant des informations exactes et actualisées.

La compagnie d'assurance vérifie si l'IA est fiable et fournit des résultats non discriminatoires, aussi bien pendant le développement du produit que finalement avant sa mise sur le marché. Lorsque l'IA est pleinement formée et opérationnelle, la compagnie d'assurance utilise les résultats pour étayer les évaluations des risques d'assurance, mais sans toutefois s'appuyer uniquement sur l'IA pour décider d'accorder ou non l'assurance, à moins que la décision ne soit prise conformément aux exceptions prévues à l'article 22, paragraphe 2, du RGPD.

De même, la compagnie d'assurance examinera régulièrement les résultats de l'IA afin de garantir la fiabilité et, le cas échéant, d'adapter l'algorithme.

Exemple 2

Le responsable du traitement est un établissement de santé qui recherche des méthodes pour garantir l'intégrité et l'exactitude des données à caractère personnel figurant dans ses registres de clients.

Dans les cas où deux personnes arrivent dans l'établissement en même temps et reçoivent le même traitement, il existe un risque de confusion si le seul paramètre permettant de les distinguer est leur nom. Pour garantir l'exactitude des données, le responsable du traitement a besoin d'un identifiant unique pour chaque personne, et donc de plus d'informations que le seul nom du client.

L'établissement utilise plusieurs systèmes contenant des informations à caractère personnel de clients et doit veiller à ce que les informations relatives aux clients soient correctes, exactes et cohérentes dans tous les systèmes et à tout moment. L'établissement a recensé plusieurs risques susceptibles de se poser en cas de modification des informations dans un des systèmes mais pas dans les autres.

Le responsable du traitement décide d'atténuer le risque en recourant à une technique de hachage qui peut être utilisée pour garantir l'intégrité des données du journal de traitement. Un horodatage cryptographique immuable est créé pour les entrées du journal de traitement et le client qui y est associé, de sorte que toutes les modifications puissent être reconnues, corrélées et suivies.

## 3.7 Limitation de la conservation

80. Le responsable des données doit veiller à ce que les données à caractère personnel soient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées[40].
Il est essentiel que le responsable du traitement sache exactement quelles données à caractère personnel l'entreprise traite et pourquoi. La finalité du traitement est le critère principal pour déterminer la durée de conservation des données à caractère personnel.

[40] Article 5, paragraphe 1, point c), du RGPD.

81. Les mesures et garanties qui mettent en œuvre le principe de limitation de la conservation doivent compléter les droits et libertés des personnes concernées, en particulier le droit à l'effacement et le droit d'opposition.

82. En ce qui concerne la limitation de la conservation, on peut citer parmi les éléments clés pour la protection dès la conception et par défaut:

- Suppression et anonymisation – Le responsable du traitement doit disposer de procédures et de fonctionnalités internes claires en matière de suppression et/ou d'anonymisation.
- Effectivité de l'anonymisation/la suppression - Le responsable du traitement doit faire en sorte qu'il ne soit pas possible de réidentifier des données anonymisées ni de récupérer des données supprimées, et doit procéder à des vérifications à cet égard.
- Automatisation - La suppression de certaines données à caractère personnel devrait être automatisée.
- Critères de conservation - Le responsable du traitement doit déterminer quelles données et quelle durée de conservation sont nécessaires au regard des finalités.
- Justification – Le responsable du traitement doit être en mesure, d'une part, de justifier pourquoi la durée de conservation est nécessaire au regard de la finalité et des données à caractère personnel en question, et, d'autre part, de divulguer la justification et les fondements juridiques de la durée de conservation.
- Contrôle de l'application des politiques en matière de conservation - Le responsable du traitement doit faire appliquer les politiques internes en matière de conservation et vérifier si l'organisation met en œuvre ses politiques.
- Sauvegardes/journaux – Le responsable du traitement détermine les données à caractère personnel et la durée de conservation nécessaires pour les sauvegardes et journaux.
- Flux de données – Les responsables du traitement devraient faire preuve de vigilance à l'égard du flux de données à caractère personnel et de la conservation de toute copie de ces données, et ils devraient chercher à en limiter la conservation «temporaire».

