RGPD et amendes administratives : le CEPD présente ses lignes directrices

David Dias Matos, le 29 juillet 2022

Le Comité européen de la protection des données a présenté son projet de lignes directrices sur le calcul des amendes administratives prononcées sur la base du RGPD. La présente contribution en restitue les grandes lignes.

Comité européen de la protection des données (CEPD), Lignes directrices 4/2022 sur le calcul des amendes administratives dans le cadre du RGPD, version 1.0, du 12 mai 2022 (disponibles uniquement en anglais à ce jour).

Le 12 mai 2022, le CEPD a publié son projet de lignes directrices sur le calcul des amendes administratives dans le cadre du RGPD (Lignes Directrices). Elles viennent compléter celles concernant l'application et la fixation des amendes administratives (WP 253) portant sur les circonstances dans lesquelles infliger de telles amendes. Ces dernières ont été adoptées par le Groupe de l'Article 29 préalablement à l'entrée en vigueur du RGPD et ont été approuvées par le CEPD.

Ces Lignes Directrices ont pour but d'harmoniser la cohérence des méthodologies de calcul des amendes administratives prononcées, ainsi que d'assurer l'application et l'exécution du RGPD. À noter que le RGPD ne prévoit pas de montant minimum pour les amendes administratives, mais des montants maximums selon l'art. 83 par. 4 à 6 RGPD.

Le CEPD propose une méthode de calcul en 5 étapes pouvant se résumer comme suit.

1ère étape : Identifier les traitements de données du cas et évaluer l'application de l'art. 83 par. 3 RGPD

Les autorités de contrôle (art. 51 ss RGPD) doivent identifier quels agissements sanctionnables sont en cause et lesquels enfreignent quelle(s) disposition(s) du RGPD. Dans le cas d'un concours d'infractions, elles doivent déterminer le type de concours en l'espèce. L'idée étant de déterminer quelles infractions peuvent être sanctionnées ensemble ou séparément par une amende administrative.

2ème étape : Trouver le point de départ pour le calcul de l'amende administrative basé sur différents facteurs

Le CEPD estime que le calcul de l'amende administrative doit débuter par un « point de départ » harmonisé. Néanmoins, les autorités de contrôle restent libres de procéder au cas par cas et de fixer l'amende administrative jusqu'au maximum légal.

Pour former le point de départ du calcul, le CEPD fixe trois éléments à prendre en considération en vue d'imposer une amende administrative effective, dissuasive et proportionnée : la catégorisation des infractions par nature (i), la gravité de l'infraction (ii) et le chiffre d'affaires de l'entreprise (iii).

Concernant la catégorisation des infractions tout d'abord, le RGPD prévoit deux catégories d'infractions : celles punissables selon l'art. 83 par. 4 RGPD et celles punissables selon l'art. 83 par. 4 et 5. Pour la première catégorie, l'amende est plafonnée à EUR 10 millions ou 2% du chiffre d'affaires mondial (le plus élevé sera considéré). Pour la deuxième catégorie, l'amende ne peut excéder EUR 20 millions ou 4% du chiffre d'affaires mondial.

La catégorie dans laquelle l'infraction se trouve est un premier indicateur de la gravité de celle-ci. Le RGPD requiert des autorités de contrôle qu'elles prennent en compte d'autres facteurs tels que la nature, la gravité et la durée de l'infraction. Elles doivent également considérer la nature, le champ et le but du traitement de données personnelles concerné, comprenant le nombre de personnes concernées affectées et le dommage qu'elles ont subi (art. 83 par. 3 let. a RGPD). Le caractère intentionnel ou négligent de l'infraction (art. 83 par. 2 let. b RGPD) et les catégories de données personnelles affectées par l'infraction (art. 83 par. 2 let. g RGPD) sont les facteurs restant à considérer.

L'évaluation de ces différents facteurs doit se faire selon les circonstances du cas concret. Elle vise à déterminer la gravité de l'infraction dans son ensemble. Les autorités de contrôle peuvent alors considérer le niveau de gravité de l'infraction comme « bas », « moyen » ou « élevé ». Selon les Lignes Directrices, pour calculer le montant de l'amende pour un niveau jugé « bas », les autorités détermineront un montant de départ pour le calcul entre 0 et 10% du maximum légal applicable. Pour un niveau « moyen », le montant de départ se situera entre 10 et 20% et pour un niveau « élevé », entre 20 et 100%.

