GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP 253

Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679

Adoptées le 3 octobre 2017

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant chargé de la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (droits fondamentaux et citoyenneté de l'Union) de la direction générale Justice et consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 03/075.

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

Table des matières:

I. Introduction 4
II. Principes 5
III. Critères d'évaluation visés à l'article 83, paragraphe 2 9
IV. Conclusions 18

I. Introduction

L'Union européenne a mené à bien une réforme approfondie de la réglementation relative à la protection des données en Europe. Cette réforme repose sur plusieurs piliers (éléments clés): des règles cohérentes, des procédures simplifiées, des actions coordonnées, la participation des utilisateurs, une information plus efficace et des pouvoirs renforcés d'application des règles.

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 règlement général sur la protection des données (ci-après le «règlement») ainsi que les droits des personnes concernées sont respectés conformément à l'esprit et à la lettre du règlement.

L'application cohérente des règles relatives à la protection des données est essentielle à un régime harmonisé de protection des données. Les amendes administratives sont au cœur du nouveau régime d'application introduit par le règlement. Elles constituent un élément efficace de la panoplie dont les autorités de contrôle disposent pour faire respecter la réglementation, parallèlement aux autres mesures prévues par l'article 58.

Le présent document vise à aider les autorités de contrôle, auxquelles il est destiné, à améliorer l'application du règlement et à mieux le faire respecter. Il reflète leur compréhension commune des dispositions de l'article 83 du règlement ainsi que son interaction avec les articles 58 et 70 et les considérants correspondants.

En particulier, l'article 70, paragraphe 1, point e), prévoit que le comité européen de la protection des données (ci-après le «CEPD») est habilité à publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente du présent règlement. L'article 70, paragraphe 1, point k), précise la disposition pour ce qui est des lignes directrices concernant la fixation des amendes administratives.

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

Afin d'assurer une approche cohérente de l'imposition des amendes administratives, qui reflète de manière adéquate l'ensemble des principes énoncés dans les présentes lignes directrices, le CEPD a convenu d'une définition commune des critères d'évaluation visés à l'article 83, paragraphe 2, du règlement. Le CEPD et chaque autorité de contrôle conviennent donc d'utiliser les présentes lignes directrices dans le cadre d'une approche commune.

II. Principes

Dès qu'une violation du règlement a été établie sur la base de l'évaluation des faits de l'espèce, l'autorité de contrôle compétente doit définir la ou les mesures correctives les plus adéquates pour remédier à la violation. Les dispositions de l'article 58, paragraphe 2, points b à j[1], énoncent les instruments que les autorités de contrôle peuvent utiliser pour remédier aux cas de non-conformité dus à un responsable du traitement ou un sous-traitant. Lorsqu'elles exercent ces pouvoirs, les autorités de contrôle doivent respecter les principes suivants:

1. La violation du règlement devrait entraîner l'imposition de «sanctions équivalentes».

La notion d'«équivalence» est essentielle pour déterminer la portée de l'obligation qui incombe aux autorités de contrôle de veiller à être cohérentes lorsqu'elles exercent leur pouvoir d'adopter des mesures correctives conformément à l'article 58, paragraphe 2, de manière générale, et lorsqu'elles infligent des amendes administratives en particulier[2].

Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, ***le niveau de protection [...] devrait être équivalent*** *dans tous les États membres* (considérant 10). Le considérant 11 précise qu'un niveau équivalent de protection des données à caractère personnel dans l'ensemble de l'Union exige, entre autres, «*dans les États membres, des pouvoirs équivalents de surveillance et de contrôle du respect des règles relatives à la protection des données à caractère personnel et des sanctions équivalentes pour les violations*». En outre, des sanctions équivalentes dans l'ensemble des États membres ainsi qu'une coopération efficace entre les autorités de contrôle des différents États membres sont considérées comme une manière «*d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur*», conformément au considérant 13 du règlement.

Le règlement offre une base plus solide que la directive 95/46/CE pour assurer un niveau plus élevé de cohérence, puisqu'il est directement applicable dans les États membres. Si les autorités de contrôle agissent en «totale indépendance» (article 52) à l'égard des gouvernements, des responsables du traitement ou des sous-traitants, elles sont tenues de coopérer «*en vue d'assurer une application cohérente du présent règlement et des mesures prises pour en assurer le respect*» [article 57, paragraphe 1, point g)].

Le règlement appelle à une plus grande cohérence que la directive 95/46/CE lorsque des sanctions sont infligées. Dans les cas transfrontaliers, la cohérence sera garantie essentiellement par le mécanisme de coopération (guichet unique) et, dans une certaine mesure, par le mécanisme de contrôle de la cohérence décrit par le nouveau règlement.

