Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD

Version 2.1

Adoptées le 24 mai 2023

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Historique des versions

Version 1.0	12 mai 2022	Adoption des lignes directrices pour consultation publique
Version 2.0	24 mai 2023	Adoption des lignes directrices après la consultation publique
Version 2.1	29 juin 2023	Correction mineure

RÉSUMÉ

Le comité européen de la protection des données (EDPB) a adopté les présentes lignes directrices dans le but d'harmoniser la méthode employée par les autorités de contrôle pour calculer le montant des amendes. Les présentes lignes directrices viennent compléter les lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 (WP 253), précédemment adoptées, qui portent principalement sur les circonstances dans lesquelles l'imposition d'une amende est nécessaire.

L'autorité de contrôle peut décider du calcul du montant de l'amende, sous réserve de l'observation des règles prévues par le RGPD. Dans ce contexte, le RGPD exige que le montant de l'amende soit, dans chaque cas, effectif, proportionné et dissuasif (article 83, paragraphe 1, du RGPD). Par ailleurs, lorsqu'elles décident du montant de l'amende, les autorités de contrôle tiennent dûment compte d'une liste de circonstances ayant trait aux caractéristiques de la violation (sa gravité) ou à la nature de l'auteur de la violation (article 83, paragraphe 2, du RGPD). Pour finir, le montant de l'amende n'excède pas les montants maximaux prévus à l'article 83, paragraphes 4, 5 et 6, du RGPD. La détermination du montant de l'amende repose dès lors sur une appréciation spécifique réalisée pour chaque cas d'espèce et suivant les paramètres prévus par le RGPD.

Eu égard aux éléments qui précèdent, l'EDPB a conçu la méthode suivante, qui se compose de cinq étapes, afin de calculer les amendes administratives à infliger en cas de violation du RGPD.

La première étape consiste à recenser les opérations de traitement de l'espèce et à évaluer le caractère applicable de l'article 83, paragraphe 3, du RGPD (**chapitre 3**). La deuxième étape consiste à fixer le montant de départ pour le calcul ultérieur de l'amende (**chapitre 4**). Pour y parvenir, il convient d'évaluer la qualification de la violation au titre du RGPD, de jauger la gravité de la violation à la lumière des circonstances de l'espèce et de quantifier le chiffre d'affaires de l'entreprise. La troisième étape consiste à apprécier les circonstances aggravantes et atténuantes liées au comportement passé ou actuel du responsable du traitement ou du sous-traitant et à majorer ou minorer le montant de l'amende en conséquence (**chapitre 5**). La quatrième étape consiste à déterminer les montants maximaux légaux applicables aux différentes violations. Les majorations appliquées aux étapes précédentes ou suivantes ne peuvent dépasser ce montant maximal (**chapitre 6**). La dernière étape consiste à déterminer si le montant final calculé est bien effectif, proportionné et dissuasif, tel que l'exige le RGPD. L'amende peut encore être ajustée en conséquence (**chapitre 7**), sans toutefois dépasser le montant maximal légal applicable.

Il faut garder à l'esprit, tout au long des étapes exposées ci-dessus, que le calcul d'une amende n'est pas qu'un simple exercice mathématique. Bien au contraire, les circonstances du cas d'espèce spécifique constituent les facteurs déterminants permettant de fixer le montant final, qui peut (dans tous les cas) être n'importe quel montant jusqu'à concurrence du montant maximal légal.

L'EDPB assurera un réexamen constant des présentes lignes directrices et de la méthode qui y est exposée.

Table des matières

Le comité européen de la protection des données,

vu l'article 70, paragraphe 1, points e), j) et k), 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 sur l'Espace économique européen, et notamment 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[1],

vu les articles 12 et 22 de son règlement intérieur,

vu les lignes directrices du groupe de travail «Article 29» sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679, WP 253, qui ont été approuvées par le comité européen de la protection des données (ci-après l'«EDPB») lors de sa première réunion plénière,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES

CHAPITRE 1 – INTRODUCTION

1.1 – Cadre juridique

1. Avec le règlement général sur la protection des données (ci-après le «RGPD»), en vigueur depuis le 25 mai 2018, l'Union européenne a mené à bien une réforme approfondie de la réglementation relative à la protection des données en Europe. La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. Le règlement repose sur plusieurs éléments clés, notamment le renforcement des pouvoirs d'application des règles des autorités de contrôle. Le règlement impose un nouveau niveau d'amendes considérablement plus élevé, et prévoit l'harmonisation des calculs d'amendes entre les États membres.

2. Les responsables du traitement et les sous-traitants sont plus que jamais chargés de veiller à la protection effective des données à caractère personnel des individus. Les autorités de contrôle sont investies de pouvoirs pour garantir que les principes du RGPD ainsi que les droits des personnes concernées sont respectés conformément à l'esprit et à la lettre du RGPD.

3. C'est pourquoi l'EDPB a formulé des orientations visant à fournir une base claire et transparente pour la fixation des amendes par les autorités de contrôle. Les lignes directrices sur l'application et la fixation des amendes administratives précédemment publiées abordent les circonstances dans lesquelles une amende administrative constituerait un outil adéquat et interprètent les critères visés à l'article 83 du RGPD à cet égard[2]. Les présentes lignes directrices portent sur la méthode de calcul desdites amendes administratives.

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».
[2] Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679, WP 253 (ci-après les «lignes directrices WP 253»). Les lignes directrices WP 253 ont été approuvées par l'EDPB au cours de sa première réunion plénière du 25 mai 2018. Voir la déclaration d'approbation 1/2018, disponible en ligne à cette adresse.

Ces deux séries de lignes directrices peuvent s'appliquer simultanément et doivent être considérées comme complémentaires.

1.2 – Objectifs

4. Les présentes lignes directrices sont destinées aux autorités de contrôle, qui les utilisent afin de veiller à une application cohérente du RGPD. Elles reflètent en outre la compréhension commune par l'EDPB des dispositions de l'article 83 du RGPD.

5. Les présentes lignes directrices ont pour ambition de fixer des montants de départ harmonisés et d'en faire des orientations communes sur la base desquelles les amendes administratives dans chaque cas d'espèce peuvent être calculées. Néanmoins, selon une jurisprudence constante, il n'est pas nécessaire que de telles lignes directrices soient si spécifiques qu'elles permettent à un responsable du traitement ou à un sous-traitant de calculer précisément le montant de l'amende anticipée[3]. Il est souligné, tout au long des présentes lignes directrices, que le montant final de l'amende est fonction de l'ensemble des circonstances de l'espèce. L'EDPB envisage dès lors d'harmoniser les montants de départ et la méthode de calcul des amendes, plutôt que le résultat.

6. Les présentes lignes directrices peuvent être considérées comme une approche progressive à suivre, bien que les autorités de contrôle ne soient aucunement tenues d'en observer toutes les étapes si ces dernières ne trouvent pas application dans un cas donné, ni d'exposer des motivations ayant trait aux aspects des lignes directrices qui sont sans objet. Cependant, le raisonnement devrait inclure au minimum les facteurs qui ont permis de déterminer le degré de gravité, le chiffre d'affaires appliqué ainsi que les facteurs aggravants et atténuants qui ont été pris en considération.

7. Nonobstant les présentes lignes directrices, les autorités de contrôle restent soumises à toutes les obligations procédurales prévues par le droit national et le droit de l'Union, y compris l'obligation de motiver leurs décisions de même que les obligations qui leur incombent en vertu du mécanisme du «guichet unique». Dans cet esprit, bien que les autorités de contrôle soient tenues de motiver leurs conclusions de manière adéquate conformément au droit national et au droit de l'Union, les présentes lignes directrices ne doivent pas être interprétées en ce sens qu'elles imposent à l'autorité de contrôle d'indiquer le montant de départ exact ou de quantifier l'incidence précise de chaque circonstance aggravante ou atténuante. Qui plus est, une simple référence aux présentes lignes directrices ne saurait remplacer les motivations à énoncer dans un cas particulier.

8. Les présentes lignes directrices feront l'objet d'un réexamen constant, au fil de l'évolution des pratiques au sein de l'UE et de l'EEE. Il y a lieu de souligner qu'à l'exception du Danemark et de l'Estonie[4], les autorités de contrôle sont habilitées à infliger des amendes administratives, qui sont contraignantes si aucun recours n'est formé à leur encontre. Ainsi, avec le temps, les pratiques administratives et judiciaires continueront à évoluer.

1.3 – Champ d'application

9. Les présentes lignes directrices entendent régir et jeter les bases de la fixation des amendes par les autorités de contrôle à un niveau général. Les orientations formulées s'appliquent à tous les types de responsables du

[3] Voir, par exemple, les affaires jointes C-189/02 P, C-202/02 P, C-205/02 P à C-208/02 P et C-213/02 P, *Dansk Rørindustri A/S e.a./Commission*, point 172 et l'affaire T-91/11, *InnoLux Corp./Commission*, point 88.
[4] Voir considérant 151 du RGPD.

traitement et de sous-traitants au sens de l'article 4, paragraphes 7 et 8, du RGPD, à l'exception des personnes physiques lorsqu'elles n'agissent pas en tant qu'entreprises. Cela étant, les autorités nationales restent investies du pouvoir d'infliger des amendes aux personnes physiques.

10. Conformément à l'article 83, paragraphe 7, du RGPD, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire. Pour autant que les autorités de contrôle aient ce pouvoir sur la base des dispositions du droit national, les présentes lignes directrices s'appliquent au calcul de l'amende à infliger aux autorités et organismes publics, à l'exception du chapitre 4.3. Les autorités de contrôle ont néanmoins toute latitude pour appliquer une méthode analogue à celle décrite dans ledit chapitre. En outre, le chapitre 6 ne s'applique pas au calcul de l'amende à infliger aux autorités et organismes publics lorsque le droit national prévoit des montants maximaux légaux différents et que l'autorité ou l'organisme public visé n'agit pas en tant qu'entreprise au sens du chapitre 6.2.1.

11. Les lignes directrices s'appliquent aux affaires transfrontières et non transfrontières.

12. Les présentes lignes directrices ne sont pas exhaustives et ne fournissent pas d'explications sur les différences entre les systèmes administratifs, civils ou pénaux nationaux lors de l'imposition de sanctions administratives en général.

1.4 – Applicabilité

13. Aux termes de l'article 70, paragraphe 1, point e), du RGPD, l'EDPB est habilité à publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente du RGPD L'article 70, paragraphe 1, point k), du RGPD précise que le comité veille à l'application cohérente du RGPD et, de sa propre initiative ou, le cas échéant, à la demande de la Commission européenne, élabore, notamment, à l'intention des autorités de contrôle, des lignes directrices concernant l'application des mesures visées à l'article 58 ainsi que la fixation des amendes administratives en vertu de l'article 83.

14. Afin d'assurer une approche cohérente de l'imposition des amendes administratives, qui reflète de manière adéquate l'ensemble des principes énoncés dans le RGPD, l'EDPB est convenu d'une définition commune des critères d'évaluation visés à l'article 83 du RGPD. Les différentes autorités de contrôle intégreront cette approche commune, conformément au droit administratif et judiciaire local qui les régit.

CHAPITRE 2 – MÉTHODE DE CALCUL DU MONTANT DE L'AMENDE

2.1 – Considérations générales

15. Nonobstant les obligations de coopération et d'application cohérente du règlement, le calcul du montant de l'amende est laissé à la discrétion de l'autorité de contrôle. Le RGPD exige que le montant de l'amende soit, dans chaque cas, effectif, proportionné et dissuasif (article 83, paragraphe 1, du RGPD). Par ailleurs, lorsqu'elles décident du montant de l'amende, les autorités de contrôle tiennent dûment compte d'une liste de circonstances ayant trait aux caractéristiques de la violation (sa gravité) ou à la nature de l'auteur de la violation (article 83, paragraphe 2, du RGPD). La détermination du montant de l'amende repose dès lors sur une appréciation spécifique réalisée pour chaque cas d'espèce, en prenant en considération les paramètres prévus par le RGPD.

16. Le RGPD ne prévoit aucune amende minimale pour les comportements enfreignant les règles en matière de protection des données. En effet, des montants maximaux ne sont prévus qu'à l'article 83, paragraphes 4 à 6, du RGPD, qui regroupe plusieurs types de comportements divers. Au bout du compte, une amende ne peut être calculée qu'en considérant l'ensemble des facteurs expressément recensés à l'article 83, paragraphe 2, points a) à j), du RGPD, pertinents pour le cas en l'espèce, ainsi que tout autre élément utile, même s'il n'est pas explicitement répertorié dans lesdites dispositions [l'article 83, paragraphe 2, point k), du RGPD, exigeant qu'il soit tenu dûment compte de tout autre facteur applicable]. Enfin, le montant final de l'amende résultant de cette appréciation doit être effectif, proportionné et dissuasif pour chaque cas d'espèce (article 83, paragraphe 1, du RGPD). Toute amende infligée doit prendre l'ensemble de ces paramètres en considération, de manière satisfaisante, sans pour autant excéder le montant maximal légal fixé à l'article 83, paragraphes 4 à 6, du RGPD.

2.2 – Vue d'ensemble de la méthode

17. Compte tenu de ces paramètres, l'EDPB a conçu la méthode suivante pour le calcul des amendes administratives à infliger en cas de violation du RGPD.

Étape 1	Recenser les opérations de traitement en l'espèce et évaluer le caractère applicable de l'article 83, paragraphe 3, du RGPD. **(Chapitre 3)**
Étape 2	Fixer le montant de départ pour le calcul ultérieur sur la base d'une appréciation (**chapitre 4**) a) de la qualification au titre de l'article 83, paragraphes 4 à 6, du RGPD; b) de la gravité de la violation conformément à l'article 83, paragraphe 2, points a), b) et g), du RGPD; c) du chiffre d'affaires de l'entreprise en tant qu'élément utile à prendre en considération en vue d'infliger une amende effective, proportionnée et dissuasive, dans le respect de l'article 83, paragraphe 1, du RGPD.
Étape 3	Apprécier les circonstances aggravantes et atténuantes liées au comportement passé ou actuel du responsable du traitement ou du sous-traitant et majorer ou minorer le montant de l'amende en conséquence. **(Chapitre 5)**
Étape 4	Déterminer les montants maximaux légaux applicables pour les différentes opérations de traitement. Les majorations appliquées aux étapes précédentes ou suivantes ne peuvent dépasser ces montants. **(Chapitre 6)**
Étape 5	Déterminer si le montant final de l'amende calculée est bien effectif, proportionné et dissuasif, tel que l'exige l'article 83, paragraphe 1, du RGPD, et majorer ou minorer l'amende en conséquence. **(Chapitre 7)**

2.3 – Violations passibles d'amendes fixes

18. Dans certaines circonstances, l'autorité de contrôle peut estimer que certaines violations sont passibles d'une amende d'un montant fixe prédéterminé. L'application d'un montant fixe à certains types de violations ne peut entraver l'application du RGPD, plus particulièrement de son article 83. Qui plus est, l'application de montants fixes ne dispense pas les autorités de contrôle de respecter les obligations de coopération et de cohérence (chapitre VII du RGPD).

19. L'autorité de contrôle est libre de déterminer quels types de violation sont passibles d'une amende d'un montant fixe prédéterminé, selon leur nature, leur gravité et leur durée, sauf si cette détermination est proscrite ou si elle est contraire au droit national de l'État membre.

20. Les montants fixes peuvent être définis à la discrétion de l'autorité de contrôle, en tenant compte, entre autres, du contexte social et économique de l'État membre concerné, au regard de la gravité de la violation telle qu'interprétée par l'article 83, paragraphe 2, points a), b) et g), du RGPD. Nous recommandons que l'autorité de contrôle communique au préalable les montants et les modalités d'application.

CHAPITRE 3 – CONCOURS D'INFRACTIONS ET APPLICATION DE L'ARTICLE 83, PARAGRAPHE 3, DU RGPD

21. Avant de pouvoir calculer le montant d'une amende au moyen de la méthode exposée dans les présentes lignes directrices, il est essentiel de déterminer, en premier lieu, quel comportement (circonstances de fait entourant les agissements) et quelles violations (descriptions juridiques abstraites de ce qui est passible de sanctions) motivent l'imposition de l'amende. En effet, un cas d'espèce particulier peut présenter des circonstances pouvant être considérées comme constituant soit un seul et même comportement, soit des comportements passibles de sanctions distincts. Il est également possible que plusieurs violations diverses naissent d'un seul et même comportement. Dans un tel cas, l'imputation d'une violation peut empêcher l'imputation d'une autre violation, ou toutes les violations peuvent être imputées ensemble. En d'autres termes, il peut y avoir des cas de concours d'infractions. En fonction des règles relatives aux concours d'infractions, ces violations peuvent donner lieu à des calculs d'amendes différents.

22. Selon l'analyse des traditions des États membres en matière de règles relatives aux concours d'infractions, telles qu'elles sont décrites dans la jurisprudence de la CJUE, [5]
et compte tenu des champs d'application et conséquences juridiques divers, ces principes peuvent être grossièrement regroupés dans les **trois catégories** suivantes:
    - **Concours d'infractions (chapitre 3.1.1)**,
    - **Unité d'action (chapitre 3.1.2)**,
    - **Pluralité d'actions (chapitre 3.2)**.

23. Ces différentes catégories de concours n'entrent pas en conflit les unes avec les autres, mais elles ont des champs d'application distincts et elles s'inscrivent dans un système général cohérent permettant d'instaurer un programme de tests logique.