Exemple

Le responsable du traitement collecte des données à caractère personnel lorsque le traitement a pour finalité de gérer une affiliation de la personne concernée. Les données à caractère personnel sont supprimées lorsque l'affiliation est résiliée et qu'il n'existe pas de base juridique pour une conservation ultérieure des données.

Le responsable du traitement définit d'abord une procédure interne en matière de conservation et de suppression des données. Conformément à cette procédure, les salariés doivent supprimer manuellement les données à caractère personnel à l'issue de la période de conservation. Le salarié suit la procédure pour supprimer et corriger régulièrement les données de tous les dispositifs, des sauvegardes, des journaux, des courriers électroniques et d'autres supports de stockage pertinents.

Au lieu de cela, pour rendre la suppression plus efficace et moins susceptible d'erreur, le responsable du traitement met ensuite en œuvre un système automatique permettant de supprimer les données de manière automatique, fiable et plus régulière. Le système est configuré pour suivre la procédure de suppression des données déterminée, qui intervient alors à intervalles réguliers prédéfinis afin de supprimer les données à caractère personnel de tous les supports de stockage de l'entreprise. Le responsable du traitement examine et teste régulièrement la procédure de conservation et s'assure qu'elle est conforme à la politique de conservation la plus récente.

## 3.8 Intégrité et confidentialité

83. Le principe d'intégrité et de confidentialité comprend la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dommages d'origine accidentelle, à l'aide des mesures techniques ou organisationnelles appropriées. La sécurité des données à caractère personnel requiert des mesures appropriées visant à prévenir et à gérer les incidents de violation des données, à garantir la bonne exécution des tâches de traitement des données et le respect des autres principes, ainsi qu'à faciliter l'exercice effectif des droits des personnes.

84. Le considérant 78 indique qu'une des mesures en matière de protection des données dès la conception et de protection des données par défaut pourrait consister à permettre au responsable du traitement de *«mettre en place des dispositifs de sécurité ou de les améliorer»*. Parallèlement à d'autres mesures en matière de protection des données dès la conception et de protection des données par défaut, le considérant 78 laisse entendre qu'il incombe aux responsables du traitement d'évaluer en permanence s'ils utilisent les moyens de traitement appropriés à tout moment et d'évaluer si les mesures choisies permettent de remédier aux vulnérabilités existantes. En outre, les responsables du traitement devraient procéder à des examens réguliers des mesures relatives à la sécurité de l'information qui entourent et protègent les données à caractère personnel, ainsi que de la procédure de traitement des violations de données.

85. En ce qui concerne l'intégrité et la confidentialité, on peut citer parmi les éléments clés pour la protection dès la conception et par défaut:
    - Système de gestion de la sécurité de l'information (SGSI) - Disposer d'un moyen opérationnel de gérer les politiques et les procédures en matière de sécurité de l'information.
    - Analyse de risque – Évaluer les risques pesant sur la sécurité des données à caractère personnel en considérant l'impact sur les droits des personnes et faire face aux risques recensés. En vue d'une utilisation dans l'évaluation des risques, développer et maintenir une «modélisation des menaces» complète, systématique et réaliste, ainsi qu'une analyse de la surface d'attaque du logiciel conçu pour réduire les vecteurs d'attaque et les possibilités d'exploiter les points faibles et les vulnérabilités.
    - Sécurité dès la conception – Tenir compte des exigences de sécurité le plus en amont possible dans la conception et le développement du système, et intégrer et effectuer en permanence les tests pertinents.
    - Maintenance – Examen et test réguliers des logiciels, du matériel, des systèmes et des services, etc., afin de repérer les éventuelles vulnérabilités des systèmes utilisés pour le traitement.
    - Gestion du contrôle d'accès – Seul le personnel autorisé et ayant besoin d'en connaître devrait avoir accès aux données à caractère personnel nécessaires à ses tâches de traitement, et le responsable du traitement devrait différencier les privilèges d'accès du personnel autorisé.
        - Limitation de l'accès (agents) – Concevoir le traitement de données de manière à ce qu'un nombre minimal de personnes aient besoin d'accéder aux données à caractère personnel pour exercer leurs fonctions, et limiter l'accès en conséquence.
        - Limitation de l'accès (contenu) – Dans le cadre de chaque opération de traitement, limiter l'accès aux seuls attributs par ensemble de données qui sont nécessaires pour effectuer cette opération. Limiter également l'accès aux données relatives aux personnes concernées qui relèvent de la compétence du salarié concerné.
        - Ségrégation de l'accès – Concevoir le traitement de données de manière à ce qu'aucun individu n'ait besoin d'un accès complet à toutes les données collectées sur une personne concernée, et encore moins à toutes les données personnelles d'une catégorie particulière de personnes concernées.