Dans les cas nationaux couverts par le règlement, les autorités de contrôle appliqueront les présentes lignes directrices dans un esprit de coopération, conformément à l'article 57, paragraphe 1, point g), et

[1] L'article 58, paragraphe 2, point a), prévoit que des avertissements peuvent être adressés lorsque «les opérations de traitement [...] sont susceptibles de violer les dispositions du présent règlement». Autrement dit, dans le cas couvert par la disposition, la violation du règlement n'a pas encore eu lieu.

[2] Même lorsque le système juridique de certains pays de l'Union ne permet pas l'imposition d'amendes administratives comme le règlement le prévoit, une telle application des règles dans ces États membres doit avoir un effet équivalent aux amendes administratives infligées par les autorités de contrôle (considérant 151). Les juridictions sont tenues par le règlement mais pas par les présentes lignes directrices du CEPD.

à l'article 63, en vue d'assurer une application cohérente du règlement et des mesures prises pour en assurer le respect. Bien que les autorités de contrôle restent libres de choisir les mesures correctives présentées à l'article 58, paragraphe 2, elles doivent éviter d'appliquer des mesures correctives différentes à des cas similaires.

Il en va de même lorsque ces mesures correctives prennent la forme d'amendes.

2. Comme toutes les mesures correctives choisies par les autorités de contrôle, les amendes administratives devraient être «effectives, proportionnées et dissuasives».

Comme toutes les mesures correctives en général, les amendes administratives devraient répondre de manière adéquate à la nature, à la gravité et aux conséquences de la violation, et les autorités de contrôle doivent apprécier l'ensemble des faits de l'espèce d'une manière cohérente et objectivement justifiée. L'appréciation du caractère effectif, proportionné et dissuasif dans chaque cas devra également prendre en considération l'objectif poursuivi par la mesure corrective retenue, à savoir de restaurer le respect des règles ou de sanctionner un comportement illicite (ou les deux).

Les autorités de contrôle devraient déterminer une mesure corrective qui soit «*effective, proportionnée et dissuasive*» (article 83, paragraphe 1), tant dans les cas nationaux (article 55) que dans les cas impliquant un traitement transfrontalier de données à caractère personnel (tel que défini à l'article 4, paragraphe 23).

Les présentes lignes directrices reconnaissent le fait que les législations nationales peuvent fixer des exigences supplémentaires pour la procédure coercitive devant être suivie par les autorités de contrôle. Ces exigences peuvent comprendre, par exemple, l'envoi de notifications, les exigences de formes, les délais pour la présentation d'observations, le recours, l'exécution des règles et le paiement[3].

Ces exigences ne devraient toutefois pas porter atteinte, dans la pratique, au caractère effectif, proportionné ou dissuasif des mesures.

La pratique émergente au sein des autorités de contrôle en matière de protection des données, mais aussi les enseignements tirés d'autres secteurs réglementés préciseront la notion de caractère effectif, proportionné ou dissuasif, de même que la jurisprudence des juridictions appelées à interpréter ces principes.

Pour infliger des amendes effectives, proportionnées et dissuasives, les autorités de contrôle s'en remettront à la définition de la notion d'entreprise fournie par la CJUE aux fins de l'application des articles 101 et 102 du traité FUE, à savoir que la notion d'entreprise **doit s'entendre** comme une unité économique pouvant être formée par la société mère et toutes les filiales concernées. Conformément au droit et à la jurisprudence de l'Union[4], il y a lieu d'entendre par entreprise l'unité économique engagée dans des activités commerciales ou économiques, quelle que soit la personne morale impliquée (considérant 150).

[3] Par exemple, le cadre constitutionnel et le projet de loi sur la protection des données en Irlande prévoient qu'une décision formelle est prise sur l'établissement de la violation et que celle-ci est communiquée aux parties concernées avant l'évaluation de la sévérité de la ou des sanctions. La décision sur l'établissement de la violation ne peut être modifiée pendant l'évaluation de la sévérité de la ou des sanctions.

[4] Dans sa jurisprudence, la Cour de justice en donne la définition suivante: «la notion d'entreprise comprend toute entité exerçant une activité économique, indépendamment du statut juridique de cette entité et de son mode de financement» (arrêt Höfner et Elsner, ECLI:EU:C:1991:161, point 21). Une entreprise «doit être comprise comme désignant une unité économique même si, du point de vue juridique, cette unité économique est constituée de plusieurs personnes physiques ou morales» (arrêt Confederación Española de Empresarios de Estaciones de Servicio, ECLI:EU:C:2006:784, point 40).

3. L'autorité de contrôle compétente appréciera «chaque cas d'espèce»

Les amendes administratives peuvent être infligées pour répondre à toute une série de violations. L'article 83 du règlement prévoit une approche harmonisée des violations des obligations explicitement énumérées aux paragraphes 4 à 6. La législation d'un État membre peut étendre l'application de l'article 83 aux autorités et organismes publics établis dans cet État membre. En outre, la législation des États membres peut permettre ou même rendre obligatoire l'imposition d'une amende en cas de violation d'autres dispositions que celles visées à l'article 83, paragraphes 4 à 6.