24. En conséquence, il est important de déterminer tout d'abord
    a. si les circonstances de l'espèce doivent être considérées comme constituant un seul comportement (**chapitre 3.1**) ou

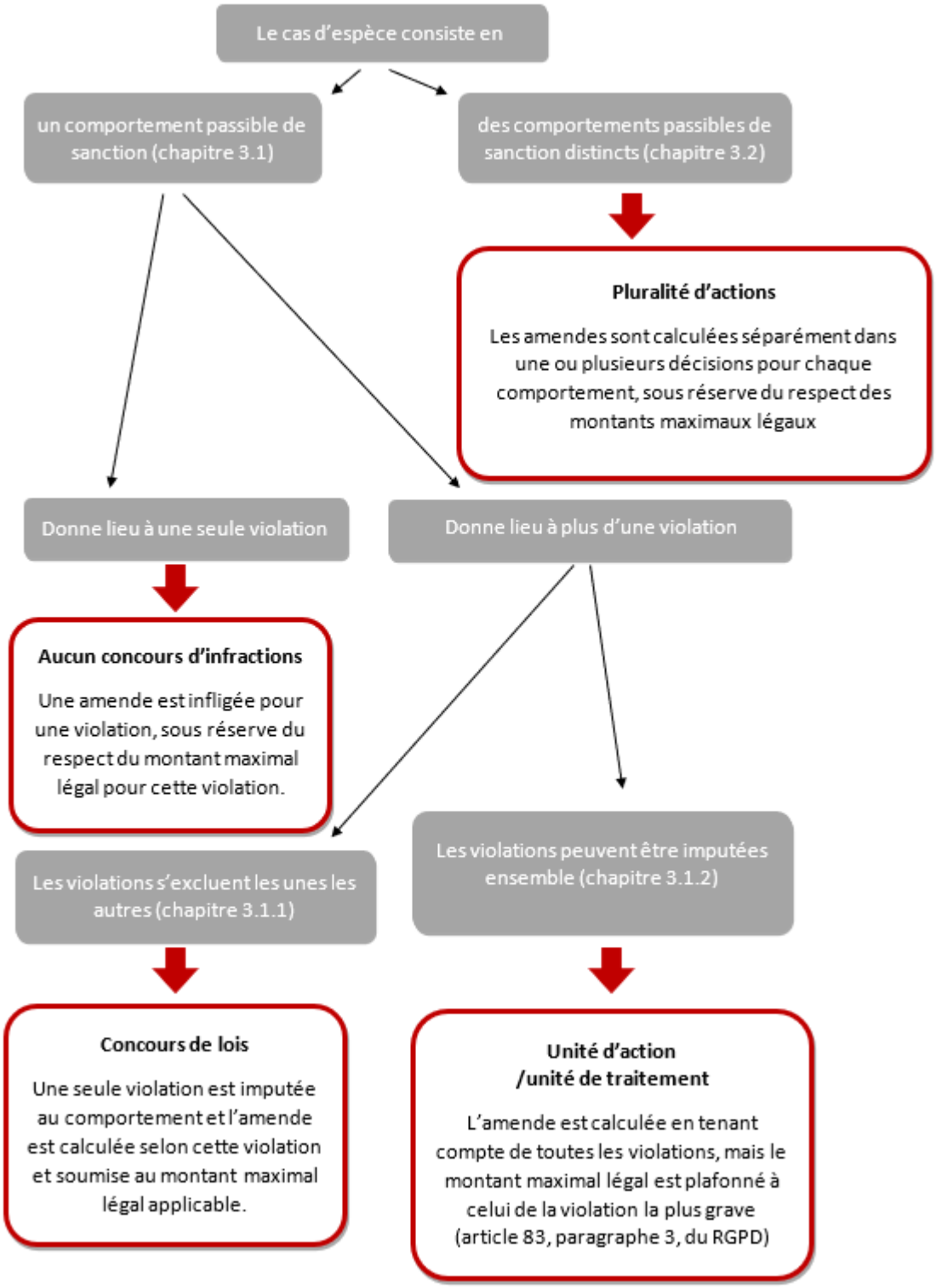
       plusieurs comportements passibles de sanctions (**chapitre 3.2**),
    b. dans le cas d'un comportement unique (**chapitre 3.1**), si ce dernier donne lieu à

       une ou plusieurs violations, et

[5] Voir plus particulièrement l'analyse approfondie exposée dans les conclusions de l'avocat général Tanchev dans l'affaire C-10/18 P, *Marine Harvest*.

c. dans le cas d'un comportement unique donnant lieu à des violations multiples, si l'imputation d'une violation empêche l'imputation d'une autre violation (**chapitre 3.1.1**) ou si les violations doivent être imputées ensemble (**chapitre 3.1.2**).

SCHÉMA


Le cas d'espèce consiste en
un comportement passible de sanction (chapitre 3.1)
des comportements passibles de sanction distincts (chapitre 3.2)
Pluralité d'actions
Les amendes sont calculées séparément dans une ou plusieurs décisions pour chaque comportement, sous réserve du respect des montants maximaux légaux
Donne lieu à une seule violation
Donne lieu à plus d'une violation
Aucun concours d'infractions
Une amende est infligée pour une violation, sous réserve du respect du montant maximal légal pour cette violation.
Les violations s'excluent les unes les autres (chapitre 3.1.1)
Les violations peuvent être imputées ensemble (chapitre 3.1.2)
Concours de lois
Une seule violation est imputée au comportement et l'amende est calculée selon cette violation et soumise au montant maximal légal applicable.
Unité d'action /unité de traitement
L'amende est calculée en tenant compte de toutes les violations, mais le montant maximal légal est plafonné à celui de la violation la plus grave (article 83, paragraphe 3, du RGPD)

3.1 – Comportement unique passible de sanctions

25. Dans un premier temps, il est crucial d'estimer si un seul et même comportement passible de sanctions est en cause («idem») ou si plusieurs comportements sont en cause de façon à définir quels sont les agissements passibles de sanctions pertinents qui doivent faire l'objet d'une amende. Dès lors, il est essentiel de saisir quelles circonstances sont considérées comme constituant un seul et même comportement, par opposition à des comportements multiples. Les agissements passibles de sanctions en question doivent être évalués et recensés au cas par cas. Par exemple, dans certains cas d'espèce, «la même opération de traitement ou [des] opérations de traitement liées» peuvent constituer un seul et même comportement.

26. La notion d'«opération de traitement» est incluse dans l'article 4, point 2), du RGPD, dans lequel «traitement» est défini comme «toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que 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.»

27. Lorsqu'il est question d'évaluer «[une] même opération de traitement ou [des] opérations de traitement liées», il convient de garder à l'esprit que toutes les obligations nécessaires sur le plan juridique pour que les opérations de traitement soient réalisées dans le respect des lois peuvent être prises en considération par l'autorité de contrôle dans le cadre de son appréciation des violations, y compris, par exemple, les obligations en matière de transparence (par exemple, l'article 13 du RGPD). Ce point est également mis en avant par les termes «dans le cadre de la même opération de traitement ou d'opérations de traitement liées», qui indique que le champ d'application de cette disposition englobe toute violation liée aux mêmes opérations de traitement ou à des opérations de traitement liées et susceptible d'avoir une incidence sur celles-ci.

28. Le terme «liées» renvoie au principe selon lequel un comportement unique peut consister en plusieurs agissements perpétrés dans le cadre d'une volonté unitaire et qui sont si étroitement liés sur le plan contextuel (notamment en ce qui concerne l'identité de la personne concernée, la finalité et la nature), spatial et temporel que, d'un point de vue objectif, ils seraient considérés comme constituant un comportement unique cohérent. Un lien suffisant ne devrait pas être facilement présumé pour que l'autorité de contrôle évite d'enfreindre les principes de dissuasion et d'application effective du droit européen. Par conséquent, ces aspects des relations nécessaires à la détermination d'un lien suffisant doivent être appréciés au cas par cas.

Exemple 1a – Opérations de traitement identiques ou liées
Un établissement financier demande à une agence d'évaluation du crédit de réaliser un examen de la solvabilité. L'établissement financier reçoit les informations demandées et les stocke dans son système.

Bien que la collecte et la conservation des données relatives à la solvabilité par l'établissement financier constituent chacune, en elle-même, une opération de traitement, elles forment un ensemble d'opérations de traitement qui sont effectuées dans le cadre d'une volonté unitaire et qui sont si étroitement liées sur le plan contextuel, spatial et temporel que, d'un point de vue objectif, elles seraient considérées comme constituant un comportement unique cohérent. Dès lors, les opérations de traitement réalisées par l'établissement financier doivent être considérées comme «liées» et constituent un comportement unique.

Exemple 1b – Opérations de traitement identiques ou liées

Un courtier en données décide de mettre en œuvre une nouvelle activité de traitement qui est la suivante: il décide de collecter, en tant que tiers, l'historique des transactions de consommateurs auprès de dizaines de détaillants, sans aucune base juridique, afin de réaliser une analyse psychométrique visant à prédire le comportement futur des personnes, notamment leur comportement électoral, leur intention de démissionner et plus encore. Parallèlement, le courtier en données décide de ne pas inclure cette procédure dans ses registres des activités de traitement, de ne pas informer les personnes concernées et d'ignorer toute demande d'accès introduite par ces personnes en lien avec les nouvelles opérations de traitement. Les opérations concernées par cette activité forment un ensemble d'opérations de traitement qui sont effectuées dans le cadre d'une volonté unitaire et qui sont liées sur le plan contextuel, spatial et temporel. Ces opérations doivent être considérées comme étant «liées» et comme constituant un comportement unique. Ce comportement englobe aussi le non-respect des obligations d'inscrire l'activité de traitement dans les registres, d'informer les personnes concernées et d'établir des procédures permettant d'accorder le droit d'accès en ce qui concerne les nouvelles opérations de traitement. Ces obligations ont été violées pour les opérations de traitement liées.

Exemple 1c – Opérations de traitement différentes ou non liées
i) Une autorité compétente en matière de construction vérifie les antécédents d'un candidat à un poste. Cette vérification porte également sur les affinités politiques, l'affiliation à une organisation syndicale ainsi que l'orientation sexuelle. ii) Cinq jours plus tard, l'autorité exige de ses fournisseurs (entrepreneurs individuels) une divulgation excessive de données ayant trait aux accords commerciaux qu'ils concluent avec d'autres entités, indépendamment de la pertinence desdites données par rapport au contrat passé avec l'autorité ou aux obligations de mise en conformité qui incombent à cette dernière. iii) Une semaine plus tard, l'autorité est victime d'une violation de données à caractère personnel. Le réseau de l'autorité est piraté, malgré l'existence de mesures techniques et organisationnelles adéquates, et le pirate parvient à obtenir l'accès à un système de traitement des données à caractère personnel des citoyens ayant déposé des demandes auprès de l'autorité. Bien que les données aient été convenablement chiffrées, conformément aux normes en vigueur, le pirate réussit à les déchiffrer au moyen d'une technologie de déchiffrement militaire et vend les données sur le dark web. L'autorité se garde d'informer l'autorité de contrôle, bien qu'elle soit tenue de le faire. Les opérations de traitement concernées en l'espèce, à savoir la vérification des antécédents, les demandes de divulgation de la part des fournisseurs et le manquement à l'obligation de notifier la violation de données à caractère personnel, ne sont pas liées sur le plan contextuel. Ainsi, il n'y a pas lieu de les considérer comme des opérations «liées», mais comme des opérations constituant des comportements distincts.

29. Lorsqu'il est établi que les circonstances de l'espèce constituent un seul et même comportement et donnent lieu à une violation unique, l'amende peut être calculée sur la base de cette violation et du montant maximal légal correspondant. Néanmoins, si les circonstances du cas d'espèce forment un seul et même comportement, mais que ce dernier donne lieu non pas à une seule, mais à plusieurs violations, il y a lieu de déterminer si l'imputation d'une violation empêche l'imputation d'une autre violation (chapitre 3.1.1) ou si les violations peuvent être imputées ensemble (chapitre 3.1.2). Lorsque des comportements multiples naissent des circonstances de l'espèce, ils doivent être considérés comme des actions multiples et traités conformément au chapitre 3.2.

3.1.1 – Concours d'infractions

30. Le principe de concours d'infractions (également appelé «conflit apparent»[6] ou «faux conflit») s'applique lorsque l'application d'une disposition exclut ou englobe l'application d'une autre disposition. En d'autres termes, le concours d'infractions se produit déjà au niveau abstrait des dispositions légales. Il peut s'agir du principe de spécialité[7], de subsidiarité ou de consommation, qui s'applique souvent lorsque des dispositions protègent le même intérêt juridique. Dans de tels cas, il serait contraire aux lois de sanctionner deux fois l'auteur d'une violation pour le même acte répréhensible[8].

31. Dans un tel cas de concours d'infractions, le montant de l'amende devrait être calculé uniquement sur la base de la violation retenue conformément aux règles susmentionnées («violation prépondérante»)[9].

Principe de spécialité[10]

32. Le principe de spécialité (*specialia generalibus derogant*) est un principe juridique en vertu duquel une disposition plus spécifique (dérivée du même acte juridique ou d'actes juridiques distincts ayant même valeur légale) supplante une disposition plus générale, bien que les deux dispositions poursuivent le même objectif. L'infraction plus spécifique est alors parfois considérée comme une «qualification» de l'infraction moins spécifique. Une infraction qualifiée peut être passible d'une amende d'un montant supérieur, pour laquelle le montant maximal est plus élevé ou le délai de prescription plus long.

33. Cependant, le principe de spécialité peut également trouver application, parfois par voie interprétative, lorsque, du fait de sa nature et de son caractère systémique, une infraction est considérée comme une qualification d'une infraction apparemment plus spécifique, bien que le libellé seul ne mentionne pas explicitement un élément supplémentaire.

34. Lorsque, au contraire, deux dispositions poursuivent des objectifs indépendants, cela constitue un facteur de différenciation justifiant l'imposition d'amendes distinctes. Par exemple, si la violation d'une des dispositions entraîne automatiquement la violation de l'autre, mais que la violation de cette dernière n'entraîne pas la violation de la première, ces violations poursuivent des objectifs indépendants.

35. Le principe de spécialité ne peut s'appliquer que si et dans la mesure où les objectifs poursuivis par les violations en cause sont effectivement concordants dans le cas d'espèce. Étant donné que les principes relatifs à la protection des données prévus à l'article 5 du RGPD sont établis en tant que concepts généraux, des situations peuvent survenir dans lesquelles d'autres dispositions constituent une concrétisation d'un tel principe, mais ne le circonscrivent pas dans son intégralité. Autrement dit, une disposition ne définit pas toujours l'ensemble du champ d'application du principe[11]. En conséquence, selon les circonstances de l'espèce[12], les violations peuvent, dans certains cas, se chevaucher de manière concordante et une violation peut prédominer sur une autre, tandis que dans d'autres cas, le chevauchement n'est que partiel et les violations ne concordent donc pas totalement. Dans la mesure où les violations ne concordent pas, il n'y a

[6] Voir, par exemple, la décision du *Verwaltungsgerichtshof* (Autriche), Ra 2018/02/0123, point 9.
[7] Tel qu'évalué dans l'affaire C-10/18 P, *Marine Harvest/Commission*.
[8] Voir, par exemple, la décision du *Verwaltungsgerichtshof* (Autriche), Ra 2018/02/0123, point 7.
[9] Tel qu'évalué dans l'affaire C-10/18 P, *Marine Harvest/Commission*.
[10] Tel qu'évalué dans l'affaire C-10/18 P, *Marine Harvest/Commission*.
[11] Décision contraignante 1/2021 de l'EDPB concernant le litige relatif au projet de décision de l'autorité de contrôle irlandaise concernant WhatsApp Ireland en application de l'article 65, paragraphe 1, point a), du RGPD (ci-après la «décision contraignante 1/2021 de l'EDPB»), point 192.
[12] Décision contraignante 1/2021 de l'EDPB, point 193.

pas de concours d'infractions. En revanche, les violations peuvent être imputées ensemble lors du calcul de l'amende.

Principe de subsidiarité

36. Une autre forme de concours d'infractions est souvent appelée «principe de subsidiarité». Ce principe s'applique lorsqu'une infraction est considérée comme subsidiaire par rapport à une autre. Cette application peut être due au fait que la loi déclare formellement la subsidiarité ou au fait que cette dernière est déclarée pour des raisons matérielles[13]. Cette déclaration peut survenir lorsque les violations poursuivent le même objectif, mais que l'une d'entre elles implique une accusation moins grave d'immoralité ou d'acte répréhensible (par exemple, une infraction administrative peut être subsidiaire par rapport à une infraction pénale, etc.)

Principe de consommation

37. Le principe de consommation s'applique dans les cas où la violation d'une disposition entraîne régulièrement la violation de l'autre, souvent parce que la première violation constitue une étape préliminaire à l'autre.

3.1.2 – Unité d'action – Article 83, paragraphe 3, du RGPD

38. À l'instar du concours d'infractions, le principe de l'unité d'action (également appelé «concours idéal») s'applique dans les cas où un comportement tombe sous le coup de plusieurs dispositions légales, à la différence qu'une disposition n'est ni exclue ni englobée par l'application de l'autre, parce que les principes de spécialité, de subsidiarité ou de consommation ne s'y appliquent pas et qu'elles poursuivent pour la plupart des objectifs distincts.

39. Le principe de l'unité d'action a été précisé au niveau du droit dérivé à l'article 83, paragraphe 3, du RGPD sous la forme d'une «unité de traitement». Il est crucial de comprendre que l'article 83, paragraphe 3, du RGPD est limité dans son application et ne s'appliquera pas à chaque cas dans lequel des violations multiples sont constatées, mais uniquement aux cas dans lesquels des violations multiples ont découlé «de la même opération de traitement ou d'opérations de traitement liées», comme expliqué ci-dessus.[14] Dans ces cas, le montant total de l'amende administrative n'excède pas le montant fixé pour la violation la plus grave[15].

---

[13] L'idée d'une subsidiarité formelle est également indirectement impliquée à l'article 35, paragraphe 2, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), bien que le conflit soit résolu sur le plan procédural plutôt que matériel. La disposition réglemente que «[l]orsque les autorités de contrôle visées à l'article 55 ou 56 du règlement (UE) 2016/679 imposent une amende administrative en vertu de l'article 58, paragraphe 2, point i), dudit règlement, les autorités compétentes n'imposent pas d'amende administrative au titre de l'article 34 de la [directive SRI 2] pour une violation visée [à l'article 35, paragraphe 1, de la directive SRI 2] et découlant du même comportement que celui qui a fait l'objet d'une amende administrative au titre de l'article 58, paragraphe 2, point i), du règlement (UE) 2016/679 […].» Dans la mesure où la violation visée à l'article 35, paragraphe 1, de la directive SRI 2, est indirectement considérée comme subsidiaire par rapport à une amende infligée au titre du RGPD lorsque le comportement en cause est le même.

[14] Décision contraignante 1/2021 de l'EDPB, point 320.

[15] L'article 83, paragraphe 3, du RGPD dispose dans son intégralité: «Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du présent règlement, dans le cadre de la même

40. Dans certains cas d'espèce particuliers, une unité d'action peut également être présumée lorsqu'une action unique enfreint plusieurs fois la même disposition légale. Plus particulièrement, cette présomption peut survenir lorsque les circonstances donnent lieu à une infraction itérative et semblable de la même disposition légale dans un enchaînement spatial et temporel rapproché.

> ***Exemple 2 – Unité d'action***
> *Un responsable du traitement envoie différentes vagues de courriers électroniques de prospection à des groupes de personnes concernées au cours d'une même journée sans aucune base juridique et enfreint ainsi, à plusieurs reprises, l'article 6, paragraphe 1, du RGPD par le biais d'une unité d'action.*

41. Le libellé de l'article 83, paragraphe 3, du RGPD ne semble pas s'appliquer directement à ce dernier cas d'unité d'action, puisque «plusieurs dispositions» ne sont pas enfreintes. Néanmoins, il y aurait traitement injuste et inéquitable si l'auteur d'une violation qui, par une action, enfreint différentes dispositions poursuivant des objectifs distincts se trouvait privilégié par rapport à l'auteur d'une violation qui, par la même action, enfreint plusieurs fois la même disposition poursuivant le même objectif. Afin d'éviter toute incohérence de principe juridique et de respecter le droit fondamental à l'égalité de traitement consacré dans la charte, l'article 83, paragraphe 3, du RGPD s'applique mutatis mutandis à de tels cas.

42. En cas d'unité d'action, le montant total de l'amende administrative n'excède pas le montant fixé pour la violation la plus grave. «En ce qui concerne l'interprétation de l'article 83, paragraphe 3, du RGPD, l'EDPB souligne que le principe de l'effet utile impose à toutes les institutions de donner pleinement effet au droit de l'Union»[16]. À cet égard, l'article 83, paragraphe 3, du RGPD ne doit pas être interprété en ce sens que «peu importe qu'un responsable du traitement ait commis une ou plusieurs violations du RGPD […] lors de l'appréciation de l'amende»[17].

43. La formulation «montant total» suppose que toutes les violations commises doivent être prises en considération lors de l'appréciation du montant de l'amende[18], et la formulation «montant fixé pour la violation la plus grave» renvoie aux montants maximaux légaux des amendes (par exemple, les montants prévus à l'article 83, paragraphe 4 à 6, du RGPD). Par conséquent, «[b]ien que l'amende elle-même ne puisse pas dépasser le maximum légal du niveau de l'amende le plus élevé, le contrevenant doit toujours être explicitement reconnu coupable d'avoir violé plusieurs dispositions et ces violations doivent être prises en considération lors de l'appréciation du montant de l'amende finale à infliger»[19]. Bien que cela soit sans préjudice de l'obligation, pour l'autorité de contrôle imposant l'amende, de respecter l'exigence relative au caractère proportionné de l'amende, les autres violations commises ne peuvent être écartées et doivent être prises en considération lors du calcul de l'amende.