- Transferts sécurisés – Les transferts doivent être protégés contre tout accès et toute modification non autorisés ou accidentels.
- Conservation sécurisée - La conservation des données doit être protégée contre tout accès et toute modification non autorisés. Des procédures devraient être mises en place pour évaluer le risque d'une conservation centralisée ou décentralisée et déterminer quelles catégories de données personnelles sont concernées. Certaines données peuvent nécessiter des mesures de sécurité renforcées, ou il peut être nécessaire de les isoler d'autres données.
- Pseudonymisation - Les données à caractère personnel et sauvegardes/journaux devraient être pseudonymisés à titre de mesure de sécurité destinée à réduire au minimum les risques de violation potentielle des données, par exemple en utilisant le hachage ou le cryptage.
- Sauvegardes/journaux - Conserver les sauvegardes et les journaux dans la mesure nécessaire à la sécurité de l'information, utiliser les pistes d'audit et la surveillance des événements comme contrôle de sécurité de routine. Les sauvegardes et journaux sont protégés contre tout accès et toute modification non autorisés ou accidentels et sont examinés régulièrement. Les incidents doivent être traités rapidement.
- Reprise après sinistre/continuité d'activité – Répondre aux besoins de reprise après sinistre et de continuité d'activité des systèmes d'information, afin de rétablir la disponibilité des données à caractère personnel à la suite d'incidents majeurs.
- Protection en fonction du risque – Toutes les catégories de données à caractère personnel devraient être protégées par des mesures adéquates au regard du risque de violation de la sécurité. Les données présentant des risques particuliers devraient, lorsque cela est possible, être conservées séparément du reste des données à caractère personnel.
- Gestion de l'intervention en cas d'incident lié à la sécurité – Disposer de pratiques, de procédures et de ressources permettant de détecter, de contenir, de traiter et de signaler les violations de données, ainsi que d'en tirer des leçons.
- Gestion des incidents – Le responsable du traitement devrait disposer de processus permettant de traiter les violations et les incidents, afin de rendre le système de traitement plus robuste. Parmi ces processus figurent les procédures de notification, telles que la gestion de la notification (à l'autorité de contrôle) et l'information (aux personnes concernées).

Exemple

Un responsable du traitement souhaite extraire de grandes quantités de données à caractère personnel d'une base de données médicale contenant des dossiers médicaux électroniques (patients) vers un serveur de base de données dédié au sein de l'entreprise, afin de traiter les données extraites à des fins d'assurance qualité. Selon l'évaluation de l'entreprise, l'acheminement des extraits vers un serveur accessible à tous les salariés de l'entreprise constitue pour les droits et libertés des personnes concernées un risque susceptible d'être élevé. Étant donné qu'il n'existe qu'un seul service dans l'entreprise qui a besoin de traiter les extraits de données des patients, le responsable du traitement décide de limiter l'accès au serveur dédié aux salariés de ce service. De plus, pour réduire encore les risques, les données seront pseudonymisées avant d'être transférées.

Afin de réguler l'accès et d'atténuer les éventuels dommages causés par des logiciels malveillants, l'entreprise décide de séparer le réseau et d'établir des contrôles de l'accès au serveur. En outre, elle met en place une surveillance de la sécurité ainsi qu'un système de détection et de prévention des intrusions, et elle l'isole de l'utilisation courante. Un système de contrôle automatisé est mis en place pour surveiller l'accès et les modifications. Celui-ci produit des rapports et des alertes automatiques lorsque certains événements liés à l'utilisation sont configurés. Le responsable de la sécurité veillera à

ce que les utilisateurs n'aient accès aux données que sur la base du besoin d'en connaître et avec le niveau d'accès approprié. Toute utilisation inappropriée peut être rapidement et facilement repérée.