Le règlement exige que chaque cas d'espèce soit apprécié[5]. L'article 83, paragraphe 2, est le point de départ d'une telle appréciation individuelle. Ce paragraphe énonce que «[p]*our décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants* (...)». Par conséquent, et compte tenu également du considérant 148[6], l'autorité de contrôle est tenue de choisir la ou les mesures les plus adéquates. Dans les cas mentionnés à l'article 83, paragraphes 4 à 6, ce choix **doit** prendre en considération l'ensemble des mesures correctives, et notamment l'imposition de l'amende administrative appropriée, que ce soit parallèlement à une mesure corrective au titre de l'article 58, paragraphe 2, ou de manière autonome.

Les amendes sont un instrument important que les autorités de contrôle devraient utiliser dans les circonstances appropriées. Les autorités de contrôle sont encouragées à adopter une approche mûrement réfléchie et équilibrée lorsqu'elles appliquent des mesures correctives afin de réagir à la violation d'une manière tant effective et dissuasive que proportionnée. Il ne s'agit pas de considérer les amendes comme un recours ultime ni de craindre de les imposer, mais, en revanche, elles ne doivent pas non plus être utilisées de telle manière que leur efficacité s'en trouverait amoindrie.

---

[5] Outre l'application des critères prévus à l'article 83, d'autres dispositions sous-tendent cette approche, notamment:

- le considérant 141 («*L'enquête faisant suite à une réclamation devrait être menée, sous contrôle juridictionnel, dans la mesure appropriée au cas d'espèce.*»);
- le considérant 129 («*Les pouvoirs des autorités de contrôle devraient être exercés conformément aux garanties procédurales appropriées prévues par le droit de l'Union et le droit des États membres, d'une manière impartiale et équitable et dans un délai raisonnable. Toute mesure devrait notamment être appropriée, nécessaire et proportionnée en vue de garantir le respect du présent règlement, compte tenu des circonstances de l'espèce...»);*
- l'article 57, paragraphe 1, point f) («*traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association, conformément à l'article 80, examine l'objet de la réclamation, dans la mesure nécessaire...;*»).

[6] *Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle en vertu du présent règlement. En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il convient toutefois 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. L'application de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.*»

Dans les cas où l'article 65 du règlement reconnaît sa compétence, le CEPD adopte une décision contraignante dans les litiges entre autorités qui concernent en particulier l'établissement d'une violation. Lorsque l'objection pertinente et motivée soulève la question de la conformité de la mesure corrective avec le RGPD, la décision du CEPD examine également la manière dont les principes d'efficacité, de proportionnalité et de dissuasion sont respectés par l'amende administrative proposée dans le projet de décision de l'autorité de contrôle compétente. Les lignes directrices distinctes que le CEPD formulera sur l'application de l'article 65 du règlement apporteront plus de précisions sur le type de décision devant être prise par le CEPD.

4. Une approche harmonisée des amendes administratives dans le domaine de la protection des données requiert la participation active des autorités de contrôle et des échanges d'informations entre elles

Les présentes lignes directrices reconnaissent le fait que le pouvoir d'infliger des amendes représente, pour certaines autorités de contrôle nationales, une nouveauté dans le domaine de la protection des données et qu'il soulève de nombreuses questions de ressources, d'organisation et de procédure. Ainsi, les décisions par lesquelles les autorités de contrôle exercent le pouvoir d'infliger des amendes qui leur a été confié pourront être attaquées devant les juridictions nationales.

Les autorités de contrôle coopèrent entre elles et, le cas échéant, avec la Commission européenne au travers des mécanismes de coopération prévus par le règlement afin de favoriser les échanges d'informations formels et informels, notamment lors d'ateliers. Cette coopération devrait se concentrer sur leur expérience et leur pratique dans l'exercice du pouvoir d'infliger des amendes, le but ultime étant d'atteindre une plus grande cohérence.

Ce partage proactif d'informations, parallèlement à la jurisprudence émergente sur l'exercice de ce pouvoir, pourrait donner lieu à une révision des principes ou de certains points des présentes lignes directrices.

III. Critères d'évaluation visés à l'article 83, paragraphe 2

L'article 83, paragraphe 2, contient une liste de critères que les autorités de contrôle sont censées appliquer lorsqu'elles apprécient l'opportunité d'infliger une amende ainsi que le montant de celle-ci. Il n'est pas recommandé d'effectuer une évaluation répétée des mêmes critères, mais une évaluation qui tienne compte de l'ensemble des circonstances de chaque cas d'espèce, conformément à l'article 83[7].

Les conclusions établies au premier stade de l'évaluation peuvent être utilisées à la seconde étape relative au montant de l'amende, afin d'éviter de devoir effectuer une deuxième évaluation sur la base des mêmes critères.