3.2 – Comportements multiples passibles de sanctions

opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave.»

[16] Décision contraignante 1/2021 de l'EDPB, point 322.

[17] Ibidem, point 323.

[18] Ibidem, point 325.

[19] Ibidem, point 326.

44. Le principe de la pluralité d'actions (également appelé «Realkonkurrenz», «concours de faits» ou «concours de coïncidences») décrit tous les cas d'espèce auxquels les principes du concours d'infractions (chapitre 3.1.1) ou l'article 83, paragraphe 3, du RGPD (chapitre 3.1.2) ne s'appliquent pas.

45. Ces violations sont traitées dans une seule décision pour l'unique raison qu'elles ont été portées au même moment à l'attention de l'autorité de contrôle, par coïncidence, sans qu'il s'agisse pour autant d'opérations de traitement identiques ou liées au sens de l'article 83, paragraphe 3, du RGPD. Dès lors, le contrevenant est réputé avoir enfreint plusieurs dispositions légales et des amendes distinctes sont infligées conformément à la procédure nationale, soit dans la même décision, soit dans des décisions distinctes. Par ailleurs, l'article 83, paragraphe 3, du RGPD ne trouvant pas application, le montant total de l'amende administrative peut dépasser le montant fixé pour la violation la plus grave (argumentum e contrario). Les cas de pluralité d'actions ne sauraient motiver le fait de privilégier le contrevenant lors du calcul de l'amende. Toutefois, ils sont sans préjudice de l'obligation de respecter le principe général de proportionnalité de l'amende.

Exemple 3 – Pluralité d'actions
Après avoir effectué un audit en matière de protection des données dans les locaux d'un responsable du traitement, l'autorité de contrôle constate que ce dernier n'a mis en place aucune procédure d'examen et d'amélioration continue de la sécurité de son site web, qu'il n'a pas fourni à ses employés les informations visées à l'article 13 concernant le traitement des données relatives aux ressources humaines et qu'il n'a pas informé l'autorité de contrôle d'une récente violation de données ciblant les données de ses fournisseurs. Aucune de ces violations n'est exclue ou englobée au titre du principe de spécialité, de subsidiarité ou de consommation. Qui plus est, elles ne peuvent être qualifiées ni d'opération de traitement identique ni d'opérations de traitement liées: elles ne constituent pas une unité d'action, mais une pluralité d'actions. L'autorité de contrôle conclura donc que le responsable du traitement a enfreint, par des comportements distincts, les articles 13, 32 et 33 du RGPD. Elle infligera, dans sa décision, des amendes individuelles pour chaque violation, sans qu'un maximum légal unique s'applique à leur somme.

CHAPITRE 4 – MONTANT DE DÉPART DU CALCUL

46. L'EDPB considère que les amendes administratives doivent être calculées à partir d'un montant de départ harmonisé[20]. Ce montant de départ constitue le montant de base d'un calcul ultérieur, pour lequel toutes les circonstances du cas d'espèce ont été prises en considération et pondérées, de manière à parvenir au montant final de l'amende à infliger au responsable du traitement ou au sous-traitant.

47. La fixation de montants de départ harmonisés dans les présentes lignes directrices n'empêche pas et ne devrait en aucun cas empêcher les autorités de contrôle d'évaluer chaque cas dans leur spécificité. L'amende imposée à un responsable du traitement ou à un sous-traitant peut aller de n'importe quel montant jusqu'au montant maximal légal correspondant, à condition que cette amende soit effective, dissuasive et

[20] Pour autant que les lignes directrices laissent une marge de manœuvre suffisante pour ajuster l'amende administrative aux circonstances du cas d'espèce, la Cour de justice de l'UE (ci-après la «CJUE») accepte généralement que les calculs débutent à partir d'un montant de départ abstrait. En particulier dans les affaires jointes C-189/02 P, C-202/02 P, C-205/02 P à C-208/02 P et C-213/02 P, *Dansk Rørindustri*, mais aussi plus récemment dans l'affaire T-15/02, *BASF AG/Commission*, points 120 et 121; 134, l'affaire C-227/14 P, *LG Display Co. Ltd/Commission*, point 53 et l'affaire T-26/02, *Daiichi Pharmaceutical Co. Ltd/Commission*, point 50.

proportionnée. L'existence d'un montant de départ n'empêche pas l'autorité de contrôle de minorer ou de majorer l'amende (jusqu'au montant maximal) si les circonstances du cas d'espèce l'exigent.

48. L'EDPB estime que trois éléments constituent le point de départ d'un calcul ultérieur: la classification des violations par nature en vertu de l'article 83, paragraphes 4 à 6, du RGPD, la gravité de la violation (telle qu'indiquée à la section 4.2 ci-dessous) et le chiffre d'affaires de l'entreprise en tant qu'élément pertinent à prendre en considération en vue d'imposer une amende effective, dissuasive et proportionnée, en application de l'article 83, paragraphe 1, du RGPD. Ces éléments sont exposés aux chapitres 4.1, 4.2 et 4.3 ci-dessous.

4.1 – Classification des violations au titre de l'article 83, paragraphes 4 à 6, du RGPD

49. Presque toutes les obligations qui incombent aux responsables du traitement et aux sous-traitants en vertu du règlement sont classées en fonction de leur nature dans les dispositions de l'article 83, paragraphes 4 à 6[21]. Le RGPD prévoit deux catégories de violations: les violations punissables en vertu de l'article 83, paragraphe 4, du RGPD, d'une part, et les violations punissables au titre de l'article 83, paragraphes 5 et 6, du RGPD, d'autre part. La première catégorie de violations est passible d'une amende maximale de 10 millions d'EUR ou de 2 % du chiffre d'affaires annuel de l'entreprise, le montant le plus élevé étant retenu, tandis que la seconde catégorie est passible d'une amende maximale de 20 millions d'EUR ou de 4 % du chiffre d'affaires annuel de l'entreprise, le montant le plus élevé étant retenu.

50. À travers cette distinction, le législateur a donné une première indication de la gravité de la violation, de manière abstraite. Plus la violation est grave, plus l'amende est susceptible d'être élevée.

4.2 – Gravité de la violation dans chaque cas d'espèce

51. Le RGPD exige des autorités de contrôle qu'elles prennent en considération, de manière adéquate, la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi [article 83, paragraphe 2, point a), du RGPD]; le fait que la violation a été commise délibérément ou par négligence [article 83, paragraphe 2, point b), du RGPD]; et les catégories de données à caractère personnel concernées par la violation [article 83, paragraphe 2, point g), du RGPD]. Aux fins des présentes lignes directrices, l'EDPB désigne ces facteurs comme étant la gravité de la violation.

52. L'autorité de contrôle doit examiner ces facteurs à la lumière des circonstances du cas d'espèce et doit déterminer, sur la base de cet examen, le degré de gravité tel qu'indiqué au paragraphe 60. À cet égard, l'autorité de contrôle peut également chercher à savoir si les données en cause étaient directement identifiables. En réalité, même si ces facteurs sont abordés individuellement dans les présentes lignes directrices, ils sont souvent étroitement liés et doivent être analysés en relation avec tous les faits du cas d'espèce.

4.2.1 – Nature, gravité et durée de la violation

53. L'article 83, paragraphe 2, point a), du RGPD, a un champ d'application large et exige de l'autorité de contrôle qu'elle procède à un examen complet de tous les éléments qui constituent la violation et qui sont à même de la différencier d'autres violations du même type. Cet examen doit donc tenir compte des facteurs spécifiques suivants:

[21] Voir à cet égard les lignes directrices WP 253, p. 9.

a) La **nature de la violation**, analysée en fonction des circonstances concrètes du cas d'espèce. En ce sens, cette analyse est plus spécifique que la classification abstraite prévue à l'article 83, paragraphes 4 à 6, du RGPD. L'autorité de contrôle peut se pencher sur l'intérêt que la disposition enfreinte œuvre à protéger et l'importance de cette disposition dans le cadre de la protection des données. En outre, l'autorité de contrôle peut chercher à déterminer dans quelle mesure la violation a empêché l'application effective de la disposition et la réalisation de l'objectif qu'elle visait à protéger.

b) La **gravité de la violation**, appréciée sur la base des circonstances spécifiques. Comme énoncé à l'article 83, paragraphe 2, point a), du RGPD, cela concerne la nature du traitement, mais aussi «la portée ou [...] la finalité du traitement concerné, ainsi que [le] nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi», qui donneront une indication de la gravité de la violation.

   i. La **nature du traitement**, y compris le contexte dans lequel le traitement s'inscrit sur le plan fonctionnel (par exemple, une activité commerciale, un organisme à but non lucratif, un parti politique, etc.) ainsi que toutes les caractéristiques du traitement[22]. Lorsque la nature du traitement comporte des risques plus élevés, par exemple lorsque la finalité est de contrôler, d'évaluer des aspects personnels ou de prendre des décisions ou d'adopter des mesures ayant des retombées négatives pour les personnes concernées, en fonction du contexte du traitement et du rôle du responsable du traitement ou du sous-traitant, l'autorité de contrôle peut envisager d'accorder plus d'importance à ce facteur. En outre, une autorité de contrôle peut accorder plus d'importance à ce facteur lorsque les personnes concernées et le responsable du traitement sont liés par un rapport de force manifestement déséquilibré (par exemple, lorsque les personnes concernées sont des employés, des élèves ou des patients) ou lorsque le traitement concerne des personnes vulnérables, en particulier des enfants.

   ii. La **portée du traitement**, en référence à la portée locale, nationale ou transfrontière du traitement réalisé et à la relation entre cette information et la portée réelle du traitement en ce qui concerne l'allocation des ressources par le responsable du traitement. Cet élément met en évidence un facteur de risque réel, associé à la plus grande difficulté, pour la personne concernée et l'autorité de contrôle, de mettre un frein à un comportement illicite au fur et à mesure que la portée du traitement s'élargit. Plus la portée du traitement est large, plus l'autorité de contrôle peut accorder d'importance à ce facteur.

   iii. La **finalité du traitement** amènera l'autorité de contrôle à accorder plus d'importance à ce facteur. L'autorité de contrôle peut également chercher à savoir si le traitement des données à caractère personnel relève des activités dites principales du responsable du traitement. Plus le traitement est au cœur des activités principales du responsable du traitement ou du sous-traitant, plus les irrégularités dans ce traitement seront graves.

[22] À titre d'exemple, en analysant l'élément relatif à la «nature de la violation», l'EDPB a, dans sa décision 01/2020 concernant le litige relatif au projet de décision de l'autorité de contrôle irlandaise concernant Twitter International Company en application de l'article 65, paragraphe 1, point a), du RGPD (ci-après la «décision contraignante 01/2020 de l'EDPB») fait remarquer que le «traitement concerné» impliquait des communications publiées par des personnes concernées ayant délibérément choisi de restreindre l'audience à laquelle ces communications étaient destinées, et a recommandé que cet aspect soit pris en considération lors de l'évaluation de la nature du traitement. Dans ce contexte, voir également la décision contraignante 01/2020 de l'EDPB, point 186.

L'autorité de contrôle peut accorder plus d'importance à ce facteur dans ces circonstances. Toutefois, il peut arriver que le traitement de données à caractère personnel soit davantage à la périphérie des activités principales du responsable du traitement ou du sous-traitant, mais qu'il exerce malgré cela une influence considérable sur l'évaluation (tel est le cas, par exemple, du traitement de données à caractère personnel de travailleurs lorsque la violation porte gravement atteinte à la dignité de ces derniers).

iv. Le **nombre de personnes concernées** concrètement mais aussi le nombre de personnes concernées potentiellement affectées doivent être pris en considération. Plus il y a de personnes concernées, plus l'autorité de contrôle peut accorder d'importance à ce facteur. Dans de nombreux cas, on peut également estimer que la violation prend une connotation «systémique» et qu'elle peut de ce fait affecter d'autres personnes concernées qui n'ont introduit aucune réclamation ou aucun signalement auprès de l'autorité de contrôle, même à des moments différents. L'autorité de contrôle peut, en fonction des circonstances du cas d'espèce, étudier le rapport entre le nombre de personnes concernées affectées et le nombre total de personnes concernées dans ce contexte (par exemple, le nombre de citoyens, de clients ou d'employés), de façon à trancher sur la question de savoir si la violation revêt un caractère systémique.

v. Le **niveau de dommage** subi et la mesure dans laquelle le comportement peut affecter les droits et les libertés individuels. La mention du «niveau» de dommage subi vise donc à attirer l'attention des autorités de contrôle sur le dommage subi ou susceptible d'avoir été subi en tant que paramètre complémentaire et distinct en rapport avec le nombre de personnes concernées impliquées (par exemple, dans les cas où il y a beaucoup de personnes concernées affectées par le traitement illicite, mais où le dommage subi par ces personnes est négligeable). Conformément au considérant 75 du RGPD, le niveau de préjudice subi renvoie aux dommages physiques, matériels ou à un préjudice moral. En tout état de cause, l'appréciation du dommage doit se limiter à ce qui est nécessaire sur le plan fonctionnel pour parvenir à une évaluation correcte du degré de gravité de la violation, comme indiqué au point 60 ci-dessous, sans déborder sur les activités des autorités judiciaires chargées de cerner les différentes formes de dommage individuel.

c) La **durée de la violation**, ce qui signifie qu'une autorité de contrôle peut généralement accorder plus d'importance à une violation ayant duré plus longtemps. Plus la durée de la violation est longue, plus l'autorité de contrôle peut accorder d'importance à ce facteur. Sous réserve du droit national, si un comportement donné était également illicite au titre du cadre réglementaire précédent, tant la période postérieure à la date d'entrée en vigueur du RGPD que la période antérieure à cette entrée en vigueur peuvent être prises en considération pour fixer le montant de l'amende, compte tenu des conditions dudit cadre.

54. L'autorité de contrôle peut accorder une certaine importance aux facteurs susmentionnés, en fonction des circonstances du cas d'espèce. S'ils ne sont pas particulièrement utiles, ces facteurs peuvent également être réputés neutres.

4.2.2 – Caractère délibéré ou négligent de la violation

55. Dans ses orientations antérieures, l'EDPB affirmait qu'«[e]n général, l'"intention" comprend à la fois la connaissance et la volonté en rapport avec les caractéristiques d'une infraction, tandis que "non délibérément" signifie qu'il n'y a pas eu d'intention de commettre la violation, bien que le responsable du

traitement ou le sous-traitant n'ait pas respecté l'obligation de diligence qui lui incombe en vertu de la législation[23]». Dans ce sens, «non délibérément» n'est pas synonyme de «non volontaire».

Exemple 4 – Illustrations du caractère délibéré et de la négligence (extraites du document WP 253)[24]
«Les circonstances qui dénotent une violation délibérée peuvent être un traitement illicite autorisé explicitement par la haute direction du responsable du traitement, ou contre l'avis du délégué à la protection des données ou au mépris des politiques existantes, par exemple le fait d'obtenir et de traiter des données concernant les salariés d'un concurrent dans l'intention de discréditer celui-ci sur le marché. Voici d'autres exemples:

- *la modification de données à caractère personnel dans le but de donner faussement l'impression que des objectifs ont été atteints — cela s'est vu dans le contexte des objectifs concernant les listes d'attente dans les hôpitaux;*
- *la vente de données à caractère personnel à des fins de commercialisation, c'est-à-dire le fait de vendre des données comme si la personne concernée avait donné son consentement préalable sans vérifier son avis à ce sujet ou en passant outre celui-ci.*

D'autres circonstances, comme le fait de ne pas lire et de ne pas respecter les politiques existantes, les erreurs humaines ou le fait de ne pas vérifier la présence de données à caractère personnel dans les informations publiées, de ne pas appliquer à temps les mises à jour techniques ou de ne pas adopter de politiques (au lieu de s'abstenir uniquement de les appliquer) peuvent dénoter une négligence.»

56. Le caractère délibéré ou négligent de la violation [article 83, paragraphe 2, point b), du RGPD] doit être évalué en tenant compte des éléments objectifs du comportement, recueillis à partir des faits du cas d'espèce. L'EDPB a souligné qu'«[i]l est généralement admis que les violations commises délibérément, qui manifestent un mépris pour les dispositions législatives, sont plus graves que les violations commises non délibérément»[25]. En cas de violation commise délibérément, l'autorité de contrôle est susceptible d'accorder une plus grande importance à ce facteur. Selon les circonstances en l'espèce, l'autorité de contrôle peut également accorder de l'importance au degré de négligence. Dans le meilleur des cas, la négligence peut être réputée neutre.

4.2.3 – Catégories de données à caractère personnel concernées

57. Concernant l'obligation de tenir compte des catégories de données à caractère personnel concernées [article 83, paragraphe 2, point g), du RGPD], le RGPD met clairement en évidence les types de données nécessitant une protection particulière et donc une amende plus stricte. Il s'agit, au minimum, des types de données visés aux articles 9 et 10 du RGPD, et des données ne relevant pas du champ d'application de ces articles, dont la diffusion cause à la personne concernée un dommage immédiat ou une souffrance[26] (par exemple, les données de localisation, les données relatives aux communications privées, les numéros d'identification nationaux ou les données financières, telles que les relevés de transactions ou les numéros de cartes de crédit)[27]. Généralement, plus il y a de catégories de données concernées ou plus les données concernées sont sensibles, plus l'autorité de contrôle peut accorder d'importance à ce facteur.

[23] Voir les lignes directrices WP 253, p. 11.
[24] Exemples cités directement dans les lignes directrices WP 253, p. 12.
[25] Voir les lignes directrices WP 253, p. 12.
[26] Ibid, p. 14.
[27] La diffusion de communications privées et de données de localisation peut causer des dommages immédiats ou une souffrance à la personne concernée, ce qui a été mis en évidence par la protection spéciale accordée par le législateur de l'Union aux communications privées à l'article 7 de la charte des droits fondamentaux et dans la directive 2002/58/CE ainsi que par la CJUE en ce qui concerne les données de localisation dans certains cas, voir les affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 117 et la jurisprudence qui y est citée.

58. En outre, la quantité de données ayant trait à chaque personne concernée est pertinente, étant donné que la violation du droit au respect de la vie privée et à la protection des données à caractère personnel s'aggrave au fur et à mesure que la quantité de données concernant chaque personne concernée augmente.

4.2.4 – Classification de la gravité de la violation et fixation du montant de départ adéquat

59. L'appréciation des facteurs susmentionnés (chapitre 4.2.1 à 4.2.3) permet de déterminer la gravité de la violation dans son ensemble. Cette appréciation n'est pas un calcul mathématique dans le cadre duquel les facteurs susmentionnés sont examinés individuellement, mais plutôt une évaluation rigoureuse des circonstances concrètes de l'espèce, dans laquelle tous les facteurs susmentionnés sont liés. Dès lors, au cours de l'examen de la gravité de la violation, il convient de tenir compte de la violation dans son ensemble.

60. Sur la base de l'évaluation des facteurs susmentionnés, le degré de gravité de la violation est considéré comme étant i) faible, ii) moyen ou iii) élevé. Ces degrés ne préjugent pas de la question de savoir si une amende peut être imposée ou non.