Certains des extraits doivent être comparés avec de nouveaux extraits et doivent donc être conservés pendant une période de trois mois. Le responsable du traitement décide de les placer dans des bases de données séparées sur le même serveur et d'utiliser un chiffrement de colonnes transparent pour les conserver. Les clés de décryptage des données de colonnes sont conservées dans des modules de sécurité dédiés, qui ne peuvent être utilisés que par le personnel autorisé, mais qui ne peuvent pas être extraits.

Le traitement des incidents ultérieurs rend le système plus robuste et plus fiable. Le responsable du traitement comprend que des mesures et garanties préventives et effectives devraient être intégrées dans tout traitement de données à caractère personnel actuel et futur, et que cette manière de procéder peut contribuer à prévenir à l'avenir les incidents liés à la violation de données.

Le responsable du traitement établit ces mesures de sécurité à la fois pour garantir l'exactitude, l'intégrité et la confidentialité, mais aussi pour empêcher que des logiciels malveillants ne se propagent en cas de cyberattaques, de façon à rendre la solution plus robuste. Le fait de disposer de mesures de sécurité solides contribue à renforcer la confiance avec les personnes concernées.

### 3.9 Responsabilité[41]

86. En vertu du principe de responsabilité, le responsable du traitement est responsable de la conformité avec tous les principes susmentionnés et doit être en mesure de démontrer cette conformité.

87. Le responsable du traitement doit être en mesure de démontrer le respect des principes. Pour cela, le responsable du traitement peut démontrer les effets des mesures prises pour protéger les droits des personnes concernées, et les raisons pour lesquelles les mesures sont considérées comme appropriées et efficaces. Par exemple, en démontrant pourquoi une mesure est appropriée pour garantir le principe de limitation de la conservation de façon effective.

88. Pour être en mesure de traiter les données à caractère personnel de façon responsable, le responsable du traitement devrait avoir à la fois la connaissance et la capacité de mettre en œuvre la protection des données. Cela implique que le responsable du traitement doit comprendre les obligations en matière de protection des données que lui impose le RGPD et doit être en mesure de s'y conformer.

## 4 ARTICLE 25, PARAGRAPHE 3 CERTIFICATION

89. Conformément à l'article 25, paragraphe 3, la certification en vertu de l'article 42 peut servir d'élément pour démontrer le respect de la protection des données dès la conception et de la protection des données par défaut. Inversement, les documents démontrant le respect de la protection des données dès la conception et de la protection des données par défaut peuvent également être utiles dans le cadre d'un processus de certification. Cela signifie que, lorsqu'un traitement effectué par un responsable du traitement ou un sous-traitant a été certifié en vertu de l'article 42, les autorités de contrôle en tiendront compte dans leur évaluation de la conformité avec le RGPD, en particulier en ce qui concerne la protection des données dès la conception et la protection des données par défaut.

[41] Voir le considérant 74, qui dispose que les responsables du traitement sont tenus de démontrer l'efficacité des mesures qu'ils mettent en œuvre.

90. Lorsqu'un traitement effectué par un responsable du traitement ou un sous-traitant est certifié conformément à l'article 42, les éléments qui contribuent à démontrer le respect de l'article 25, paragraphes 1 et 2, sont les processus de conception, c'est-à-dire le processus consistant à déterminer les moyens du traitement, la gouvernance et les mesures techniques et organisationnelles pour mettre en œuvre les principes de protection des données. Les critères de certification en matière de protection des données sont déterminés par les organismes de certification ou par les propriétaires du système de certification, puis approuvés par l'autorité de contrôle compétente ou par le comité européen de la protection des données. Pour plus d'informations sur les mécanismes de certification, le lecteur est renvoyé aux lignes directrices du comité européen de la protection des données concernant la certification[42], ainsi qu'à d'autres lignes directrices pertinentes, telles que publiées sur le site web du comité.

91. Même lorsqu'un traitement fait l'objet d'une certification conformément à l'article 42, le responsable du traitement est toujours tenu de contrôler et d'améliorer en permanence le respect des critères de l'article 25, en ce qui concerne la protection des données dès la conception et la protection des données par défaut.