Les lignes directrices de la présente section visent à aider les autorités de contrôle à interpréter les faits de l'espèce à la lumière des critères énoncés à l'article 83, paragraphe 2.

a) la nature, la gravité et la durée de l'infraction

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. En fixant deux montants maximaux différents pour l'amende administrative (10 et 20 millions d'euros), le règlement indique déjà que la violation de certaines dispositions du règlement peut être plus grave que celle d'autres dispositions. Lorsqu'elle évalue les faits de l'espèce à la lumière des critères généraux contenus à l'article 83, paragraphe 2, l'autorité de contrôle compétente peut toutefois considérer que, dans le cas d'espèce, la nécessité de réagir par une mesure corrective sous la forme d'une amende est plus ou moins élevée. Lorsqu'une amende est choisie comme mesure corrective appropriée ou qu'elle figure parmi de telles mesures, le système par paliers prévu par le règlement (article 83, paragraphes 4 à 6) est appliqué pour déterminer l'amende maximale pouvant être infligée en fonction de la nature de la violation en question.

Le considérant 148 introduit la notion de «violations mineures». Ces violations peuvent porter sur une ou plusieurs dispositions du règlement, énumérées à l'article 83, paragraphe 4 ou 5. L'évaluation des critères énoncés à l'article 83, paragraphe 2, peut toutefois amener l'autorité de contrôle à considérer que, dans les circonstances concrètes de l'espèce, la violation n'engendre pas un risque important pour les droits des personnes concernées, par exemple, et qu'elle n'affecte pas l'essence de l'obligation en question. Dans de tels cas, l'amende est parfois (mais pas toujours) remplacée par un rappel à l'ordre.

Le considérant 148 ne fait pas obligation à l'autorité de contrôle de remplacer d'office l'amende par un rappel à l'ordre dans le cas d'une violation mineure («*un rappel à l'ordre peut être adressé plutôt qu'une amende*»), mais il lui laisse la possibilité de le faire après une évaluation concrète de toutes les circonstances de l'espèce.

Le considérant 148 offre la même possibilité de remplacer une amende par un rappel à l'ordre lorsque le responsable du traitement est une personne physique et que l'amende susceptible de lui être infligée constituerait une charge disproportionnée. Le principe est que l'autorité de contrôle doit évaluer si, compte tenu des circonstances du cas d'espèce, l'imposition d'une amende est nécessaire. Si elle tranche en faveur de l'imposition d'une amende, l'autorité de contrôle doit alors également évaluer si cette amende constituerait une charge disproportionnée pour une personne physique.

[7] En raison des règles de procédure nationales qui découlent, dans certains pays, d'exigences constitutionnelles, l'évaluation de la sanction à infliger peut être effectuée séparément après l'évaluation de la question de savoir si une violation a été commise. Le contenu et le degré de précision d'un projet de décision adopté par l'autorité de contrôle principale dans ces pays peuvent s'en trouver limités.

Le règlement n'attribue pas un taux d'amende précis à chaque violation, mais se borne à les plafonner (montant maximal). Cela peut indiquer que la violation des obligations énoncées à l'article 83, paragraphe 4, est moins grave que la violation de celles énumérées à l'article 83, paragraphe 5. La réaction effective, proportionnée et dissuasive à une violation de l'article 83, paragraphe 5, dépendra néanmoins des circonstances de l'espèce.

Il convient de noter que les violations du règlement qui, par leur nature, pourraient relever de la catégorie allant «jusqu'à 10 millions d'euros ou jusqu'à 2 % du chiffre d'affaires annuel mondial total», visée à l'article 83, paragraphe 4, pourraient finalement relever d'une catégorie de niveau supérieur (20 millions d'euros) dans certaines circonstances. Cela pourrait être le cas lorsque ces violations ont fait précédemment l'objet d'une injonction[8] de l'autorité de contrôle que le responsable du traitement ou le sous-traitant n'a pas respectée[9] (article 83, paragraphe 6). Les dispositions de la législation nationale peuvent, dans la pratique, affecter cette évaluation[10]. La nature de la violation, 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*» donneront une indication de la **gravité** de la violation. La survenance de plusieurs violations différentes commises simultanément dans un cas particulier implique que l'autorité de contrôle a la possibilité d'infliger les amendes administratives à un niveau qui rend celles-ci efficaces, proportionnées et dissuasives, dans les limites de la violation la plus grave. Par conséquent, si une violation des articles 8 et 12 a été constatée, l'autorité de contrôle a la possibilité d'appliquer les mesures correctives visées à l'article 83, paragraphe 5, qui correspondent à la catégorie de la violation la plus grave, à savoir celle de l'article 12. La fourniture, à ce stade, d'informations plus détaillées dépasserait le cadre des présentes lignes directrices (des calculs détaillés pourraient en effet faire l'objet d'une éventuelle version ultérieure).