- Lors du calcul de l'amende administrative à infliger pour les violations de **gravité faible**, l'autorité de contrôle fixe un montant de départ pour le calcul ultérieur compris entre 0 et 10 % du montant maximal légal applicable.

- Lors du calcul de l'amende administrative à infliger pour les violations de **gravité moyenne**, l'autorité de contrôle fixe un montant de départ pour le calcul ultérieur compris entre 10 et 20 % du montant maximal légal applicable.

- Lors du calcul de l'amende administrative à infliger pour les violations de **gravité élevée**, l'autorité de contrôle fixe un montant de départ pour le calcul ultérieur compris entre 20 et 100 % du montant maximal légal applicable.

61. En règle générale, plus la violation est grave au sein de sa catégorie propre, plus le montant de départ est susceptible d'être élevé.

62. Les fourchettes dans lesquelles le montant de départ est déterminé font l'objet d'un examen constant par l'EDPB et ses membres et peuvent être adaptées si nécessaire.

Exemple 5a – Qualification de la gravité d'une violation (gravité élevée)
Après avoir enquêté sur de nombreuses plaintes concernant des appels non sollicités introduites par les clients d'une compagnie téléphonique, l'autorité de contrôle compétente a constaté que ladite compagnie utilisait les coordonnées de ses clients à des fins de démarchage téléphonique sans base juridique valable (violation de l'article 6 du RGPD). Plus particulièrement, la compagnie téléphonique a proposé les noms et les numéros de téléphone enregistrés de ses clients à des tiers à des fins de démarchage. La compagnie téléphonique a agi de la sorte au mépris de l'avis contraire du délégué à la protection des données, sans faire d'efforts pour enrayer cette pratique ou offrir aux clients un moyen de s'y opposer. Dans les faits, cette pratique avait lieu depuis mai 2018 et se poursuivait toujours au moment de l'enquête. La compagnie téléphonique en question opérait à l'échelle nationale et la pratique affectait l'ensemble de ses 4 millions de clients. L'autorité de contrôle a constaté que tous ces clients avaient régulièrement fait l'objet d'appels non sollicités de la part de tiers, sans qu'aucun moyen efficace ait été prévu pour y mettre un terme.

L'autorité de contrôle a été chargée d'évaluer la gravité de la violation dans ce cas d'espèce. Tout d'abord, l'autorité de contrôle a noté qu'une violation de l'article 6 du RGPD ***figure parmi les violations de l'article 83, paragraphe 5, du RGPD****, et qu'elle tombe donc sous le coup du niveau supérieur de l'article 83 du RGPD. Ensuite, l'autorité de contrôle a apprécié les circonstances du cas d'espèce. À cet égard, l'autorité de contrôle a accordé une grande importance à la* ***nature de la violation****, étant donné que la disposition enfreinte (article 6 du RGPD) sous-tend la légalité du traitement des données dans son ensemble. Le non-respect de cette disposition invalide la légalité du traitement dans son ensemble. Par ailleurs, l'autorité de contrôle a accordé une grande importance à la* ***durée de la violation****, qui a débuté au moment de l'entrée en vigueur du RGPD et n'avait pas cessé au moment de l'enquête. Le fait que la compagnie téléphonique opérait à l'échelle nationale a renforcé l'importance de la* ***portée du traitement****. Le* ***nombre de personnes concernées*** *impliquées a été jugé très élevé (4 millions, sur une population totale de 14 millions de personnes), tandis que le* ***niveau de dommage*** *subi par ces personnes a été jugé modéré (préjudice moral, sous la forme d'une nuisance). Cette dernière appréciation a été réalisée en tenant compte des* ***catégories de données concernées*** *(noms et numéros de téléphone). La gravité de la violation a toutefois été accrue par le fait que ladite violation a été commise au mépris d'un avis du délégué à la protection des données et qu'elle a donc été considérée comme* ***délibérée****.*

Compte tenu de tout ce qui précède (gravité, longue durée, nombre élevé de personnes concernées, portée nationale, caractère délibéré, dommage modéré), l'autorité de contrôle conclut qu'il y a lieu de considérer la violation comme étant de ***gravité élevée****. L'autorité de contrôle fixera un montant de départ pour le calcul ultérieur compris entre 20 et 100 % du montant maximal légal prévu à l'article 83, paragraphe 5, du RGPD.*

Exemple 5b – Qualification de la gravité d'une violation (gravité moyenne)
Une autorité de contrôle a reçu une notification de violation de données à caractère personnel de la part d'un hôpital. Il ressort de cette notification que plusieurs membres du personnel ont pu consulter des parties de dossiers médicaux de patients auxquelles ils n'auraient pas dû avoir accès, en raison du service auquel ils sont affectés. L'hôpital avait œuvré à l'élaboration de procédures pour réglementer l'accès aux dossiers médicaux des patients et avait mis en place des mesures strictes de restriction d'accès. Ainsi, le personnel d'un service ne pouvait accéder qu'aux informations médicales utiles pour ce service particulier. Qui plus est, l'hôpital avait investi dans des actions de sensibilisation de son personnel au sujet de la protection de la vie privée. Toutefois, il s'est avéré qu'il existait certains problèmes concernant le suivi des autorisations. Les membres du personnel transférés d'un service vers un autre pouvaient toujours accéder aux dossiers médicaux des patients de leur «ancien» service et l'hôpital n'avait aucune procédure établie permettant d'actualiser les autorisations en fonction des nouveaux postes occupés par les membres du personnel. Une enquête interne menée par l'hôpital a révélé qu'au moins 150 membres du personnel (sur 3 500) disposaient d'autorisations erronées, affectant au moins 20 000 des 95 000 dossiers médicaux de patients. L'hôpital a pu démontrer qu'à 16 reprises au moins, des membres du personnel avaient utilisé leurs autorisations pour consulter des dossiers médicaux de patients. L'autorité de contrôle considère qu'il y a eu violation de l'article 32 du RGPD.

Pour évaluer la gravité du cas d'espèce, l'autorité de contrôle a tout d'abord noté qu'une violation de l'article 32 du RGPD ***figure parmi les violations de l'article 83, paragraphe 4, du RGPD****, et qu'elle tombe donc sous le coup du niveau inférieur de l'article 83 du RGPD. Ensuite, l'autorité de contrôle a apprécié les circonstances du cas d'espèce. À cet égard, l'autorité de contrôle a estimé que, même si le* ***nombre de personnes concernées affectées*** *par la violation n'était que de 16, ce nombre aurait*

*pu être porté à 20 000 dans les circonstances du cas d'espèce et même à 95 000, compte tenu de la nature systémique du problème. Qui plus est, l'autorité de contrôle a qualifié la violation de **négligence**, mais à un faible degré, ce facteur ayant été réputé neutre dans les circonstances de ce cas d'espèce particulier, puisque l'hôpital n'a adopté aucune politique d'autorisation alors qu'il aurait certainement dû le faire, mais qu'il avait par ailleurs pris des dispositions pour mettre en œuvre des mesures strictes de restriction d'accès. Cette évaluation n'a pas été influencée par le fait que d'autres politiques de protection des données et de sécurité avaient été mises en place avec succès, comme l'exige le RGPD. Enfin, l'autorité de contrôle a accordé une grande importance au fait que les dossiers médicaux des patients contiennent des données relatives à la santé, qui constituent des **catégories particulières de données** au sens de l'article 9 du RGPD.*

*Compte tenu de tout ce qui précède (nature du traitement et catégories particulières de données par rapport au nombre de personnes concernées effectivement et potentiellement affectées), l'autorité de contrôle conclut qu'il y a lieu de considérer la violation comme étant de **gravité moyenne**. L'autorité de contrôle fixera un montant de départ pour le calcul ultérieur compris entre 10 et 20 % du montant maximal légal prévu à l'article 83, paragraphe 4, du RGPD.*

Exemple 5c – Qualification de la gravité d'une violation (gravité faible)
Une autorité de contrôle a reçu de nombreuses plaintes concernant la manière dont un site de vente en ligne gère le droit d'accès des personnes concernées. Selon les plaignants, le traitement de leurs demandes d'accès a pris entre 4 et 6 mois, soit bien plus de temps que le délai autorisé au titre du RGPD. L'autorité de contrôle mène l'enquête sur ces plaintes et constate que le site de vente en ligne répond aux demandes d'accès avec un retard maximal de trois mois dans 5 % des cas. Au total, le site de vente en ligne a reçu environ 1 000 demandes d'accès par an et a confirmé que 950 d'entre elles ont été traitées dans les délais. Par ailleurs, le site de vente en ligne a mis en place des politiques visant à garantir que toutes les demandes d'accès sont traitées correctement et dans leur intégralité. Néanmoins, l'autorité de contrôle a conclu que le site de vente en ligne avait enfreint l'article 12, paragraphe 3, du RGPD, et a décidé d'infliger une amende.

*Lors du calcul du montant de l'amende à infliger, l'autorité de contrôle a été chargée d'évaluer la gravité de la violation dans ce cas d'espèce. Tout d'abord, l'autorité de contrôle a noté qu'une violation de l'article 12 du RGPD **figure parmi les violations de l'article 83, paragraphe 5, du RGPD**, et qu'elle tombe donc sous le coup du niveau supérieur de l'article 83 du RGPD. Ensuite, l'autorité de contrôle a apprécié les circonstances du cas d'espèce. À cet égard, l'autorité de contrôle a rigoureusement analysé la **nature de la violation**. Bien que le droit d'accès aux données à caractère personnel dans des délais appropriés soit l'une des pierres angulaires des droits des personnes concernées, l'autorité de contrôle a estimé que la violation était d'une gravité limitée à cet égard, étant donné que toutes les demandes avaient, au bout du compte, été traitées avec un retard limité. En ce qui concerne la **finalité du traitement**, l'autorité de contrôle a constaté que le traitement des données à caractère personnel ne constituait pas l'activité principale du site de vente en ligne, mais qu'il s'agissait tout de même d'une activité auxiliaire importante nécessaire à la réalisation de son objectif de vente de biens en ligne. L'autorité de contrôle a considéré que ce dernier état de fait rendait la violation plus grave. Par ailleurs, le **niveau de dommage** subi par les personnes concernées a été jugé minime, car toutes les demandes d'accès avaient été traitées dans un délai de six mois.*

*Compte tenu de tout ce qui précède (nature de la violation, finalité du traitement et niveau de dommage), l'autorité de contrôle conclut qu'il y a lieu de considérer la violation comme étant de **gravité faible**. L'autorité de contrôle fixera un montant de départ pour le calcul ultérieur compris entre 0 et 10 % du montant maximal légal prévu à l'article 83, paragraphe 5, du RGPD.*

4.3 – Prise en considération du chiffre d'affaires de l'entreprise en vue de l'imposition d'une amende effective, dissuasive et proportionnée

63. Le RGPD exige de chaque autorité de contrôle qu'elle veille à ce que les amendes administratives imposées soient effectives, proportionnées et dissuasives dans chaque cas d'espèce (article 83, paragraphe 1, du RGPD). L'application de ces principes prévus par le droit de l'Union peut avoir de profondes conséquences dans les cas individuels, étant donné que les montants de départ proposés par le RGPD pour le calcul des amendes administratives s'appliquent tant aux microentreprises qu'aux firmes multinationales. De manière à imposer une amende effective, proportionnée et dissuasive en tout état de cause, les autorités de contrôle sont censées ajuster les amendes administratives tout en restant dans la fourchette prévue jusqu'au montant maximal légal. Cela peut conduire à des majorations ou des minorations significatives de l'amende, selon les circonstances du cas d'espèce.

64. L'EDPB part du principe qu'il est équitable de tenir compte de la taille de l'entreprise pour établir les montants de départ indiqués ci-dessous et, dès lors, prend le chiffre d'affaires de l'entreprise en considération[28]. L'EDPB observe les exigences énoncées à l'article 83 du RGPD, le RGPD dans son ensemble ainsi que la jurisprudence constante de la CJUE selon laquelle le chiffre d'affaires d'une entreprise peut constituer une indication de la taille et de la puissance économique de ladite entreprise[29]. Néanmoins, cette prise en considération du chiffre d'affaires ne permet pas à l'autorité de contrôle de se soustraire à sa responsabilité d'examiner le caractère effectif, dissuasif et proportionné de l'amende à la fin du calcul (voir chapitre 7). Ce dernier point s'applique à toutes les circonstances du cas d'espèce, y compris, par exemple, l'accumulation de violations multiples, les majorations et minorations au titre des circonstances aggravantes et atténuantes et du contexte financier/socioéconomique. Il incombe cependant à l'autorité de contrôle de s'assurer que les mêmes circonstances ne sont pas comptabilisées deux fois. Plus particulièrement, les autorités de contrôle ne devraient pas, en vertu du chapitre 7, réitérer les majorations ou minorations par rapport au chiffre d'affaires de l'entreprise, mais plutôt revoir leur fixation du montant de départ adéquat.

65. Pour les motifs exposés précédemment, l'autorité de contrôle peut envisager d'ajuster le montant de départ en fonction de la gravité de la violation dans les cas où cette violation est commise par une entreprise dont le chiffre d'affaires annuel est inférieur ou égal à 2 millions d'EUR, à 10 millions d'EUR ou à 50 millions d'EUR[30].

- **Pour les entreprises dont le chiffre d'affaires annuel est ≤ 2 millions d'EUR**, les autorités de contrôle peuvent envisager de procéder aux calculs sur la base d'une somme comprise entre 0,2 % et 0,4 % du montant de départ fixé.

[28] Voir également la décision contraignante 1/2021 de l'EDPB, points 411 et 412: «[Dans la mesure où] le chiffre d'affaires d'une entreprise n'est pas exclusivement pertinent pour la détermination du montant maximal de l'amende, conformément à l'article 83, paragraphes 4 à 6, du RGPD, mais qu'il peut être pris en considération [en tant qu'élément pertinent parmi d'autres] pour le calcul de l'amende proprement dite, afin de garantir que l'amende soit effective, proportionnée et dissuasive, conformément à l'article 83, paragraphe 1, du RGPD.» La détermination du chiffre d'affaires de l'entreprise en question est abordée plus en détail au chapitre 6.2 des présentes lignes directrices.

[29] C'est ce qui ressort de l'arrêt du Tribunal dans l'affaire T-25/06, *Alliance One International, Inc./Commission européenne*, point 211, avec mention faite à d'autres jurisprudences, par exemple dans l'affaire T-9/99, *HFB e.a./Commission*, points 528 et 529, et l'affaire T-175/05, *Akzo Nobel e.a./Commission*, point 114.

[30] Ces chiffres d'affaires sont fondés sur la recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises. Pour déterminer les montants de départ, l'EDPB s'appuie sur le seul chiffre d'affaires annuel de l'entreprise (voir chapitre 6 ci-dessous).

- **Pour les entreprises dont le chiffre d'affaires annuel est compris entre 2 et 10 millions d'EUR**, les autorités de contrôle peuvent envisager de procéder aux calculs sur la base d'une somme comprise entre 0,3 % et 2 % du montant de départ fixé.

- **Pour les entreprises dont le chiffre d'affaires annuel est compris entre 10 et 50 millions d'EUR**, les autorités de contrôle peuvent envisager de procéder aux calculs sur la base d'une somme comprise entre 1,5 % et 10 % du montant de départ fixé.

66. Pour les mêmes motifs, l'autorité de contrôle peut envisager d'ajuster le montant de départ en fonction de la gravité de la violation dans les cas où cette violation est commise par une entreprise dont le chiffre d'affaires annuel est inférieur ou égal à 100 millions d'EUR, à 250 millions d'EUR ou à 500 millions d'EUR[31].

- **Pour les entreprises dont le chiffre d'affaires annuel est compris entre 50 et 100 millions d'EUR**, les autorités de contrôle peuvent envisager de procéder aux calculs sur la base d'une somme comprise entre 8 % et 20 % du montant de départ fixé.

- **Pour les entreprises dont le chiffre d'affaires annuel est compris entre 100 et 250 millions d'EUR**, les autorités de contrôle peuvent envisager de procéder aux calculs sur la base d'une somme comprise entre 15 % et 50 % du montant de départ fixé.

- **Pour les entreprises dont le chiffre d'affaires annuel est compris entre 250 et 500 millions d'EUR**, les autorités de contrôle peuvent envisager de procéder aux calculs sur la base d'une somme comprise entre 40 % et 100 % du montant de départ fixé.

- **Pour les entreprises dont le chiffre d'affaires annuel est supérieur à 500 millions d'euros**, les autorités de contrôle peuvent envisager de procéder sans ajuster le montant de départ fixé. En effet, ces entreprises dépasseront le montant maximal légal fixe et, de ce fait, la taille de l'entreprise est déjà prise en considération dans le montant maximal légal évolutif utilisé pour fixer le montant de départ pour le calcul ultérieur sur la base de l'appréciation de la gravité de la violation.

67. En règle générale, plus le chiffre d'affaires de l'entreprise est élevé au sein du niveau applicable, plus le montant de départ est susceptible de l'être également. Ce dernier point est particulièrement vrai pour les entreprises les plus grandes, pour lesquelles la fourchette des montants de départ est la plus large.

68. Qui plus est, l'autorité de contrôle n'est aucunement tenue de procéder à cet ajustement s'il n'est pas nécessaire, en ce qui concerne le caractère effectif, dissuasif et proportionné de l'amende, d'ajuster le montant initial de cette dernière.

69. Il y a lieu de rappeler que ces chiffres représentent les montants de départ d'un calcul ultérieur, et non des montants fixes (étiquettes de prix) pour les violations des dispositions du RGPD. L'autorité de contrôle peut, à sa discrétion, recourir à l'ensemble de la fourchette des amendes, de n'importe quel montant jusqu'au montant maximal légal, en veillant à ce que l'amende soit adaptée aux circonstances du cas d'espèce, comme l'exige la Cour de justice en cas d'utilisation d'un montant de départ abstrait.

Exemple 6a – Fixation des montants de départ pour le calcul ultérieur
Une chaîne de supermarchés dont le chiffre d'affaires s'élève à 450 millions d'EUR a enfreint l'article 12 du RGPD. L'autorité de contrôle, sur la base d'une analyse minutieuse des circonstances

[31] Ces chiffres sont ajoutés pour combler l'écart entre le seuil le plus élevé fixé au paragraphe précédent et le seuil de chiffre d'affaires fixé à l'article 83, paragraphes 4 à 6, du RGPD.

du cas d'espèce, a estimé que la violation était de gravité faible. Dans le but de fixer le montant de départ du calcul ultérieur, l'autorité de contrôle a d'abord constaté que la violation de l'article 12 du RGPD figurait à l'article 83, paragraphe 5, point b), du RGPD et que, sur la base du chiffre d'affaires de l'entreprise (450 millions d'EUR), un montant maximal légal de 20 millions d'EUR s'appliquait.

En fonction du niveau de gravité déterminé par l'autorité de contrôle (faible), un montant de départ compris entre 0 et 2 millions d'EUR devrait être envisagé (entre 0 et 10 % du montant maximal légal applicable, voir le point 60 ci-dessus).

L'autorité de contrôle est d'avis qu'un ajustement allant jusqu'à 90 % du montant de départ est justifié du fait de la taille de l'entreprise, dont le chiffre d'affaires atteint 450 millions d'EUR. Ce montant constitue la base d'un calcul ultérieur qui devrait aboutir à un montant final n'excédant pas le montant maximal légal applicable de 20 millions d'EUR.