# 5 APPLICATION DE L'ARTICLE 25 ET CONSEQUENCES

92. Les autorités de contrôle peuvent évaluer le respect des dispositions de l'article 25 conformément aux procédures énumérées à l'article 58. Les pouvoirs concernant les mesures correctrices sont précisés à l'article 58, paragraphe 2, et comprennent la délivrance d'avertissements, de rappels à l'ordre et d'ordres de respecter les droits des personnes concernées, l'imposition de limitations du traitement ou l'interdiction de celui-ci, l'imposition d'amendes administratives, etc.

93. La protection des données dès la conception et la protection des données par défaut sont également des facteurs à prendre en considération dans la détermination du niveau des sanctions pécuniaires pour infraction au RGPD (voir l'article 83, paragraphe 4)[43] [44].

# 6 RECOMMANDATIONS

94. Bien qu'ils ne soient pas directement visés par l'article 25, les sous-traitants et les producteurs sont également reconnus comme des facilitateurs clés pour la protection des données dès la conception et la protection des données par défaut. À ce titre, ils doivent savoir que les responsables du traitement sont tenus de ne traiter les données à caractère personnel qu'avec des systèmes et des technologies qui intègrent un dispositif de protection des données.

95. Lorsqu'ils réalisent des opérations de traitement au nom de responsables du traitement, ou qu'ils fournissent des solutions auxdits responsables, les sous-traitants et les producteurs devraient utiliser

[42] Comité. «Lignes directrices 1/2008 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement» Version 3.0 du 4 juin 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_fr.pdf

[43] L'article 83, paragraphe 2, point d), du RGPD dispose que, lors de la détermination du montant des amendes pour infraction au RGPD, *«il est dûment tenu compte»* du «degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32».

[44] De plus amples informations sur les amendes sont disponibles dans le document du groupe de travail «Article 29» intitulé «Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679». WP 253 du 3 octobre 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 - adoptées par le comité.

leur expertise, instaurer un climat de confiance et guider leurs clients, y compris les PME, dans la conception/fourniture de solutions intégrant la protection des données au traitement. Cela signifie que la conception des produits et des services devrait faciliter les besoins des responsables du traitement.

96. Lors de la mise en œuvre de l'article 25, il convient de garder à l'esprit que l'objectif principal de la conception est la *mise en œuvre effective* des principes et la *protection* des droits des personnes concernées dans le cadre des mesures appropriées du traitement. Afin de faciliter et d'améliorer l'adoption de la protection des données dès la conception et de la protection des données par défaut, les recommandations suivantes sont formulées à l'intention des responsables du traitement et des producteurs et sous-traitants:

- Les responsables du traitement devraient penser à la protection des données dès la conception et à la protection des données par défaut dès les *premiers stades* de la planification d'une opération de traitement, avant même le moment de la détermination des moyens du traitement.
- Lorsque le responsable du traitement dispose d'un délégué à la protection des données (DPD), le comité européen de la protection des données encourage la participation active du DPD afin d'intégrer la protection des données dès la conception et la protection des données par défaut dans les procédures de passation de marchés et de développement, ainsi que dans l'ensemble du cycle de vie du traitement.
- Une opération de traitement peut être *certifiée*. La possibilité de faire certifier une opération de traitement apporte une valeur ajoutée au responsable du traitement lorsque celui-ci doit choisir entre les différents logiciels, matériels, services et/ou systèmes de traitement des producteurs ou sous-traitants. Par conséquent, les producteurs devraient s'efforcer de démontrer la protection des données dès la conception et la protection des données par défaut dans le cycle de vie du développement d'une solution de traitement. Un label de certification peut également guider les personnes concernées dans leur choix entre différents produits et services. La possibilité de faire certifier un traitement peut constituer un avantage concurrentiel pour les producteurs, les sous-traitants et les responsables du traitement, et peut même renforcer la confiance des personnes concernées à l'égard du traitement de leurs données à caractère personnel. Si aucune certification n'est proposée, les responsables du traitement devraient s'efforcer d'obtenir d'autres *garanties* que les producteurs ou les sous-traitants respectent les exigences relatives à la protection des données dès la conception et à la protection des données par défaut.
- Les responsables du traitement, les sous-traitants et les producteurs devraient tenir compte de leur obligation de fournir une protection spécifique aux enfants de moins de 18 ans et aux autres groupes vulnérables, dans le cadre de la conformité avec la protection des données dès la conception et la protection des données par défaut.
- Les producteurs et les sous-traitants devraient chercher à faciliter la mise en œuvre de la protection des données dès la conception et de la protection des données par défaut, afin de soutenir la capacité du responsable du traitement à se conformer aux obligations de l'article 25. De leur côté, les responsables du traitement ne devraient pas choisir de producteurs ou de sous-traitants qui ne proposent pas de systèmes permettant ou aidant les responsables du traitement à se conformer à l'article 25, parce que ces derniers seront tenus responsables en cas de mise en œuvre déficiente de cet article.