---

[8] Les injonctions visées à l'article 58, paragraphe 2, sont les suivantes:

- ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement;
- ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé;
- ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel;
- imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;
- ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19;
- ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites;
- ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

[9] L'application de l'article 83, paragraphe 6, doit nécessairement tenir compte du droit de procédure national. La législation nationale détermine la manière dont une injonction est émise et notifiée ainsi que le moment à partir duquel elle entre en vigueur. Elle détermine également si un délai peut être accordé pour la mise en conformité. En particulier, l'effet d'un recours sur la force exécutoire d'une injonction devrait être pris en considération.

[10] Les dispositions législatives relatives à la prescription peuvent avoir pour effet qu'une injonction précédente de l'autorité de contrôle ne puisse plus être prise en considération en raison du laps de temps qui s'est écoulé depuis qu'elle a été émise. Dans certaines juridictions, les règles prévoient qu'à l'expiration de la période de prescription concernant une injonction, aucune amende ne peut être infligée pour le non-respect de cette injonction au titre de l'article 83, paragraphe 6. Il incombe à chaque autorité de contrôle dans chaque juridiction de déterminer comment elle sera affectée par ces dispositions.

Les facteurs ci-dessous devraient être évalués en combinaison avec, par exemple, le nombre de personnes concernées et les effets possibles sur celles-ci.

Le **nombre** de personnes concernées devrait être évalué afin de déterminer si le fait est isolé ou s'il est révélateur d'une violation plus systématique ou de l'absence de routines adéquates. Cela ne veut pas dire que des faits isolés ne devraient pas donner lieu à l'application des règles, étant donné qu'ils peuvent tout de même affecter de nombreuses personnes concernées. En fonction des circonstances de l'espèce, ce nombre se rapportera, par exemple, au nombre total de déclarants dans la base de données en cause, au nombre d'utilisateurs d'un service, au nombre de clients ou à la population du pays, le cas échéant.

La **finalité** du traitement doit également être évaluée. L'avis du groupe de travail «article 29» relatif à la limitation des finalités[11] a déjà analysé les deux grands éléments fondateurs de ce principe de la législation sur la protection des données: la spécification des finalités et l'utilisation compatible. Lorsqu'elles apprécient la finalité du traitement dans le contexte de l'article 83, paragraphe 2, les autorités de contrôle devraient se demander dans quelle mesure le traitement respecte les deux éléments clés de ce principe[12]. Dans certaines situations, l'autorité de contrôle peut estimer nécessaire de procéder à une analyse plus approfondie de la finalité du traitement en tant que tel dans l'analyse visée à l'article 83, paragraphe 2.

Si les personnes concernées ont subi un **dommage**, le niveau du dommage doit être pris en considération. Le traitement de données à caractère personnel peut engendrer des risques pour les droits et les libertés de l'individu, comme l'exprime le considérant 75:

> «*Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier: lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.*»

[11] WP 203, avis 03/2013 sur la limitation des finalités, consultable à la page: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Voir également WP 217, avis 6/2014 sur la notion d'intérêt légitime du responsable du traitement au titre de l'article 7, page 24, sur la question: «Qu'est-ce qui fait qu'un intérêt est "légitime" ou "illégitime"?»

Si des dommages ont été subis ou sont susceptibles de l'être en raison d'une violation du règlement, l'autorité de contrôle devrait en tenir compte dans le choix de la mesure corrective, même si elle n'est pas elle-même compétente pour octroyer le dédommagement correspondant au préjudice subi.

L'imposition d'une amende ne dépend pas de la capacité de l'autorité de contrôle à établir un lien de cause à effet entre la violation et le préjudice matériel (voir, par exemple, l'article 83, paragraphe 6).

La **durée** de la violation peut être indicative, par exemple:

a) d'un acte intentionnel de la part du responsable du traitement ou

b) d'une omission de prendre les mesures préventives appropriées ou

c) d'une incapacité à mettre en place les mesures techniques et organisationnelles requises.

b) le fait que la violation a été commise délibérément ou par négligence

En 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.

Il 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 et que, par conséquent, elles sont davantage susceptibles de justifier l'application d'une amende administrative. Les conclusions pertinentes concernant la volonté ou la négligence seront tirées sur la base des éléments objectifs de comportement déduits des faits de l'espèce. En outre, la jurisprudence et les pratiques émergentes dans le domaine de la protection des données résultant de l'application du règlement fourniront des exemples de circonstances indiquant des seuils plus précis pour apprécier si la violation a été commise ou non de manière délibérée.

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.

Les entreprises devraient veiller à mettre en place des structures et des ressources adaptées à la nature et à la complexité de leurs activités. En conséquence, les responsables du traitement et les sous-traitants ne peuvent se prévaloir d'un manque de ressources pour justifier des violations de la législation relative à la protection des données. D'après le règlement, les routines et la documentation des activités de traitement s'inspirent d'une approche basée sur le risque.