Exemple 6b – Fixation des montants de départ pour le calcul ultérieur
L'autorité de contrôle constate qu'une jeune entreprise ayant développé une application de rencontre, dont le chiffre d'affaires s'élève à 500 000 EUR, a vendu les données à caractère personnel sensibles de ses clients à plusieurs courtiers en données à des fins d'analyse, enfreignant ce faisant l'article 5, paragraphe 1, point a), et l'article 9, du RGPD. L'autorité de contrôle, sur la base d'une analyse minutieuse des circonstances du cas d'espèce, a estimé que la violation était de gravité élevée. Dans le but de fixer le montant de départ du calcul ultérieur, l'autorité de contrôle a d'abord constaté que la violation des articles 5 et 9 du RGPD figurait à l'article 83, paragraphe 5, point a), du RGPD et que, sur la base du chiffre d'affaires de l'entreprise (500 000 EUR), un montant maximal légal de 20 millions d'EUR s'appliquait.

En fonction du niveau de gravité déterminé par l'autorité de contrôle (élevée), un montant de départ compris entre 4 et 20 millions d'EUR devrait être envisagé (entre 20 et 100 % du montant maximal légal applicable, voir le paragraphe 60 ci-dessus).

L'autorité de contrôle est d'avis qu'un ajustement allant jusqu'à 0,25 % du montant de départ est justifié du fait de la taille de l'entreprise, dont le chiffre d'affaires est de 500 000 EUR. Ce montant constitue la base d'un calcul ultérieur qui devrait aboutir à un montant final n'excédant pas le montant maximal applicable de 20 millions d'EUR.

CHAPITRE 5 – CIRCONSTANCES AGGRAVANTES ET ATTÉNUANTES

5.1 – Définition des facteurs aggravants et atténuants

70. Conformément à la structure du RGPD, après avoir évalué la nature, la gravité et la durée de la violation de même que son caractère délibéré ou négligent et les catégories de données à caractère personnel concernées, l'autorité de contrôle doit tenir compte des autres facteurs aggravants et atténuants énumérés à l'article 83, paragraphe 2, du RGPD.

71. En ce qui concerne l'appréciation de ces facteurs, la majoration ou la minoration d'une amende ne saurait être prédéterminée au moyen de tableaux ou de pourcentages. Il convient de rappeler que la quantification

effective de l'amende sera fonction de tous les éléments recueillis dans le cadre de l'enquête et d'autres considérations également liées à l'expérience de l'autorité de contrôle en matière d'imposition d'amendes.

72. Par souci de clarté, il y a lieu de souligner que chaque critère exposé à l'article 83, paragraphe 2, du RGPD (qu'il soit évalué au titre du chapitre 4 ou du présent chapitre) ne doit être pris en considération qu'une seule fois dans l'appréciation globale au regard de l'article 83, paragraphe 2, du RGPD.

5.2 – Mesures prises par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées

73. La première étape pour déterminer si des circonstances aggravantes ou atténuantes entourent le cas d'espèce consiste à procéder à un examen au regard de l'article 83, paragraphe 2, point c), qui concerne «toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées».

74. Comme le rappellent les lignes directrices WP 253, les responsables du traitement et les sous-traitants sont déjà tenus de «mettre en œuvre les mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté au risque, d'effectuer des analyses d'impact relatives à la protection des données et d'atténuer les risques pour les droits et les libertés des personnes résultant du traitement des données à caractère personnel». Toutefois, lorsqu'une violation a lieu, le responsable du traitement ou le sous-traitant «devrait faire tout ce qui est en son pouvoir pour réduire les conséquences de la violation pour la personne concernée»[32].

75. L'adoption de mesures adéquates en vue d'atténuer le dommage subi par les personnes concernées peut être vue comme un facteur atténuant, entraînant une minoration de l'amende.

76. Les mesures adoptées doivent être plus particulièrement évaluées au regard de leur caractère opportun, c'est-à-dire le moment où elles sont mises en œuvre par le responsable du traitement ou le sous-traitant, et de leur efficacité. En ce sens, les mesures instaurées spontanément avant que le responsable du traitement ou le sous-traitant n'ait connaissance de l'ouverture de l'enquête de l'autorité de contrôle sont davantage de nature à être jugées comme un facteur atténuant que les mesures mises en place après la prise de connaissance de l'ouverture de l'enquête.

5.3 – Degré de responsabilité du responsable du traitement ou du sous-traitant

77. Dans le respect de l'article 83, paragraphe 2, point d), du RGPD, le degré de responsabilité du responsable du traitement ou du sous-traitant devra être évalué, compte tenu des mesures qu'ils ont mises en œuvre en vertu des articles 25 et 32 du RGPD. Conformément aux lignes directrices WP 253 «la question à laquelle l'autorité de contrôle doit répondre est de savoir dans quelle mesure le responsable du traitement "a fait ce qui pouvait être attendu de lui" compte tenu de la nature, de la finalité ou de l'ampleur du traitement considéré à la lumière des obligations qui lui incombent en vertu du règlement[33].»

78. Plus particulièrement, concernant ce critère, il y a lieu d'apprécier le risque résiduel pour les libertés et les droits des personnes concernées, l'atteinte portée aux personnes concernées et le dommage persistant après l'adoption des mesures par le responsable du traitement, ainsi que le degré de robustesse des mesures adoptées en application des articles 25 et 32 du RGPD.

[32] Lignes directrices WP 253, p. 12.
[33] Ibidem, p. 13.

79. À cet égard, l'autorité de contrôle peut également chercher à savoir si les données en cause étaient directement identifiables et/ou disponibles, sans protections techniques[34]. Néanmoins, il ne faut pas oublier que l'existence d'une telle protection ne constitue pas nécessairement un facteur atténuant (voir le point 82 ci-dessous). Cela dépendra de l'ensemble des circonstances du cas d'espèce.

80. Afin d'évaluer correctement les éléments susmentionnés, l'autorité de contrôle devrait prendre en considération toute documentation utile remise par le responsable du traitement ou le sous-traitant, par exemple dans le cadre de l'exercice de leurs droits de défense. Plus particulièrement, cette documentation pourrait fournir des preuves en ce qui concerne la date d'adoption des mesures et la manière dont elles ont été mises en œuvre, l'existence d'interactions entre le responsable du traitement et le sous-traitant (le cas échéant) ou l'existence d'un contact avec le délégué à la protection des données ou les personnes concernées (le cas échéant).

81. Compte tenu du fait que, par comparaison avec la directive 95/46/CE, le RGPD responsabilise beaucoup plus le responsable du traitement ou le sous-traitant[35], il est vraisemblable que le degré de responsabilité de ces derniers soit réputé être un facteur aggravant ou neutre. Ce n'est que dans des circonstances exceptionnelles, lorsque le responsable du traitement ou le sous-traitant est allé au-delà des obligations qui lui sont imposées, que ce degré de responsabilité sera considéré comme un facteur atténuant.

5.4 – Violations commises précédemment par le responsable du traitement ou le sous-traitant

82. On entend par «violations commises précédemment» des violations qui ont déjà été constatées avant que la décision ne soit publiée. En cas de coopération au titre du chapitre VII du RGPD, les violations commises précédemment sont celles qui ont déjà été constatées avant la publication du projet de décision (au sens de l'article 60 du RGPD).

83. Conformément à l'article 83, paragraphe 2, point e), du RGPD, toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant doit être prise en considération lorsqu'il s'agit de décider s'il y a lieu d'infliger une amende administrative et d'en fixer le montant. Un libellé semblable est énoncé au considérant 148 du RGPD.

5.4.1 – Appréciation temporelle

84. Pour commencer, il convient de tenir compte du moment où la violation commise précédemment a eu lieu, étant donné que plus la violation commise précédemment et la violation faisant l'objet de l'enquête actuelle sont espacées dans le temps, moins la violation antérieure est importante. Dès lors, plus la violation antérieure remonte dans le temps, moins les autorités de contrôle lui accordent d'importance. Cette appréciation est laissée à la discrétion de l'autorité de contrôle, sous réserve du respect du droit et des principes nationaux et européens applicables.

85. Néanmoins, étant donné que les violations commises il y a longtemps peuvent encore être pertinentes pour l'évaluation des «antécédents» du responsable du traitement ou du sous-traitant, il n'y a pas lieu de fixer des délais de prescription fixes à cette fin. Certaines législations nationales empêchent cependant l'autorité de contrôle de prendre en considération des violations commises précédemment après une période

[34] Ibidem, p. 14 et 15.
[35] Ibidem, p. 13.

déterminée. De même, certaines législations nationales imposent une obligation de suppression des données après un certain temps, empêchant ainsi les autorités de contrôle de tenir compte de ces antécédents.

86. Pour cette même raison, il convient de noter que les violations du RGPD devront être considérées comme plus pertinentes que les violations de dispositions nationales adoptées pour la transposition de la directive 95/46/CE (si la législation nationale permet à l'autorité de contrôle de tenir compte de ces violations), puisqu'elles seront plus récentes.

5.4.2 – Objet

87. Aux fins de l'article 83, paragraphe 2, point e), du RGPD, les violations commises précédemment portant sur le même objet ou sur un objet différent de celui visé par l'enquête peuvent être considérées comme «pertinentes».

88. Même si toutes les violations commises précédemment peuvent fournir une indication sur le comportement général du responsable du traitement ou du sous-traitant en ce qui concerne le respect du RGPD, les violations portant sur le même objet doivent être réputées plus importantes, car elles sont plus proches de la violation faisant l'objet de l'enquête, surtout lorsque le responsable du traitement ou le sous-traitant s'est déjà rendu coupable de la même violation (récidives). Ainsi, les violations portant sur le même objet doivent être vues comme plus pertinentes que les violations antérieures portant sur un sujet différent.

89. Par exemple, le fait que le responsable du traitement ou le sous-traitant n'ait pas, par le passé, répondu aux personnes concernées exerçant leurs droits dans les délais prévus doit être considéré comme plus pertinent lorsque la violation évaluée a également trait à l'absence de réponse à une personne concernée exerçant ses droits que lorsqu'elle porte sur une violation de données à caractère personnel.

90. Malgré cela, il convient de tenir dûment compte des violations commises précédemment portant sur un autre sujet, mais commises de la même manière, car elles peuvent révéler des problèmes persistants au sein de l'organisation du responsable du traitement ou du sous-traitant. Tel serait le cas, par exemple, si des violations avaient lieu en raison du mépris manifesté envers les avis formulés par le délégué à la protection des données.

5.4.3 – Autres considérations

91. Lorsqu'elles tiennent compte d'une violation antérieure des dispositions nationales adoptées pour transposer la directive 95/46/CE, les autorités de contrôle doivent garder à l'esprit le fait que les exigences de la directive et du RGPD peuvent différer (si la législation nationale permet à l'autorité de contrôle de tenir compte de ces violations).

92. Lorsqu'elles apprécient la pertinence d'une violation commise précédemment, les autorités de contrôle doivent tenir compte de l'état d'avancement de la procédure au cours de laquelle la violation antérieure a été constatée (et plus particulièrement de toute mesure prise par l'autorité de contrôle ou par l'autorité judiciaire) conformément au droit national.

93. Les violations commises précédemment pourraient également être prises en considération lorsqu'elles ont été constatées par une autre autorité de contrôle en ce qui concerne le même responsable du traitement ou sous-traitant. Par exemple, l'autorité de contrôle chef de file qui évalue une violation par le biais du mécanisme de coopération (guichet unique) conformément à l'article 60 du RGPD pourrait tenir compte des violations constatées précédemment dans le cadre d'affaires locales, par une autre autorité de contrôle, en ce qui concerne le même responsable du traitement ou sous-traitant. De même, les violations constatées

précédemment par l'autorité de contrôle chef de file pourraient être prises en considération lorsqu'une autre autorité de contrôle doit traiter une plainte introduite auprès d'elle dans des affaires n'ayant qu'une incidence locale, conformément à l'article 56, paragraphe 2, du RGPD. Lorsqu'il n'y a pas d'autorité de contrôle chef de file (par exemple, lorsque le responsable du traitement ou le sous-traitant n'est pas établi dans l'Union), les autorités de contrôle pourraient aussi tenir compte des violations constatées précédemment par une autre autorité de contrôle en ce qui concerne le même responsable du traitement ou sous-traitant.

94. L'existence de violations commises précédemment peut être considérée comme un facteur aggravant dans le cadre du calcul de l'amende. L'importance accordée à ce facteur doit être déterminée selon la nature et la fréquence des violations antérieures. L'absence de violations commises précédemment ne saurait toutefois être considérée comme un facteur atténuant, étant donné que le respect du RGPD est la norme. Si aucune violation n'a été commise précédemment, ce facteur peut être réputé neutre.

5.5 – Degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs

95. L'article 83, paragraphe 2, point f), du RGPD exige de l'autorité de contrôle qu'elle tienne compte du degré de coopération établi par le responsable du traitement ou le sous-traitant avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs.

96. Avant de poursuivre l'appréciation du niveau de coopération établi par le responsable du traitement ou le sous-traitant avec l'autorité de contrôle, il y a lieu de rappeler que ledit responsable et ledit sous-traitant sont soumis à une obligation générale de coopération en vertu de l'article 31 du RGPD et que la non-coopération peut entraîner l'imposition de l'amende prévue à l'article 83, paragraphe 4, point a), du RGPD. Il convient donc de considérer que le devoir ordinaire de coopération est obligatoire et que ce facteur doit donc être réputé neutre (et non considéré comme un facteur atténuant).

97. Néanmoins, lorsque la coopération avec l'autorité de contrôle a eu pour effet de limiter ou de prévenir les retombées négatives sur les droits des personnes concernées, qui auraient pu se manifester en l'absence de coopération, l'autorité de contrôle peut estimer que cette coopération constitue un facteur atténuant au sens de l'article 83, paragraphe 2, point f), du RGPD, entraînant dès lors une minoration de l'amende. Tel peut être le cas, par exemple lorsqu'un responsable du traitement ou un sous-traitant a «réagi d'une manière particulière aux demandes de l'autorité de contrôle pendant la phase d'enquête dans ce cas spécifique, de telle sorte que les incidences sur les droits des personnes concernées ont été considérablement limitées»[36].

5.6 – Manière dont l'autorité de contrôle a eu connaissance de la violation

98. Aux termes de l'article 83, paragraphe 2, point h), du RGPD, la manière dont l'autorité de contrôle a eu connaissance de la violation peut constituer un facteur aggravant ou atténuant pertinent. Au cours de l'évaluation de ce facteur, une importance particulière peut être accordée à la question de savoir si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation de sa propre initiative, avant que l'autorité de contrôle n'en prenne connaissance, par exemple via une plainte ou au cours d'une

[36] Lignes directrices WP 253, p. 14.

enquête. Ce facteur n'est pas pertinent lorsque le responsable du traitement est soumis à des obligations de notification spécifiques (comme dans le cas de violations de données à caractère personnel conformément à l'article 33)[37]. Dans de tels cas, la notification doit être considérée comme un facteur neutre[38].

99. Lorsque l'autorité de contrôle a pris connaissance de la violation, par exemple à la suite d'une plainte ou au cours d'une enquête, cet élément devrait également, en règle générale, être considéré comme un facteur neutre. L'autorité de contrôle peut estimer qu'il s'agit d'une circonstance atténuante si le responsable du traitement ou le sous-traitant a notifié la violation de sa propre initiative, avant que l'autorité de contrôle n'en prenne connaissance.

5.7 – Respect des mesures précédemment ordonnées pour le même objet

100. L'article 83, paragraphe 2, point i), du RGPD dispose que «lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures» doit être pris en considération lorsqu'il s'agit de décider si une amende administrative doit être infligée et d'en fixer le montant.

101. Contrairement à ce que prévoit l'article 83, paragraphe 2, point e), du RGPD, cette appréciation ne se réfère qu'aux mesures que les autorités de contrôle elles-mêmes ont prises précédemment à l'égard du même responsable du traitement ou sous-traitant concernant le même objet[39].

102. À ce sujet, le responsable du traitement ou le sous-traitant peut raisonnablement s'attendre à ce que le respect des mesures précédemment ordonnées à son égard empêche qu'une violation concernant le même objet soit commise à l'avenir. Toutefois, étant donné que le respect des mesures précédemment ordonnées est une obligation qui incombe au responsable du traitement ou au sous-traitant, il ne devrait pas constituer un facteur atténuant en soi. Au contraire, il est nécessaire que le responsable du traitement ou le sous-traitant renforce son engagement en ce qui concerne l'exécution des mesures précédentes pour que ce facteur soit considéré comme constituant un facteur atténuant, par exemple en prenant des mesures complémentaires à celles ordonnées par l'autorité de contrôle.

103. Inversement, le non-respect d'une mesure correctrice ordonnée précédemment peut être considéré soit comme un facteur aggravant, soit comme une violation distincte en elle-même, conformément à l'article 83, paragraphe 5, point e), et à l'article 83, paragraphe 6, du RGPD. Il convient dès lors de veiller à ce qu'un même comportement de non-respect des mesures ne puisse donner lieu à une double sanction dudit comportement.

5.8 – Application de codes de conduite approuvés ou de mécanismes de certification approuvés

104. L'article 83, paragraphe 2, point j), du RGPD, dispose que l'application de codes de conduite approuvés en application de l'article 40 du RGPD ou de mécanismes de certification approuvés en application de l'article 42 du RGPD peut constituer un facteur pertinent.

[37] Il convient de souligner qu'une violation de données à caractère personnel ne suppose pas forcément une violation du RGPD.
[38] Cet élément est mis en évidence dans les lignes directrices WP 253, p. 15
[39] Ibidem.

105. Comme le rappellent les lignes directrices WP 253, l'application de codes de conduite en application de l'article 40 du RGPD ou de mécanismes de certification approuvés en application de l'article 42 du RGPD peut, dans certaines circonstances, constituer un facteur atténuant. D'après l'article 40, paragraphe 4, du RGPD, les codes de conduite approuvés comprendront «les mécanismes permettant à l'organisme [de contrôle] de procéder au contrôle obligatoire du respect de ses dispositions». Certaines formes de sanction de comportements non conformes peuvent passer par le programme de contrôle, conformément à l'article 41, paragraphe 4, du RGPD, et comprendre la suspension ou l'exclusion du responsable du traitement ou du sous-traitant concerné de la communauté appliquant le code en question. Bien que l'autorité de contrôle soit libre de tenir compte des sanctions imposées précédemment dans le cadre du programme d'autorégulation, les pouvoirs de l'organe de contrôle sont, en vertu de l'article 41, paragraphe 4, du RGPD, «[s]ans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente», ce qui signifie que l'autorité de contrôle n'est aucunement tenue de tenir compte des sanctions imposées par l'organe de contrôle[40].

106. En revanche, si le non-respect des codes de conduite ou des mécanismes de certification est directement lié à la violation, l'autorité de contrôle peut estimer qu'il s'agit d'une circonstance aggravante.

5.9 – Autres circonstances aggravantes et atténuantes

107. L'article 83, paragraphe 2, point k), du RGPD, donne à l'autorité de contrôle toute latitude pour prendre en considération toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce. Dans certains cas particuliers, de nombreux éléments peuvent entrer en ligne de compte, sans qu'ils puissent tous êtres codifiés ou énumérés. Ces éléments devront être pris en considération pour garantir que la sanction infligée est effective, proportionnée et dissuasive dans chaque cas d'espèce.

108. L'article 83, paragraphe 2, point k), du RGPD donne des exemples de «toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce», telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation. Cette disposition est réputée revêtir une importance fondamentale lorsqu'il s'agit d'ajuster le montant de l'amende au cas d'espèce. En ce sens, elle doit être interprétée comme un exemple du principe d'équité et de justice appliqué à ce cas d'espèce particulier.