- Les fournisseurs de technologies devraient jouer un rôle actif pour garantir le respect des critères relatifs à l'«état des connaissances» et informer les responsables du traitement de toute modification de l'«état des connaissances» susceptible d'affecter l'effectivité des mesures mises en place. Les responsables du traitement devraient inclure cette exigence en tant que clause contractuelle afin de s'assurer d'être tenus informés.
- Le comité européen de la protection des données recommande aux responsables du traitement d'exiger des producteurs et des sous-traitants qu'ils démontrent comment leur matériel, leurs logiciels, leurs services ou leurs systèmes permettent au responsable du traitement de se conformer aux exigences en matière de responsabilité, conformément à la protection des données dès la conception et à la protection des données par défaut, par exemple en utilisant des indicateurs clés de performance pour démontrer l'efficacité des mesures et des garanties dans la mise en œuvre des principes et des droits.
- Le comité souligne la nécessité d'une approche harmonisée pour mettre en œuvre les principes et les droits de façon effective, et encourage les associations ou les organismes élaborant des codes de conduite conformément à l'article 40 à y intégrer également des lignes directrices sectorielles spécifiques concernant la protection des données dès la conception et la protection des données par défaut.
- Les responsables du traitement devraient se montrer loyaux envers les personnes concernées et faire preuve de transparence quant à la manière dont ils évaluent et démontrent la mise en œuvre effective de la protection des données dès la conception et de la protection des données par défaut, de la même manière qu'ils démontrent le respect du RGPD en vertu du principe de responsabilité.
- Les technologies renforçant la protection de la vie privée (PET) qui ont atteint le niveau de maturité le plus élevé peuvent être utilisées comme mesure, conformément aux exigences de la protection des données dès la conception et de la protection des données par défaut, le cas échéant dans le cadre d'une approche fondée sur les risques. Les PET en elles-mêmes ne couvrent pas nécessairement les obligations prévues à l'article 25. Les responsables du traitement évaluent si la mesure est appropriée et effective pour mettre en œuvre les principes de protection des données et les droits des personnes concernées.
- Les systèmes antérieurs existants sont soumis aux mêmes obligations que les nouveaux systèmes en matière de protection des données dès la conception et de protection des données par défaut. Si les systèmes antérieurs ne sont pas déjà conformes aux exigences de protection des données dès la conception et de protection des données par défaut, et que des changements ne peuvent être apportés pour respecter les obligations, alors le système antérieur ne répond tout simplement pas aux obligations du RGPD et ne peut pas être utilisé pour traiter des données à caractère personnel.
- L'article 25 n'abaisse pas le seuil des exigences pour les PME. Les points suivants peuvent faciliter le respect de l'article 25 par les PME:
    - Effectuer des évaluations précoces des risques
    - Commencer par de petits traitements, puis augmenter leur ampleur et leur complexité par la suite
    - Obtenir des garanties de protection des données dès la conception et de protection des données par défaut de la part des producteurs et des sous-traitants, telles que la certification ou le respect de codes de conduite
    - Faire appel à des partenaires ayant fait leurs preuves

- Discuter avec les autorités de protection des données
- Lire les lignes directrices des autorités de protection des données et du comité
- Adhérer aux codes de conduite lorsqu'ils existent
- Obtenir une aide et des conseils professionnels

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)