Il existe des zones grises qui influenceront la prise de décisions quant à l'opportunité d'imposer une mesure corrective. Il se peut que l'autorité doive procéder à une enquête plus poussée afin d'établir les faits de l'espèce et garantir que toutes les circonstances propres à chaque cas d'espèce ont été suffisamment prises en considération.

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées

Les responsables du traitement et les sous-traitants sont 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 et que la personne concernée subit un dommage, la partie responsable devrait faire tout ce qui est en son pouvoir pour réduire les conséquences de la violation pour la personne concernée. Un tel comportement responsable (ou son absence) devrait être pris en compte par l'autorité de contrôle lorsqu'elle choisit la ou les mesures correctives et lorsqu'elle évalue la sanction à infliger dans le cas d'espèce.

Bien que les facteurs aggravants et atténuants soient particulièrement adaptés pour calculer avec précision le montant de l'amende en fonction des circonstances particulières de l'espèce, leur rôle dans le choix de la mesure corrective appropriée ne devrait pas être sous-estimé. Dans les cas où l'évaluation basée sur d'autres critères laisse des doutes à l'autorité de contrôle quant à l'opportunité d'une amende administrative, qu'il s'agisse d'une mesure corrective unique ou d'une mesure combinée à celles visées à l'article 58, ces circonstances aggravantes ou atténuantes peuvent aider à choisir les mesures appropriées en faisant pencher la balance vers celle qui paraît la plus efficace, la plus proportionnée et la plus dissuasive dans le cas concerné.

Cette disposition vise à évaluer le degré de responsabilité du responsable du traitement après que la violation a été commise. Il se peut qu'elle couvre des cas où le responsable du traitement ou le sous-traitant n'a manifestement pas adopté une attitude irresponsable ou négligente, mais où il a fait tout son possible pour corriger son comportement lorsqu'il a pris conscience de la violation.

L'expérience dans le domaine réglementaire accumulée par les autorités de contrôle dans le cadre de la directive 95/46/CE a montré précédemment qu'il peut être approprié de faire preuve d'une certaine flexibilité à l'égard des responsables du traitement ou des sous-traitants qui ont reconnu avoir commis une violation et pris des mesures pour remédier à leur comportement ou en limiter les conséquences. Ces mesures peuvent, par exemple, prendre les formes suivantes (elles ne justifieront toutefois pas une approche plus flexible dans chaque cas):

- la prise de contact avec d'autres responsables du traitement ou sous-traitants susceptibles d'avoir été impliqués dans un élargissement du traitement, par exemple lorsque des données ont été partagées par erreur avec des tiers;
- les mesures prises en temps utile par le responsable du traitement ou le sous-traitant pour empêcher que la violation se poursuive ou qu'elle atteigne un niveau ou un stade tel que ses conséquences auraient été beaucoup plus graves.

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32

Par comparaison avec la directive 95/46/CE sur la protection des données, le règlement responsabilise beaucoup plus le responsable du traitement.

Le degré de responsabilité du responsable du traitement ou du sous-traitant peut être évalué, dans le contexte de l'application d'une mesure corrective appropriée, à partir des questions suivantes:

- le responsable du traitement a-t-il mis en œuvre des mesures techniques suivant les principes de protection des données dès la conception ou par défaut (article 25)?
- le responsable du traitement a-t-il mis en œuvre des mesures organisationnelles qui donnent effet aux principes de protection des données dès la conception et par défaut (article 25) à tous les niveaux de l'organisation?
- le responsable du traitement ou le sous-traitant a-t-il mis en œuvre un niveau approprié de sécurité (article 32)?
- les routines ou politiques pertinentes en matière de protection des données sont-elles connues et appliquées au niveau approprié de la direction au sein de l'organisation? (article 24)

Les articles 25 et 32 du règlement imposent aux responsables du traitement de tenir compte «*de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques*». Ces dispositions instaurent une obligation de moyens plutôt qu'une obligation de résultat, c'est-à-dire que le responsable du traitement doit effectuer les évaluations nécessaires et tirer les conclusions appropriées. 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.

Lors de cette évaluation, il convient de tenir dûment compte de toute procédure ou méthode relevant des «bonnes pratiques», lorsqu'elles existent et qu'elles s'appliquent. Il importe également de tenir compte des normes de l'industrie ainsi que des codes de conduite dans le domaine ou le métier concerné. Les codes de conduite pourraient donner une indication de ce qui constitue une pratique courante dans le domaine et du niveau de connaissance des différentes façons de faire face aux problèmes de sécurité habituels liés au traitement.

Si les bonnes pratiques devraient être l'idéal à poursuivre dans l'absolu, les circonstances particulières de chaque cas d'espèce doivent être prises en considération pour évaluer le degré de responsabilité.