109. Le champ d'application de cette disposition, qui est nécessairement ouvert, devrait inclure toutes les considérations motivées concernant le contexte socioéconomique dans lequel le responsable du traitement ou le sous-traitant opère, les considérations relatives au contexte juridique et les considérations concernant le contexte du marché[41].

110. Plus particulièrement, le bénéfice économique résultant de la violation pourrait constituer une circonstance aggravante s'il ressort des informations du dossier du cas d'espèce que des profits ont été réalisés à la suite de la violation du RGPD.

111. Des circonstances exceptionnelles susceptibles de modifier considérablement le contexte socioéconomique (par exemple, la déclaration d'un état d'urgence en raison d'une pandémie grave, qui pourrait modifier

[40] Ibidem.
[41] L'EDPB s'est prononcé sur cette question dans sa décision contraignante 3/2022 relative au litige soumis par l'autorité de contrôle irlandaise concernant Meta Platforms Ireland Limited et son service Facebook (article 65 du RGPD) (ci-après la «décision contraignante 3/2022 de l'EDPB»), point 368.

radicalement la manière dont les données à caractère personnel sont traitées) pourraient également être prises en considération au titre de l'article 83, paragraphe 2, point k), du RGPD.

NB: Les exemples présentés dans ce chapitre illustrent l'incidence que les circonstances aggravantes et atténuantes peuvent avoir sur le montant de l'amende. Les majorations ou minorations mentionnées dans ces cas d'espèce imaginaires ne sauraient être considérées comme constituant une jurisprudence ou des indications de pourcentages à appliquer dans des cas réels.

Exemple 7a – Pondération des circonstances aggravantes et atténuantes
Un club sportif a eu recours à des caméras dotées d'une technologie de reconnaissance faciale à l'entrée de l'un de ses locaux afin d'identifier ses clients à l'entrée. Le club de sport ayant agi en violation de l'article 9 du RGPD (traitement de données biométriques sans exception valable), l'autorité de contrôle compétente pour l'enquête concernant la violation a décidé d'imposer une amende. Compte tenu de toutes les circonstances pertinentes du cas d'espèce, l'autorité de contrôle a considéré qu'il s'agissait d'une violation de gravité élevée et, puisque le club sportif réalisait un chiffre d'affaires annuel de 150 millions d'EUR, un montant de départ de 2 millions d'EUR (échelon supérieur de la catégorie) a été jugé approprié.

Cependant, le même club sportif avait été condamné à une amende deux ans auparavant pour avoir, dans d'autres locaux, doté ses tourniquets de la technologie des empreintes digitales. L'autorité de contrôle a décidé de tenir compte de cette violation et de considérer le cas d'espèce comme une récidive [article 83, paragraphe 2, point e), du RGPD]. Ce faisant, elle a accordé de l'importance au fait que la violation concernait pratiquement le même sujet et qu'elle avait été commise deux ans auparavant seulement. En raison de ce facteur aggravant, l'autorité de contrôle a décidé de majorer l'amende dans ce cas d'espèce particulier, la portant à 2 600 000 EUR[42], sans pour autant excéder le montant maximal légal applicable de 20 millions d'EUR.

NB: Les exemples présentés dans ce chapitre illustrent l'incidence que les circonstances aggravantes et atténuantes peuvent avoir sur le montant de l'amende. Les majorations ou minorations mentionnées dans ces cas d'espèce imaginaires ne sauraient être considérées comme constituant une jurisprudence ou des indications de pourcentages à appliquer dans des cas réels.

Exemple 7b – Pondération des circonstances aggravantes et atténuantes
L'exploitant d'une plateforme de location de voitures à court terme a été victime d'une violation de données en raison de laquelle les données à caractère personnel de ses clients ont été vulnérables pendant une courte période. Compte tenu de toutes les circonstances pertinentes du cas d'espèce, l'autorité de contrôle a considéré que les manquements de l'opérateur en ce qui concerne la sécurisation de sa plateforme constituaient une violation de l'article 32 du RGPD, de gravité faible, et, le chiffre d'affaires annuel de l'opérateur étant de 255 millions d'EUR, un montant de départ de 260 000 EUR a été considéré comme approprié.

[42] Cet exemple démontre que les catégories de montants de départ ne limitent en rien la capacité des autorités de contrôle à tenir compte des circonstances aggravantes et atténuantes pour majorer ou minorer l'amende et la porter à un montant supérieur ou inférieur à ceux prévus pour ces catégories. Comme le rappelle le chapitre 4.3, ces chiffres représentent les montants de départ d'un calcul ultérieur, et non des montants fixes (étiquettes de prix) pour les violations des dispositions du RGPD. L'autorité de contrôle demeure libre de recourir à l'ensemble de la fourchette des amendes, de n'importe quel montant supérieur à 0 EUR jusqu'au montant maximal légal, en veillant à ce que l'amende soit adaptée aux circonstances du cas d'espèce.

Les données à caractère personnel compromises comprenaient des copies de permis de conduire et de cartes d'identité. De ce fait, tous les clients victimes de la violation de données se sont vus contraints de faire refaire tous ces papiers afin de limiter les risques d'usurpation d'identité. Tout en informant les personnes concernées de cet incident, l'opérateur leur a proposé de les aider à faire refaire ces papiers auprès des institutions publiques compétentes et a élaboré un système de remboursement des frais payés pour la demande. L'autorité de contrôle a considéré qu'il s'agissait de «mesures prises pour atténuer le dommage subi par les personnes concernées» [article 83, paragraphe 2, point c), du RGPD], ce qui, en tant que facteur atténuant, a motivé la minoration de l'amende. Vu le comportement proactif et l'efficacité des mesures prises par l'opérateur, l'autorité de contrôle a décidé de minorer l'amende pour la porter à 225 000 EUR[43], sans dépasser le montant maximal légal de 10 millions d'EUR.

Les exemples présentés dans ce chapitre illustrent l'incidence que les circonstances aggravantes et atténuantes peuvent avoir sur le montant de l'amende. Les majorations ou minorations mentionnées dans ces cas d'espèce imaginaires ne sauraient être considérées comme constituant une jurisprudence ou des indications de pourcentages à appliquer dans des cas réels.

Exemple 7c – Pondération des circonstances aggravantes et atténuantes
L'autorité de contrôle a constaté qu'une petite agence de notation de crédit avait enfreint plusieurs dispositions protégeant les droits des personnes concernées, notamment parce qu'elle facturait à ses clients des frais pour l'exercice de leur droit d'accès. L'agence n'a pas facturé ces frais uniquement pour les demandes visées à l'article 12, paragraphe 5, point a), du RGPD, mais pour toutes les demandes d'accès. Compte tenu de toutes les circonstances pertinentes du cas d'espèce, l'autorité de contrôle a considéré que les violations constatées étaient de gravité élevée et que, l'agence réalisant un chiffre d'affaires annuel de 35 millions d'EUR, un montant de départ de 100 000 EUR était approprié.

Néanmoins, l'autorité de contrôle a estimé que le fait que l'agence avait été en mesure de réaliser des profits du fait de cette violation constituait une circonstance aggravante [article 83, paragraphe 2, point k), du RGPD]. Afin de contrebalancer les bénéfices tirés de la violation, tout en s'assurant que l'amende reste effective, dissuasive et proportionnée dans ce cas d'espèce, l'autorité de contrôle a décidé de majorer l'amende pour la porter à 130 000 EUR, sans excéder le montant maximal légal applicable de 20 millions d'EUR.

Les exemples présentés dans ce chapitre illustrent l'incidence que les circonstances aggravantes et atténuantes peuvent avoir sur le montant de l'amende. Les majorations ou minorations mentionnées dans ces cas d'espèce imaginaires ne sauraient être considérées comme constituant une jurisprudence ou des indications de pourcentages à appliquer dans des cas réels.

Exemple 7d – Pondération des circonstances aggravantes et atténuantes
L'autorité de contrôle a constaté qu'une entreprise avait enfreint les dispositions du RGPD, notamment parce qu'elle avait vendu à des partenaires, à des fins de prospection commerciale, sa base de données contenant les données à caractère personnel de personnes qui n'avaient pas consenti à faire l'objet d'une prospection à des fins commerciales.

[43] Voir la note de bas de page précédente.

Compte tenu de toutes les circonstances pertinentes du cas d'espèce, l'autorité de contrôle a considéré que les violations constatées étaient de gravité moyenne et que, l'entreprise réalisant un chiffre d'affaires annuel de 45 millions d'EUR, un montant de départ de 150 000 EUR était approprié.

En outre, l'autorité de contrôle a jugé qu'il s'agissait d'une violation qui profitait au responsable du traitement, car le fait de ne pas avoir recueilli le consentement des personnes concernées pour le transfert de leurs données dans le but de leur envoyer de la publicité ciblée a augmenté la masse de données qu'il a pu revendre par la suite. Ainsi, l'autorité de contrôle a estimé que le fait que l'entreprise avait été en mesure de réaliser des profits du fait de cette violation constituait une circonstance aggravante [article 83, paragraphe 2, point k), du RGPD].

Afin de contrebalancer les bénéfices tirés de la violation, tout en s'assurant que l'amende reste effective, dissuasive et proportionnée dans ce cas d'espèce, l'autorité de contrôle a décidé de majorer l'amende pour la porter à 200 000 EUR, sans excéder le montant maximal légal applicable de 20 millions d'EUR.

CHAPITRE 6 – MONTANT MAXIMAL LÉGAL ET RESPONSABILITÉ DES ENTREPRISES

6.1 – Fixation du montant maximal légal

112. Comme cela a déjà été mis en évidence dans les lignes directrices WP 253, le RGPD n'attribue pas de montants fixes à des violations spécifiques. Au lieu de cela, le RGPD prévoit des montants maximaux généraux[44] et suit de la sorte la tradition générale du droit de l'Union en matière de sanctions déjà établie par d'autres actes juridiques[45].

113. Les montants prévus à l'article 83, paragraphes 4 à 6, du RGPD constituent le montant maximal légal et lesdits articles interdisent aux autorités de contrôle d'imposer des amendes dont la somme finale dépasse les montants maximaux applicables. De manière à déterminer le montant maximal légal correct, l'article 83, paragraphe 3, du RGPD[46] doit être pris en considération lorsqu'il trouve application (voir chapitre 3.1.2). Chaque autorité de contrôle doit dès lors s'assurer que ces montants maximaux ne sont pas dépassés lorsqu'elle calcule les montants des amendes sur la base des présentes lignes directrices. Selon le cas d'espèce, des montants maximaux différents peuvent se révéler pertinents.

6.1.1 – Montants maximaux fixes

114. L'article 83, paragraphes 4 à 6, du RGPD prévoit des montants fixes en principe et opère une distinction entre les violations des diverses catégories d'obligations imposées par le RGPD. Comme expliqué ci-dessus, l'article 83, paragraphe 4, du RGPD prévoit des amendes pouvant atteindre 10 millions d'EUR pour la violation des obligations énoncées dans ledit paragraphe, tandis que l'article 83, paragraphes 5 et 6, du RGPD prévoit des amendes pouvant aller jusqu'à 20 millions d'EUR pour la violation des obligations énoncées dans lesdits paragraphes.

6.1.2 – Montants maximaux évolutifs

115. Dans le cas d'une entreprise[47], la fourchette des amendes peut évoluer vers un montant maximal plus élevé calculé en fonction du chiffre d'affaires[48] . Ce montant maximal fondé sur le chiffre d'affaires est évolutif et individualisé selon l'entreprise concernée de façon à respecter les principes d'efficacité, de proportionnalité et de dissuasion.

116. Plus précisément, l'article 83, paragraphe 4, du RGPD prévoit un montant maximal de 2 % et l'article 83, paragraphes 5 et 6, un montant maximal de 4 % du chiffre d'affaires annuel total de l'entreprise réalisé au cours de l'exercice précédent. Le libellé du RGPD exige de prendre en considération le montant maximal fixe ou le montant maximal évolutif sur la base du chiffre d'affaires, «le montant le plus élevé étant retenu». En

[44] Considérant 150 du RGPD, deuxième phrase: «Le présent règlement devrait définir les violations, le montant maximal et les critères de fixation des amendes administratives dont elles sont passibles, qui devraient être fixés par l'autorité de contrôle compétente dans chaque cas d'espèce, en prenant en considération toutes les caractéristiques propres à chaque cas et compte dûment tenu, notamment, de la nature, de la gravité et de la durée de la violation et de ses conséquences, ainsi que des mesures prises pour garantir le respect des obligations découlant du règlement et pour prévenir ou atténuer les conséquences de la violation.»

[45] Plus particulièrement, l'article 23, paragraphe 2, du règlement (CE) nº 1/2003 du Conseil du 16 décembre 2002 relatif à la mise en œuvre des règles de concurrence prévues aux articles 81 et 82 du traité.

[46] Voir également la décision contraignante 1/2021 de l'EDPB, point 326.

[47] En ce qui concerne le terme «entreprise», voir le chapitre 6.2.1 des présentes lignes directrices.

[48] En ce qui concerne le terme «chiffre d'affaires», voir le chapitre 6.2.2 des présentes lignes directrices.

conséquence, ces montants maximaux fondés sur le chiffre d'affaires ne s'appliquent que s'ils dépassent le montant maximal fixe dans le cas d'espèce. Tel est le cas lorsque le chiffre d'affaires annuel total de l'entreprise réalisé au cours de l'exercice précédent s'élève à plus de 500 millions d'EUR[49].

Exemple 8a – Montant maximal évolutif

Une agence d'évaluation du crédit collecte et revend toutes les données relatives à la solvabilité de l'ensemble des citoyens de l'UE à des agences de publicité et à des entreprises de vente au détail sans aucune base juridique. Le chiffre d'affaires annuel mondial de l'agence pour l'exercice précédent s'élève à 3 milliards d'EUR. En l'espèce, l'agence d'évaluation du crédit a notamment enfreint l'article 6, ce qui est passible d'une amende en vertu de l'article 83, paragraphe 5, du RGPD. Le montant maximal fixe s'élèverait à 20 millions d'EUR. Le montant maximal évolutif s'élèverait à 120 millions d'EUR (4 % de 3 milliards d'EUR). L'amende peut aller jusqu'à 120 millions d'EUR car ce montant maximal évolutif est supérieur au montant maximal fixe de 20 millions d'EUR. Dès lors, l'amende peut dépasser le montant maximal fixe de 20 millions d'EUR, mais ne doit pas excéder le montant maximal évolutif applicable de 120 millions d'EUR.

Exemple 8b – Montant maximal fixe

Un détaillant de lunettes de soleil exploite un site de vente en ligne permettant aux clients de passer leurs commandes. Par le biais du formulaire de commande, le détaillant traite également des données à caractère personnel, y compris des coordonnées bancaires. Le détaillant ne prévoit aucun chiffrement de transport adéquat à l'aide du protocole https, de sorte que des tiers sont potentiellement en mesure d'intercepter les données à caractère personnel durant la transaction. Le détaillant enfreint l'article 32, paragraphe 1, du RGPD, et peut encourir une amende en application de l'article 83, paragraphe 4, du RGPD. Le chiffre d'affaires annuel mondial du détaillant pour l'exercice précédent s'élève à 450 millions d'EUR. En l'espèce, le montant maximal fixe de 10 millions d'EUR est plus élevé que le montant maximal évolutif de 9 millions d'EUR (= 2 % de 450 millions d'EUR). C'est donc le montant maximal fixe de 10 millions d'EUR qui est retenu. Par conséquent, l'amende ne doit pas dépasser le montant maximal légal de 10 millions d'EUR.

Exemple 8c – Responsables du traitement et sous-traitants qui ne sont pas des entreprises

Une municipalité dispose d'un système en ligne qui permet à ses citoyens de prendre des rendez-vous, par exemple pour demander un passeport ou un certificat de mariage. La municipalité est l'unique responsable du traitement de ce système en ligne. Malheureusement, il s'est avéré que le système transmettait également, en permanence, les données collectées aux serveurs externes d'un sous-traitant établi dans un pays tiers assurant un niveau de protection inadéquat, où ces données sont stockées. Aucune garantie appropriée n'est mise en place en ce qui concerne le transfert vers un pays tiers. À l'exception du transfert, les données sont collectées et traitées sur la base d'un consentement valable. La municipalité a enfreint l'article 44 du RGPD en transférant des catégories particulières de données à caractère personnel vers un pays tiers assurant un niveau de protection inadéquat, sans aucune garantie appropriée. Elle peut donc encourir une amende en vertu de l'article 83, paragraphe 5, du RGPD. Étant donné que la municipalité ne répond pas à la définition d'une entreprise, le montant maximal légal fixe s'applique. Ainsi, l'amende ne doit pas dépasser 20 millions d'EUR. Ce n'est toutefois le cas que si l'État membre dans lequel cette municipalité se trouve n'a pas établi de règles spécifiques sur la question de savoir si et dans quelle mesure des amendes administratives peuvent être infligées aux autorités et organismes publics établis dans cet État membre (article 83, paragraphe 7, du RGPD).

[49] 2 % de 500 millions d'EUR équivalent à 10 millions d'EUR (le montant maximal fixe prévu à l'article 83, paragraphe 4, du RGPD) et 4 % de 500 millions d'EUR équivalent à 20 millions d'EUR (le montant maximal fixe prévu à l'article 83, paragraphe 5, du RGPD).

6.2 – Détermination du chiffre d'affaires et de la responsabilité de l'entreprise

117. Afin de déterminer le bon chiffre d'affaires sur la base duquel le montant maximal légal peut être calculé, il est important de comprendre les concepts d'entreprise et de chiffre d'affaires tels qu'ils figurent à l'article 83, paragraphes 4 à 6, du RGPD. À cet égard, il convient d'accorder la plus grande attention aux considérants du RGPD, fournis par le législateur européen afin de guider l'interprétation du RGPD.

6.2.1 – Détermination de l'entreprise et de la responsabilité des entreprises

118. En ce qui concerne le terme «entreprise», le législateur européen apporte des précisions complémentaires. Le considérant 150 du RGPD prévoit que: «Lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne.»

119. Par conséquent, l'article 83, paragraphes 4 à 6, du RGPD, à la lumière du considérant 150, repose sur le concept d'entreprise au sens des articles 101 et 102 du TFUE[50], sans préjudice de l'article 4, point 18), du RGPD (qui définit le terme «entreprise») et de l'article 4, point 19), du RGPD (qui définit le terme «groupe d'entreprises»). Ce dernier concept est principalement utilisé au chapitre V du RGPD, dans la phrase «groupe d'entreprises engagées dans une activité économique conjointe». En outre, le terme est employé au sens général, et non dans le sens d'entité visée par une disposition ou une obligation.

120. En conséquence, dans les cas où le responsable du traitement ou le sous-traitant est (ou fait partie de) une entreprise au sens des articles 101 et 102 TFUE, le chiffre d'affaires cumulé de cette entreprise dans son ensemble peut servir afin de déterminer le montant maximal évolutif de l'amende (voir chapitre 6.2.2) et de garantir que l'amende calculée sur cette base est conforme aux principes d'efficacité, de proportionnalité et de dissuasion (article 83, paragraphe 1, du RGPD)[51].

121. La CJUE a développé une vaste jurisprudence en ce qui concerne la notion d'entreprise. Le terme «entreprise» «comprend toute entité exerçant une activité économique, indépendamment du statut juridique de cette entité et de son mode de financement»[52]. Aux fins du droit de la concurrence, les «entreprises» sont donc apparentées à des unités économiques plutôt qu'à des unités juridiques. Différentes sociétés appartenant à un même groupe peuvent constituer une unité économique et donc une entreprise au sens des articles 101 et 102 TFUE[53].