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant

Ce critère vise à évaluer les antécédents de l'entité qui a commis la violation. Les autorités de contrôle devraient être conscientes du fait que cette évaluation peut avoir une portée assez large parce que tout type de violation du règlement, même si elle est de nature différente de celle examinée dans ce cadre par l'autorité de contrôle, pourrait être «pertinente» pour l'évaluation, étant donné qu'elle pourrait donner une indication du niveau général de méconnaissance ou de non-observation des règles en matière de protection des données.

L'autorité de contrôle devrait évaluer les questions suivantes:

- le responsable du traitement ou le sous-traitant a-t-il déjà commis la même violation?
- le responsable du traitement ou le sous-traitant a-t-il violé le règlement de la même manière? (par exemple, à la suite d'une mauvaise connaissance des routines existantes au sein de l'organisation ou d'une évaluation inappropriée des risques, parce qu'il n'a pas répondu en temps voulu aux demandes de la personne concernée ou qu'il a pris un retard injustifié pour répondre aux demandes, etc.)

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs

L'article 83, paragraphe 2, prévoit qu'il peut être tenu «dûment compte» du degré de coopération pour décider d'infliger ou non une amende administrative ainsi que du montant de celle-ci. Le règlement n'apporte pas de réponse précise à la question de savoir comment il convient de tenir compte des efforts des responsables du traitement ou des sous-traitants pour remédier à une violation déjà établie par l'autorité de contrôle. En outre, il est clair que les critères seraient normalement appliqués lors du calcul du montant de l'amende à infliger.

Toutefois, lorsque l'intervention du responsable du traitement a eu pour effet d'empêcher des conséquences négatives pour les droits des personnes ou de les limiter, son intervention peut également être prise en considération lors du choix d'une mesure corrective proportionnée au cas d'espèce.

La question suivante donne un exemple de cas où la coopération avec l'autorité de contrôle est susceptible d'être prise en considération:

- l'entité a-t-elle 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?

Cela dit, il ne serait pas approprié d'accorder une attention supplémentaire à la coopération déjà requise par la loi, par exemple lorsque l'entité est de toute façon tenue de permettre à l'autorité de contrôle d'accéder à ses locaux pour mener ses audits ou ses inspections.

g) les catégories de données à caractère personnel concernées par la violation

Voici quelques exemples de questions clés auxquelles l'autorité de contrôle pourrait estimer nécessaire de répondre, le cas échéant:

- La violation concerne-t-elle le traitement des catégories particulières de données visées aux articles 9 et 10 du règlement?
- Les données sont-elles directement ou indirectement identifiables?

- Le traitement implique-t-il des données dont la diffusion pourrait causer à la personne concernée un dommage immédiat ou une souffrance (qui ne relèvent pas de la catégorie visée aux articles 9 ou 10)?
- Les données sont-elles directement disponibles, sans protections techniques, ou sont-elles cryptées[13]?

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation

Une autorité de contrôle pourrait être informée de la violation à la suite d'une enquête, de plaintes, d'articles de presse, de dénonciations anonymes ou d'une notification par le responsable du traitement. Le règlement fait obligation au responsable du traitement de signaler à l'autorité de contrôle les violations de données à caractère personnel. Lorsque le responsable du traitement ne fait que remplir cette obligation, le respect de celle-ci ne peut être considéré comme un facteur atténuant. De même, l'autorité de contrôle peut considérer qu'un responsable du traitement ou un sous-traitant qui a fait preuve de négligence en ne notifiant pas la violation, ou en ne la notifiant pas de manière détaillée en raison de son incapacité à évaluer adéquatement l'ampleur de la violation, mérite une sanction plus lourde, c'est-à-dire qu'il est peu probable qu'elle considère cette violation comme étant mineure.

i) 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

Il se peut qu'une autorité de contrôle ait déjà un responsable du traitement ou un sous-traitant dans le collimateur s'il a déjà commis une violation et après des échanges nourris avec le délégué à la protection des données, s'il existe. L'autorité de contrôle tiendra dès lors compte des échanges antérieurs.

Contrairement au critère décrit au point e), ce critère d'évaluation ne vise qu'à rappeler aux autorités de contrôle qu'elles doivent se référer aux mesures qu'elles ont elles-mêmes prises précédemment à l'égard du même responsable du traitement ou sous-traitant «*concernant le même objet*»

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42

Les autorités de contrôle ont le devoir de «*[contrôler] l'application du présent règlement et [de veiller] au respect de celui-ci*» [article 57, paragraphe 1, point a)]. L'application d'un code de conduite approuvé peut être utilisée par le responsable du traitement ou le sous-traitant pour démontrer le respect de la réglementation, conformément à l'article 24, paragraphe 3, l'article 28, paragraphe 5, ou l'article 32, paragraphe 3.

En cas de violation de l'une des dispositions du règlement, l'application d'un code de conduite approuvé pourrait donner à l'autorité de contrôle une indication de la nécessité réelle d'intervenir sous la forme d'une amende administrative efficace, proportionnée et dissuasive ou sous la forme d'autres mesures correctives. D'après l'article 40, paragraphe 4, les codes de conduite approuvés comprendront «*les mécanismes permettant à l'organisme [de contrôle] de procéder au contrôle obligatoire du respect de ses dispositions*».

Lorsque le responsable du traitement ou le sous-traitant applique un code de conduite approuvé, l'autorité de contrôle peut se contenter du fait que la communauté chargée d'administrer le code prend

[13] Le fait que la violation ne concerne que des données indirectement identifiables ou même pseudonymes ou cryptées ne devrait pas toujours être considéré comme un facteur atténuant assimilable à une «prime». Pour ces violations, une évaluation globale des autres critères pourrait faire pencher modérément ou fortement la balance en faveur de l'imposition d'une amende.

elle-même les mesures appropriées à l'encontre de son membre, par exemple au travers des programmes de contrôle et d'application des règles prévus par le code de conduite lui-même. Par conséquent, l'autorité de contrôle peut considérer que de telles mesures sont suffisamment efficaces, proportionnées ou dissuasives dans ce cas particulier et qu'il n'est pas nécessaire qu'elle impose elle-même des mesures supplémentaires. Certaines formes de sanction de comportements non conformes peuvent passer par le programme de contrôle, conformément à l'article 41, paragraphe 2, point c), et à l'article 42, paragraphe 4, et comprendre la suspension ou l'exclusion du responsable du traitement ou du sous-traitant concerné de la communauté appliquant le code en question. Néanmoins, les pouvoirs de l'organisme de contrôle sont «*sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente*», ce qui signifie que l'autorité de contrôle n'est pas tenue de prendre en considération les sanctions déjà imposées dans le cadre du programme d'autorégulation.

Le non-respect de mesures d'autorégulation pourrait également être révélateur de la négligence du responsable du traitement ou du sous-traitant ou de son intention délibérée de ne pas s'y conformer.

k) 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.

La disposition donne elle-même des exemples d'autres éléments pouvant être pris en considération pour décider du caractère approprié d'une amende administrative sanctionnant une violation des dispositions de l'article 83, paragraphes 4 à 6.

Les informations sur les avantages obtenus du fait d'une violation peuvent être particulièrement importantes pour les autorités de contrôle dans la mesure où ceux-ci ne peuvent être compensés par des mesures dénuées de tout caractère pécuniaire. Par conséquent, le fait que le responsable du traitement ait retiré un avantage de la violation du règlement peut constituer une indication claire de la nécessité d'infliger une amende.

IV. Conclusions

Les réflexions sur les questions telles que celles exposées à la section précédente aideront les autorités de contrôle à établir, à partir des faits pertinents de l'espèce, les critères les plus utiles pour décider d'infliger ou non une amende administrative appropriée en plus ou à la place des autres mesures prévues à l'article 58. Compte tenu du contexte qui se dégage d'une telle évaluation, l'autorité de contrôle déterminera la mesure corrective la plus efficace, la plus proportionnée et la plus dissuasive pour réagir à la violation.

L'article 58 donne quelques orientations quant aux mesures qu'une autorité de contrôle peut choisir, étant donné que les mesures correctives sont en soi de nature différente et qu'elles visent essentiellement à atteindre des finalités différentes. Certaines mesures visées à l'article 58 peuvent même se cumuler et constituer ainsi une action régulatrice basée sur plusieurs mesures correctives.

Il n'est pas toujours nécessaire de compléter la mesure par une autre mesure corrective. Par exemple, l'efficacité et le caractère dissuasif de l'intervention de l'autorité de contrôle, qui prend dûment en compte ce qui est proportionné dans le cas d'espèce, peuvent être garantis uniquement par l'amende.

Fondamentalement, les autorités doivent rétablir le respect de la réglementation en recourant à toutes les mesures correctives dont elles disposent. Les autorités de contrôle devront également choisir la voie la plus appropriée à leur action régulatrice. Celle-ci peut comprendre par exemple des sanctions pénales (lorsqu'elles sont disponibles au niveau national).

La pratique consistant à infliger des amendes administratives de manière cohérente dans toute l'Union européenne est en pleine évolution. Des mesures devraient être prises conjointement par les autorités de contrôle pour améliorer en permanence la cohérence. Elles peuvent prendre la forme d'échanges réguliers lors d'ateliers de traitement de cas ou d'autres événements permettant la comparaison de cas tirés des niveaux infranational, national et transnational. La création d'un sous-groupe permanent rattaché à un département compétent du CEPD est recommandée pour soutenir cette activité permanente.