122. Conformément à la jurisprudence constante de la CJUE, le terme «entreprise» figurant aux articles 101 et 102 du TFUE peut désigner une unité économique unique (UEU), même si cette unité économique se compose de plusieurs personnes physiques ou morales. La question de savoir si plusieurs entités forment une UEU dépend en grande partie de la question de savoir si l'entité individuelle est libre dans sa capacité de prendre des décisions ou si une entité principale, à savoir la société mère, exerce une influence déterminante

[50] Comme cela a déjà été précisé dans les lignes directrices WP 253 et confirmé ultérieurement par la déclaration d'approbation 1/2018 de l'EDPB du 25 mai 2018. Voir également la décision contraignante 1/2021 de l'EDPB, point 292, et l'arrêt du tribunal régional de Bonn dans l'affaire 29 OWi 1/20, 11 novembre 2020, point 92.
[51] Voir la décision contraignante 1/2021 de l'EDPB, points 412 et 423, ainsi que les affaires C-286/13 P, *Dole food et Dole Fresh Fruit Europe/Commission européenne*, point 149 et C-189/02 P, *Dansk Rørindustri e.a./Commission*, point 258.
[52] Affaire C-41/90, *Klaus Höfner et Fritz Elser/Macrotron GmbH*, point 21. Voir aussi, par exemple, les affaires jointes C-159 et 160/91, *Poucet et Pistre/Assurances Générales de France*, point 17; l'affaire C-364/92, *SAT Fluggesellschaft mbH/Eurocontrol*, point 18; les affaires jointes C-180/98 à 184/98, *Pavlov e.a.*, point 74; et l'affaire C-138/11, *Compass-Datenbank GmbH/Republik Österreich*, point 35.
[53] Affaire C-516/15 P, *Akzo Nobel et autres/Commission*, EU:C:2009:536, point 48.

sur les autres[54]. Les critères pour déterminer si une influence est exercée reposent sur les liens économiques, juridiques et organisationnels entre la société mère et sa filiale, par exemple le montant de la participation, les liens en matière de personnel ou d'organisation, les instructions et l'existence de contrats d'entreprise[55].

123. Conformément à la doctrine relative à l'UEU, l'article 83, paragraphes 4 à 6, du RGPD suit le principe de la responsabilité directe des entreprises, qui suppose que tous les actes accomplis ou négligés par des personnes physiques autorisées à agir au nom d'entreprises sont imputables à ces dernières et sont considérés comme un acte et une violation directement commis par l'entreprise elle-même[56]. Le fait que certains employés n'aient pas respecté un code de conduite ne suffit pas à renverser cette imputation[57], qui ne peut l'être que lorsque la personne physique agit uniquement à des fins privées ou pour le compte d'un tiers, devenant ainsi elle-même un responsable du traitement distinct (c'est-à-dire que la personne physique a agi au-delà de ses attributions autorisées)[58]. Ce principe du droit de l'Union et l'étendue de la responsabilité des entreprises priment et ne doivent pas être mis à mal en les limitant aux actes de certains fonctionnaires (tels que les principaux cadres), en contradiction avec le droit national. Il importe peu de savoir quelle personne physique a agi pour le compte de quelle entité. L'autorité de contrôle et les juridictions nationales ne doivent donc pas être tenues de déterminer ou d'identifier une personne physique dans le cadre des enquêtes ou de la décision d'infliger une amende[59].

124. Dans le cas particulier où une société mère détient 100 % des parts ou presque 100 % des parts d'une filiale qui a enfreint l'article 83 du RGPD et est donc en mesure d'exercer une influence déterminante sur le comportement de cette filiale, il existe une présomption selon laquelle la société mère exerce effectivement une influence déterminante sur le comportement de sa filiale (présomption dite «*Akzo*»)[60]. Cette présomption s'applique également lorsque la société mère ne détient pas directement les parts de la totalité du capital, mais détient cette totalité indirectement par l'intermédiaire d'une ou de plusieurs filiales[61]. Par exemple, il peut exister une chaîne de filiales, au sein de laquelle une entité détient 100 % ou presque des parts d'une entité intermédiaire qui détient 100 % ou presque des parts d'une autre entité, et ainsi de suite. De même, une société mère peut détenir 100 % ou presque des parts de deux entités qui détiennent chacune

[54] Pour clarifier, la «capacité de prendre des décisions» qui doit être appréciée en vue de déterminer si une société mère exerce une influence déterminante sur d'autres membres du groupe renvoie à la capacité de prendre des décisions relatives au comportement de la filiale «sur le marché». Il s'agit d'un critère différent et entièrement distinct de l'influence qu'une société mère peut ou non exercer sur le traitement en cause et, plus particulièrement, sur la capacité de prendre des décisions en ce qui concerne «les finalités et les moyens» du traitement. Ces critères doivent être appréciés dans le cadre de tout examen de l'identité du responsable du traitement et ne sont pas pertinents pour l'évaluation de l'influence déterminante aux fins de l'établissement d'une unité économique unique.

[55] Voir l'affaire C-90/09 P, *General Química et autres/Commission*. Le principal critère pour établir cette unité est l'«influence déterminante», qui doit être déduite sur la base de preuves concrètes (liens économiques, organisationnels et juridiques). Qui plus est, il existe une présomption réfutable d'influence dans le cas d'une filiale à 100 %. Voir l'affaire C-97/08 P, *Akzo Nobel et autres/Commission* et les affaires jointes C-293/13 et 294/13 P, *Fresh Del Monte*.

[56] Voir les affaires jointes C-100/80 à 103/80, *SA Musique Diffusion française et autres/Commission*, point 97, et l'affaire C-338/00 P, *Volkswagen/Commission*, points 93 à 98.

[57] Affaire C-501/11 P, *Schindler Holding e.a./Commission*, point 114; il est donc important pour les entreprises que leur système de gestion de la conformité ne soit pas qu'une «armure de paperasse», mais qu'il soit réellement efficace dans la pratique.

[58] Voir plus particulièrement les lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD (ci-après les «lignes directrices 07/2020 de l'EDPB»), point 19.

[59] Affaire C-338/00 P, *Volkswagen/Commission*, points 97 et 98; toute législation nationale contraire est incompatible avec le RGPD et le principe d'effectivité et de proportionnalité ne doit pas être appliqué.

[60] Affaire C-97/08 P, *Akzo Nobel et autres/Commission*, points 59 et 60.

[61] Affaires T-38/05, *Agroexpansión/Commission* et C-508/11 P, *Eni/Commission*, point 48.

environ 50 % d'une entité, ce qui lui permet d'exercer une influence déterminante sur chacune de ces entités. Dans de telles circonstances, il suffit à l'autorité de contrôle de prouver que la filiale est directement ou indirectement détenue à 100 % ou presque par la société mère pour présumer, sur la base de l'expérience pratique, que la société mère exerce une influence déterminante.

125. Toutefois, la présomption *Akzo* n'est pas absolue: elle peut être renversée par d'autres éléments de preuve[62]. Pour renverser la présomption, la ou les sociétés doivent apporter des éléments de preuve relatifs aux liens organisationnels, économiques et juridiques entre la filiale et sa société mère, qui sont de nature à démontrer que la société mère et la filiale ne constituent pas une UEU, bien qu'elles détiennent 100 % ou presque des parts. Afin d'établir si une filiale en elle-même agit de façon autonome, il convient de prendre en considération l'ensemble des éléments pertinents relatifs à ces liens qui unissent cette filiale à la société mère, lesquels peuvent varier selon les cas et ne sauraient donc faire l'objet d'une énumération exhaustive.

126. Si, en revanche, la société mère ne détient pas la totalité ou la quasi-totalité du capital, des faits supplémentaires doivent être étayés par des éléments de preuve par l'autorité de contrôle pour conclure à l'existence d'une UEU. Dans ce cas, l'autorité de contrôle doit démontrer non seulement que la société mère a la capacité d'exercer une influence déterminante sur sa filiale, mais aussi qu'elle a effectivement exercé ladite influence, de sorte qu'elle peut intervenir à tout moment dans la liberté de choix de la filiale et déterminer son comportement. La nature ou le type d'instruction n'est pas pertinent lorsqu'il s'agit de déterminer l'influence de la société mère.

127. L'amende est imposée[63] au(x) responsable(s) du traitement ou sous-traitant(s) (conjoints) et l'autorité de contrôle compétente a la possibilité de tenir la société mère conjointement et solidairement responsable[64] du paiement de l'amende.

6.2.2 – Détermination du chiffre d'affaires

128. Le chiffre d'affaires ressort des comptes annuels d'une entreprise, qui sont établis par rapport à son exercice financier et donnent une vue d'ensemble de l'exercice qui s'est écoulé d'une entreprise ou d'un groupe d'entreprises (comptes consolidés). Le chiffre d'affaires est défini comme la somme de tous les biens et services vendus. On entend par «chiffre d'affaires net» le montant résultant de la vente de produits et de la prestation de services, déduction faite des réductions sur ventes, de la taxe sur la valeur ajoutée (TVA) et d'autres impôts directement liés au chiffre d'affaires[65].

---

[62] Voir, entre autres, l'affaire C-595/18 P, *The Goldman Sachs Group/Commission*, ECLI: EU: C: 2021:73, point 32, citant l'affaire C-611/18 P, *Pirelli & C./Commission*, arrêt non publié, point 68, ainsi que jurisprudence citée.

[63] La décision infligeant l'amende est adressée et délivrée au(x) responsable(s) du traitement ou sous-traitant(s) en tant qu'auteurs de la violation et peut également être adressée et délivrée à d'autres entités juridiques de l'UEU qui sont conjointement et solidairement responsables du paiement de l'amende.

[64] Décision contraignante 1/2021 de l'EDPB, point 290.

[65] Voir par exemple, article 2, paragraphe 5, de la directive 2013/34/UE du Parlement européen et du Conseil du 26 juin 2013 relative aux états financiers annuels, aux états financiers consolidés et aux rapports y afférents de certaines formes d'entreprises, modifiant la directive 2006/43/CE du Parlement européen et du Conseil et abrogeant les directives 78/660/CEE et 83/349/CEE du Conseil (ci-après la «directive 2013/34/UE»), qui s'applique aux entreprises à responsabilité limitée, ou législation applicable similaire ainsi que l'article 5, paragraphe 1, du règlement (CE) nº 139/2004 du Conseil relatif au contrôle des concentrations entre entreprises (ci-après le «règlement CE sur les concentrations»).

129. Le chiffre d'affaires est tiré de la présentation du compte de résultat[66]. Le chiffre d'affaires net comprend les recettes tirées de la vente, de la location et du leasing de produits et les recettes provenant de la vente de services, après déductions des réductions sur les ventes (par exemple, les rabais, les remises) et de la TVA.

130. Si l'entreprise est soumise à l'obligation d'établir des comptes annuels consolidés[67], ces comptes consolidés de la société mère à la tête du groupe sont pertinents pour refléter le chiffre d'affaires cumulé de l'entreprise[68]. Si ces comptes n'existent pas, il convient d'obtenir et d'utiliser tout autre document susceptible de permettre de déduire le chiffre d'affaires annuel mondial de l'entreprise au cours de l'exercice en cause.

131. L'article 83, paragraphes 4 à 6, du RGPD, dispose que le chiffre d'affaires annuel mondial total de l'exercice précédent doit être utilisé. En ce qui concerne la question de savoir à quel événement le terme «précédent» se rapporte, la jurisprudence de la CJUE en matière de droit de la concurrence doit également être appliquée pour les amendes prévues par le RGPD, de sorte que l'événement pertinent est la décision d'infliger une amende émise par l'autorité de contrôle, et non le moment de la violation ni de la décision de justice[69]. En cas de traitement transfrontière, la décision d'infliger une amende pertinente n'est pas le projet de décision, mais la décision finale publiée par l'autorité de contrôle chef de file[70]. Lorsque le projet de décision entre dans le processus de consensus prévu à l'article 60 vers la fin d'une année civile, de sorte qu'il est peu probable que la décision finale soit adoptée au cours de cette même année, l'autorité de contrôle chef de file calculera toute amende proposée sur la base des informations financières les plus récentes disponibles à la date à laquelle le projet de décision est transmis aux autorités de contrôle concernées pour recueillir leurs avis. Ces informations seront ensuite mises à jour, le cas échéant, avant la finalisation et l'adoption de la décision nationale finale par l'autorité de contrôle chef de file.

CHAPITRE 7 – CARACTÈRE EFFECTIF, PROPORTIONNÉ ET DISSUASIF

132. Il est exigé que l'amende administrative imposée pour les violations du RGPD visées à l'article 83, paragraphes 4 à 6, soit, dans chaque cas d'espèce, effective, proportionnée et dissuasive. En d'autres termes, le montant de l'amende imposée est adapté à la violation commise dans son contexte spécifique. L'EDPB estime qu'il revient aux autorités de contrôle de vérifier si le montant de l'amende répond à ces exigences ou si d'autres ajustements du montant sont nécessaires.

133. Comme expliqué au chapitre 4, l'appréciation réalisée au titre de ce chapitre couvre l'intégralité de l'amende imposée et toutes les circonstances du cas d'espèce, y compris, par exemple, l'accumulation de violations multiples, les majorations et les minorations au titre des circonstances aggravantes et atténuantes et du contexte financier/socioéconomique. Il incombe cependant à l'autorité de contrôle de s'assurer que les mêmes circonstances ne sont pas comptabilisées deux fois.

134. Si ces ajustements justifient une majoration de l'amende, cette majoration ne peut (par définition) dépasser le montant maximal légal fixé au chapitre 6 ci-dessus.

---

[66] Voir, par exemple, les annexes V ou VI visées à l'article 13, paragraphe 1, de la directive 2013/34/UE sous la rubrique «chiffre d'affaires net», ou législation applicable similaire.
[67] Voir, par exemple, les articles 21 et suivants de la directive 2013/34/UE, ou législation applicable similaire.
[68] C-58/12 P *Groupe Gascogne SA/Commission européenne*, EU:C:2013:770, points 54 et 55.
[69] Arrêt du tribunal régional LG Bonn dans l'affaire 29 OWi 1/20, 11 novembre 2020, point 95, renvoyant à l'affaire C-637/13 P, *Badezimmerkartell Laufen Austria*, point 49 et l'affaire C-408/12 P, *YKK e.a.*, point 90.
[70] Décision contraignante 1/2021 de l'EDPB, point 298.

7.1 – Caractère effectif

135. Généralement parlant, une amende peut être considérée comme effective si elle permet d'atteindre les objectifs pour lesquels elle a été imposée. Il peut s'agir de restaurer le respect des règles, de sanctionner un comportement illicite, ou les deux[71]. Qui plus est, le considérant 148 du RGPD souligne que les amendes administratives doivent être imposées «[a]fin de renforcer l'application des règles du présent règlement». Le montant de l'amende infligée sur la base des présentes lignes directrices devrait donc être suffisant pour atteindre ces objectifs.

136. Ainsi que l'exige l'article 83, paragraphe 2, du RGPD, l'autorité de contrôle doit évaluer le caractère effectif de l'amende dans chaque cas d'espèce. Pour ce faire, il convient de tenir dûment compte des circonstances du cas d'espèce, et en particulier de l'appréciation réalisée ci-dessus[72], sans oublier que l'amende doit également être proportionnée et dissuasive, comme mis en évidence ci-dessous.

7.2.1 – Proportionnalité

137. Le principe de proportionnalité exige que les mesures adoptées ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation des objectifs légitimes poursuivis par la réglementation en cause. Lorsqu'un choix s'offre entre plusieurs mesures appropriées, il convient de recourir à la moins contraignante et les inconvénients causés ne doivent pas être démesurés par rapport aux buts visés[73].

138. Il s'ensuit que les montants des amendes ne doivent pas être démesurés par rapport aux buts visés (c'est-à-dire par rapport au respect des règles de protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données), et que le montant de l'amende doit être proportionné à la violation, appréciée dans son ensemble, en tenant compte, notamment, de la gravité de celle-ci[74].

139. L'autorité de contrôle vérifie dès lors que le montant de l'amende est **proportionné** aussi bien par rapport à la gravité de la violation qu'à la taille de l'entreprise à laquelle appartient l'entité ayant commis la violation[75], et que l'amende infligée n'excède donc pas ce qui est nécessaire pour atteindre les objectifs poursuivis par le RGPD.

140. Il peut découler, dans des circonstances particulières, du principe de proportionnalité que l'autorité de contrôle envisage, conformément au droit national, de minorer davantage l'amende sur la base du principe de l'incapacité de payer. Une telle minoration exige des circonstances exceptionnelles. Conformément aux

[71] Lignes directrices WP 253, p. 6.
[72] Comme le souligne également le considérant 148 du RGPD: «[il convient de tenir dûment compte de] la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante.»
[73] Affaire T-704/14, *Marine Harvest/Commission*, point 580, renvoyant à l'affaire T-332/09, *Electrabel/Commission*, point 279.
[74] Ibidem.
[75] Voir, à cet effet, l'affaire C-387/97, *Commission/Grèce*, point 90, et l'affaire C-278/01, *Commission/Espagne*, point 41, dans lesquelles l'amende devait être «d'une part, adaptée aux circonstances et, d'autre part, proportionnée au manquement constaté ainsi qu'à la capacité de paiement de l'État membre concerné».

lignes directrices de la Commission européenne pour le calcul des amendes[76], des preuves objectives doivent indiquer que l'imposition d'une amende mettrait irrémédiablement en danger la viabilité économique de l'entreprise concernée. Par ailleurs, les risques doivent être analysés en tenant compte du contexte social et économique particulier.

a) **Viabilité économique:** L'entreprise est tenue de communiquer des données financières détaillées (pour les cinq dernières années ainsi que des projections pour l'année en cours et les deux années suivantes) pour permettre à l'autorité de contrôle d'étudier l'évolution probable de facteurs clés tels que la solvabilité, la liquidité et la rentabilité. Les juridictions européennes ont déclaré que le simple fait qu'une entreprise se trouve dans une mauvaise situation financière, ou s'y trouvera après une amende élevée, ne répond pas à cette exigence car «la reconnaissance de pareille obligation reviendrait en effet, à procurer un avantage concurrentiel injustifié aux entreprises les moins adaptées aux conditions du marché»[77]. L'évaluation de la capacité de l'entreprise à payer l'amende prend également en considération les éventuels plans de restructuration et l'état d'avancement de leur mise en œuvre, les relations avec les partenaires/établissements financiers externes tels que les banques et les relations avec les actionnaires[78].

b) **Preuve de la perte de valeur:** Une minoration de l'amende ne peut être accordée que si l'imposition de l'amende mettrait en péril la viabilité économique d'une entreprise et conduirait à une perte de la valeur totale ou d'une majeure partie de la valeur des actifs[79]. Le lien de causalité direct entre l'imposition de l'amende et la perte de valeur significative des actifs doit être démontré. Il n'est pas automatiquement admis que la faillite ou l'insolvabilité d'une entreprise entraîne forcément une perte significative de la valeur des actifs. Qui plus est, il est impossible que l'amende ait menacé la viabilité économique d'une entreprise lorsque cette dernière a elle-même décidé de cesser ses activités et de vendre l'ensemble de ses actifs. L'entreprise doit prouver qu'il est probable qu'elle quitte le marché et que ses actifs soient démantelés ou vendus à des prix fortement réduits, sans que l'entreprise (ou ses actifs) ait d'autre possibilité de poursuivre ses activités. Cela signifie que l'autorité de contrôle doit exiger de l'entreprise qu'elle prouve que rien ne laisse clairement penser que l'entreprise (ou ses actifs) sera rachetée par une autre entreprise ou un autre propriétaire et sera à même de poursuivre ses activités.

c) **Contexte social et économique particulier:** Le contexte économique particulier peut être pris en considération si le secteur en cause traverse une crise conjoncturelle (par exemple, s'il souffre d'une surcapacité ou d'une déflation) ou si les entreprises ont des difficultés à mobiliser des capitaux ou à obtenir des crédits en raison de la conjoncture économique. Le contexte social particulier est susceptible d'être pertinent dans le contexte d'un chômage élevé ou croissant à un niveau régional ou à une plus grande échelle. Ce contexte peut également être apprécié à la lumière

[76] Voir sur ce principe, par exemple, les lignes directrices de la Commission pour le calcul des amendes infligées en application de l'article 23, paragraphe 2, sous a), du règlement (CE) nº 1/2003 (2006/C 210/02).

[77] Voir les affaires jointes C-189/02 P, C-202/02 P, C-205/02 P à C-208/02 P et C-213/02 P, *Dansk Rørindustri et autres/Commission*, point 327, citant les affaires jointes 96/82 à 102/82, 104/82, 105/82, 108/82 et 110/82, *NV IAZ International Belgium et autres/Commission*, points 54 et 55. Cette affirmation a été réitérée plus récemment dans l'affaire C-308/04 P, *SGL Carbon/Commission*, point 105, et dans l'affaire T-429/10 (affaires jointes T-426/10, T-427/10, T-428/10, T-429/10, T-438/12, T-439/12, T-440/12, T-441/12), *Global Steel Wire/Commission*, points 492 et 493.

[78] Voir l'affaire T-429/10 (affaires jointes T-426/10, T-427/10, T-428/10, T-429/10, T-438/12, T-439/12, T-440/12, T-441/12), *Global Steel Wire/Commission*, points 521 à 527.

[79] Voir arrêt dans les affaires jointes T-236/01, T-239/01, T-244/01 à T-246/01, T-251/01 et T-252/01, *Tokai Carbon et autres/Commission*, point 372 et affaire T-64/02, *Heubach/Commission*, point 163. Voir l'affaire INTP T-393/10, *Westfälische Drahtindustrie et autres/Commission*, points 293 et 294.

des conséquences que le paiement de l'amende pourrait avoir, notamment sur le plan d'une augmentation du chômage ou d'une détérioration des secteurs économiques en amont et en aval de l'entreprise concernée[80].

141. Si les critères sont satisfaits, les autorités de contrôle peuvent tenir compte de l'incapacité de l'entreprise à payer et minorer l'amende en conséquence.

7.3 – Caractère dissuasif

142. Enfin, une amende dissuasive est une amende qui a un véritable effet dissuasif[81]. À cet égard, une distinction peut être opérée entre la «dissuasion générale» (décourager d'autres personnes de commettre la même violation à l'avenir) et la «dissuasion spécifique» (dissuader les personnes visées par les amendes d'enfreindre de nouveau les règles à l'avenir)[82]. Lorsqu'elle impose une amende, l'autorité de contrôle veille à la dissuasion générale aussi bien qu'à la dissuasion spécifique.

143. Une amende est dissuasive lorsqu'elle décourage une personne d'entraver les objectifs poursuivis et de violer les règles établies par le droit de l'Union. La nature et le niveau de l'amende, mais surtout la probabilité que cette amende soit infligée sont des facteurs déterminants à cet égard. La personne qui se rend coupable d'une violation doit craindre de se voir effectivement imposer une amende. Ici, le critère de la dissuasion recoupe celui de l'effectivité[83].

144. Les autorités de contrôle peuvent envisager de majorer l'amende si elles estiment que le montant n'est pas assez dissuasif. Dans certaines circonstances, l'application d'un multiplicateur de dissuasion peut être justifiée[84]. Ce multiplicateur peut être fixé à la discrétion de l'autorité de contrôle en vue de respecter les objectifs de dissuasion exposés précédemment.

CHAPITRE 8 – FLEXIBILITÉ ET ÉVALUATION RÉGULIÈRE

145. Les chapitres qui précèdent définissent une méthode générale pour le calcul des amendes et faciliteront l'harmonisation et la transparence en ce qui concerne les pratiques des autorités de contrôle en la matière. Toutefois, cette méthode générale ne doit pas être interprétée comme un calcul automatique ou arithmétique. La fixation au cas par cas d'une amende doit toujours reposer sur une appréciation humaine de toutes les circonstances pertinentes du cas d'espèce et doit être efficace, proportionnée et dissuasive pour le cas en cause.

146. Il convient de garder à l'esprit que les présentes lignes directrices ne sauraient anticiper toutes les particularités possibles d'un cas d'espèce et, à cet égard, ne peuvent pas fournir d'orientations exhaustives aux autorités de contrôle. Dès lors, les présentes lignes directrices font l'objet d'un réexamen régulier dans le but de déterminer si leur application permet effectivement de réaliser les objectifs fixés par le RGPD. L'EDPB peut réviser les présentes lignes directrices sur la base de l'expérience acquise par les autorités de contrôle dans leur application pratique quotidienne et peut suspendre, modifier, limiter, amender ou remplacer les présentes lignes directrices, à tout moment et sans effet rétroactif.

---

[80] Voir l'affaire C-308/04 P, *SGL Carbon/Commission*, point 106.
[81] Voir les conclusions de l'avocat général Geelhoed dans l'affaire C-304/02, *Commission/France*, point 39.
[82] Voir, entre autres, l'affaire C-511/11 P, *Versalis Spa/Commission*, point 94.
[83] Conclusions de l'avocat général Kokott dans les affaires jointes C-387/02, C-391/02 et C-403/02, *Silvio Berlusconi e.a.*, point 89.
[84] Voir, en particulier, l'affaire C-289/04 P, *Showa Denko/Commission*, points 28 à 39.

ANNEXE – TABLEAU D'ILLUSTRATION DES LIGNES DIRECTRICES 04/2022 SUR LE CALCUL DES AMENDES ADMINISTRATIVES AU TITRE DU RGPD

Guide de lecture

- Ce tableau doit être lu conjointement avec l'ensemble des présentes lignes directrices, et n'est pas destiné à faire office de résumé exhaustif de ces dernières, ou de solution de remplacement se substituant à l'appréciation au regard des présentes lignes directrices dans leur ensemble.
- Ce tableau n'est fourni qu'à des fins d'illustration et ne constitue en aucun cas une représentation exhaustive ou finale de la position de l'EDPB sur le calcul des amendes administratives.
- Le tableau comporte deux étapes: la première illustre la fourchette du montant de départ selon la gravité de la violation, et la deuxième illustre la fourchette du montant de départ après ajustement appliqué en fonction de la taille de l'entreprise.
- Les chiffres indiqués comme montants de départ correspondent, d'une part, à la recommandation de la Commission relative aux PME et à la manière dont les chiffres d'affaires mentionnés dans ladite recommandation se rapportent au chiffre d'affaires tiré de l'article 83 du RGPD[85]. D'autre part, pour ce qui est du montant en fonction de la gravité de la violation, ces chiffres reposent sur les connaissances découlant de la pratique actuelle en matière d'imposition d'amendes et sur des tests internes approfondis réalisés sur les modèles d'imposition d'amendes sur plusieurs années. L'EDPB est convaincu que ces montants de départ sont conformes aux critères d'effectivité, de proportionnalité et de dissuasion exigés à l'article 83, paragraphe 1, du RGPD.
- Cependant et comme toujours, l'EDPB a bien conscience que le calcul d'une amende administrative n'est pas un exercice purement mathématique, et que les cas d'espèce concrets ainsi que la pratique conduiront inévitablement à la nécessité d'affiner les montants de départ indiqués dans ce tableau. À cette fin, les présentes lignes directrices avertissent que le tableau et les montants qu'il contient font l'objet d'un examen rigoureux de la part de l'EDPB et qu'ils seront adaptés si besoin.
- Il y a lieu de rappeler que ces chiffres représentent les montants de départ d'un calcul ultérieur, et non des montants fixes (étiquettes de prix). L'autorité de contrôle est libre de recourir à l'ensemble de la fourchette des amendes, de n'importe quel montant jusqu'au montant maximal légal.
- Dans la première étape, plus la violation est grave au sein de sa catégorie propre, plus le montant de départ est susceptible d'être élevé.
- Dans la deuxième étape, les pourcentages sont déterminants pour fixer le montant de départ final, tandis que des ajustements peuvent être effectués jusqu'à un certain pourcentage du montant de départ déterminé à l'étape 1. Cela signifie que le pourcentage retenu à l'étape 2 sera utilisé comme multiplicateur du montant de départ déterminé à l'étape 1. Plus le chiffre d'affaires de l'entreprise est élevé au sein du niveau applicable, plus le montant de départ est susceptible de l'être également au cours de l'étape 2.
- Les montants indiqués pour la deuxième étape illustrent simplement les montants les plus faibles de la tranche inférieure et les montants les plus élevés de la tranche supérieure, qui peuvent être appliqués dans cette catégorie. Le montant de départ final sera compris entre ces deux extrêmes. Ces fourchettes dans la deuxième étape servent donc de contrôle du discernement pour la personne en charge du dossier.
- Il convient de noter qu'aucun ajustement n'est prévu à l'étape 2 pour les entreprises dont le chiffre d'affaires est égal ou supérieur à 500 millions d'EUR, étant donné que ces entreprises dépasseront le montant maximal légal fixe et que, en conséquence, la taille de l'entreprise est déjà prise en considération dans le montant maximal légal évolutif utilisé pour fixer le montant de départ pour le calcul ultérieur à l'étape 1.

[85] Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises [notifiée sous le numéro de document C(2003) 1422, (2003/361/CE)].

- L'application de la méthode, y compris l'utilisation des tableaux, est illustrée par deux exemples à la fin de la présente annexe.

Étape 1: Calcul du montant de départ en fonction de la gravité

NB: plus la violation est grave au sein de sa catégorie propre, plus le montant de départ est susceptible d'être élevé au cours de cette première étape.

	Gravité faible		**Gravité moyenne**		**Gravité élevée**	
	Fourchette fixe	*Fourchette évolutive* dans le cas d'un chiffre d'affaires > 500 millions	*Fourchette fixe*	*Fourchette évolutive dans le cas d'un chiffre d'affaires > 500 millions*	*Fourchette fixe*	*Fourchette évolutive dans le cas d'un chiffre d'affaires > 500 millions*
Article 83, paragraphe 4, du RGPD	0 à 1 million	0 à 0,2 % du chiffre d'affaires annuel	1 à 2 millions	0,2 % à 0,4 % du chiffre d'affaires annuel	2 à 10 millions	0,4 % à 2 % du chiffre d'affaires annuel
Article 83, paragraphes 5 et 6, du RGPD	0 à 2 millions	0 à 0,4 % du chiffre d'affaires annuel	2 à 4 millions	0,4 % à 0,8 % du chiffre d'affaires annuel	4 à 20 millions	0,8 % à 4 % du chiffre d'affaires annuel

Étape 2: Ajustement du montant de départ selon la taille de l'entreprise (applicable uniquement aux entreprises auxquelles la fourchette légale fixe s'applique)

NB: plus le chiffre d'affaires de l'entreprise est élevé au sein du niveau applicable, plus le montant de départ est susceptible de l'être également au cours de cette deuxième étape.

Article 83, paragraphe 4, du RGPD

	Gravité faible	**Gravité moyenne**	**Gravité élevée**
Entreprises dont le chiffre d'affaires est compris entre 250 et 500 millions d'EUR	40 à 100 % du montant de départ		
	0 à 1 million	400 000 à 2 millions	800 000 à 10 millions

	Gravité faible	**Gravité moyenne**	**Gravité élevée**
Entreprises dont le chiffre d'affaires est compris entre 100 et 250 millions d'EUR	15 à 50 % du montant de départ		
	0 à 500 000	150 000 à 1 million	300 000 à 5 millions
Entreprises dont le chiffre d'affaires est compris entre 50 et 100 millions d'EUR	8 à 20 % du montant de départ		
	0 à 200 000	80 000 à 400 000	160 000 à 2 millions
Entreprises dont le chiffre d'affaires est compris entre 10 et 50 millions d'EUR	1,5 à 10 % du montant de départ		
	0 à 100 000	15 000 à 200 000	30 000 à 1 million
Entreprises dont le chiffre d'affaires est compris entre 2 et 10 millions d'EUR	0,3 à 2 % du montant de départ		
	0 à 20 000	3 000 à 40 000	6 000 à 200 000
Entreprises dont le chiffre d'affaires est inférieur ou égal à 2 millions d'EUR	0,2 à 0,4 % du montant de départ		
	0 à 4 000	2 000 à 8 000	4 000 à 40 000

Article 83, paragraphes 5 et 6, du RGPD

	Gravité faible	**Gravité moyenne**	**Gravité élevée**
Entreprises dont le chiffre d'affaires est compris entre 250 et 500 millions d'EUR	40 à 100 % du montant de départ		
	0 à 2 millions	800 000 à 4 millions	1,6 à 20 millions
Entreprises dont le chiffre d'affaires est compris entre 100 et 250 millions d'EUR	15 à 50 % du montant de départ		
	0 à 1 million	300 000 à 2 millions	600 000 à 10 millions
Entreprises dont le chiffre d'affaires est compris entre 50 et 100 millions d'EUR	8 à 20 % du montant de départ		
	0 à 400 000	160 000 à 800 000	320 000 à 4 millions
Entreprises dont le chiffre d'affaires est compris entre 10 et 50 millions d'EUR	1,5 à 10 % du montant de départ		
	0 à 200 000	30 000 à 400 000	60 000 à 2 millions
Entreprises dont le chiffre d'affaires est compris entre 2 et 10 millions d'EUR	0,3 à 2 % du montant de départ		
	0 à 40 000	6 000 à 80 000	12 000 à 400 000
Entreprises dont le chiffre d'affaires est	0,2 à 0,4 % du montant de départ		

	Gravité faible	Gravité moyenne	Gravité élevée
inférieur ou égal à 2 millions d'EUR	0 à 8 000	4 000 à 16 000	8 000 à 80 000

Approche progressive pour l'application du chapitre 4 des lignes directrices sur le calcul des amendes, y compris les tableaux

Exemple A
L'autorité de contrôle constate qu'une société de médias sociaux dont le chiffre d'affaires s'élève à 200 millions d'EUR a vendu les données sensibles de ses utilisateurs à plusieurs courtiers en données. Aux fins du présent exemple, la société n'a enfreint que l'article 9 du RGPD. L'autorité de contrôle, après avoir analysé toutes les circonstances pertinentes du cas d'espèce au titre de l'article 83, paragraphe 2, points a), b) et g), a estimé que la violation était de gravité élevée.

Par la suite, l'autorité de contrôle doit décider du montant de départ pour la suite du calcul. La violation de l'article 9 est répertoriée à l'article 83, paragraphe 5, point a), du RGPD, qui dispose que le montant maximal légal est de 20 millions d'EUR ou de 4 % du chiffre d'affaires annuel. En l'espèce, le chiffre d'affaires de l'entreprise est inférieur à 500 millions d'EUR, ce qui signifie que le montant maximal et la fourchette fixes s'appliquent. Dès lors, il convient d'envisager un montant de départ compris entre 20 et 100 % du montant maximal légal applicable, soit entre 4 et 20 millions d'EUR. Étant donné que plus la violation est grave dans sa catégorie propre, plus le montant de départ est susceptible d'être élevé, l'autorité de contrôle décide que le montant de départ fixé en fonction de la gravité de la violation telle qu'elle a été déterminée à l'étape 1 devrait être de 10 millions d'EUR.

À l'étape 2, le montant de départ fixé à l'étape 1 sera ajusté en fonction de la taille de l'entreprise. L'entreprise réalise un chiffre d'affaires annuel de 200 millions d'EUR et se trouve donc dans la fourchette allant de 100 à 250 millions d'EUR. Cela signifie que le montant de départ sera ajusté pour être porté à un montant compris entre 15 % et 50 % du montant de départ. Étant donné que plus le chiffre d'affaires de l'entreprise est élevé au sein du niveau applicable, plus le montant de départ est susceptible de l'être également, l'autorité de contrôle décide qu'un ajustement jusqu'à 40 % du montant de départ fixé à l'étape 1 est justifié sur la base de la taille de l'entreprise. Le montant de départ après l'ajustement sera alors de 4 millions d'EUR dans ce cas d'espèce.

Pour s'assurer que ce montant de départ est conforme aux lignes directrices, il est possible de le recouper avec les fourchettes figurant dans le tableau applicable. Puisque l'article 83, paragraphe 5, du RGPD est applicable, que l'entreprise réalise un chiffre d'affaires compris entre 100 et 250 millions d'EUR et que le degré de gravité est élevé, le montant de départ devrait se situer entre 600 000 et 10 millions d'EUR. L'autorité de contrôle arrive à la conclusion qu'un montant de départ de 4 millions d'EUR se situe dans la fourchette comprise entre 600 000 et 10 millions d'EUR. Par conséquent, le montant de départ est conforme aux lignes directrices.

À la suite de cette appréciation, l'autorité de contrôle procède au calcul du montant de l'amende sur la base du reste des présentes lignes directrices.

Exemple B
Une chaîne hôtelière dont le chiffre d'affaires s'élève à 2 milliards d'EUR a enfreint l'article 12 du RGPD. L'autorité de contrôle, après avoir analysé les circonstances du cas d'espèce au titre de l'article 83, paragraphe 2, points a), b) et g), a estimé que la violation était de gravité moyenne.

Par la suite, l'autorité de contrôle doit décider du montant de départ pour la suite du calcul. L'autorité de contrôle constate tout d'abord que la violation de l'article 12 du RGPD est répertoriée à l'article 83, paragraphe 5, point b), du RGPD. Le chiffre d'affaires de l'entreprise étant de 2 milliards d'EUR, soit plus de 500 millions d'EUR, c'est donc le montant maximal évolutif qui s'applique. En d'autres termes, le montant maximal légal s'élève à 4 % du chiffre d'affaires annuel de l'entreprise, soit 80 millions d'EUR. Le degré de gravité est moyen et, de ce fait, il y a lieu d'envisager un montant de départ compris entre 10 et 20 % du montant maximal légal applicable, c'est-à-dire entre 0,4 % et 0,8 % du chiffre d'affaires annuel, ce qui équivaut à un montant de départ compris entre 8 millions et 16 millions d'EUR.

Étant donné que plus la violation est grave dans sa catégorie propre, plus le montant de départ est susceptible d'être élevé, l'autorité de contrôle estime qu'en raison de la gravité de la violation, le montant de départ devrait être de 12 millions d'EUR, soit 15 % du montant maximal légal applicable et 0,6 % du chiffre d'affaires annuel de l'entreprise.

Puisque l'entreprise réalise un chiffre d'affaires annuel supérieur à 500 millions d'EUR et que le montant maximal légal évolutif s'applique, la taille de l'entreprise est déjà prise en considération dans ledit montant utilisé pour fixer le montant de départ. Par conséquent, aucun ajustement supplémentaire n'est réalisé.

À la suite de cette appréciation, l'autorité de contrôle procède au calcul du montant de l'amende sur la base du reste des présentes lignes directrices.