Le RGPD s'applique tant aux petites entreprises qu'aux grandes multinationales. Partant, l'amende doit tenir compte de la taille de l'entreprise, car le montant peut avoir un impact très différent en fonction du cas et conduire certaines entreprises à la faillite. Tel est le cas

de l'entreprise néerlandaise VoetbalTV contre qui l'autorité néerlandaise de protection des données a prononcé une amende de EUR 575'000 avant que celle-ci ne soit annulée par le Conseil d'État (cf. Décision du Conseil d'État du 27 juillet 2022, Uitspraak 202100045/1/A3).

Les Lignes Directrices indiquent que les autorités peuvent envisager d'ajuster le montant de départ correspondant à la gravité de l'infraction en fonction du chiffre d'affaires de l'entreprise. Par exemple, les Lignes Directrices indiquent que pour les entreprises dont le chiffre d'affaires annuel est de moins de EUR 2 millions, les autorités peuvent envisager de procéder au calcul sur la base d'une somme à hauteur de 0,2% du montant de départ identifié. En revanche, pour les entreprises dont le chiffre d'affaires annuel est égal ou supérieur à EUR 250 millions, les Lignes Directrices suggèrent que les autorités procèdent aux calculs sur la base d'une somme allant jusqu'à 50% du montant de départ identifié.

3ème étape : Prise en compte de facteurs aggravants ou atténuants susceptibles d'augmenter ou de diminuer le montant de l'amende

Après avoir évaluer la nature, la gravité et la durée de l'infraction, ainsi que son caractère intentionnel ou négligent et les catégories de données concernées, les autorités de contrôle doivent prendre en compte les facteurs aggravants ou atténuants de l'art. 83 par. 2 RGPD. Ces critères doivent être pris en compte de manière globale face aux circonstances résultant de l'investigation des autorités.

Tout d'abord, les autorités de contrôle doivent regarder quelles ont été les mesures prises par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées (art. 83 par. 2 let. c RGPD). Ensuite, elles doivent se poser la question de savoir dans quelle mesure le responsable du traitement et le sous-traitant ont « fait ce que l'on pouvait attendre d'eux » compte tenu de la nature, des finalités ou de l'ampleur du traitement, au regard des mesures techniques et organisationnelles implémentées en vertu des art. 25 à 32 RGPD (art. 83 par. 2 let. d RGPD).

Conformément à l'art. 83 par. 2 let. e RGPD, les autorités doivent ensuite examiner si d'autres infractions ont été commises par le passé par le responsable ou le sous-traitant. Les Lignes Directrices relèvent que le facteur temps est ici important. Plus le temps entre les deux infractions est long, moins les autorités devraient prendre compte ce critère dans leur calcul. Il est également important de vérifier si l'infraction porte sur le même objet que la nouvelle ou sur un traitement ou des données différents.

Finalement, d'autres facteurs sont encore à analyser, tels que le degré de coopération établi

avec les autorités en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs (art. 83 par. 2 let. f RGPD) ; la manière dont elles ont eu connaissance de la violation ainsi que sa notification éventuelle par le responsable du traitement ou le sous-traitant (art. 83 par. 2 let. g RGPD) ou encore le respect de mesures précédemment ordonnées relatives au même objet (art. 83 par. 2 let. i RGPD). De plus, l'art. 83 par. 2 let. k RGPD laisse la porte ouverte à d'autres circonstances aggravantes ou atténuantes pouvant apparaître.

4ème étape : Déterminer les plafonds légaux des amendes administratives et veiller à ce qu'elles ne les dépassent pas

Comme vu précédemment, le RGPD prévoit deux types de montants maximums pour les amendes administratives à son art. 83 par. 4 à 6 RGPD. Il y a, d'un côté, les montants dits « statiques ». Il s'agit des montant de EUR 10 millions et 20 millions pour les amendes, respectivement, des paragraphes 4 et 5–6 de l'art. 83 RGPD. De l'autre, ce sont les montants dits dynamiques qui sont un pourcentage du chiffre d'affaires mondial de l'entreprise visée, soit 2 et 4% de celui-ci. Le montant le plus élevé est retenu.

Pour déterminer ce chiffre d'affaires, le CEPD rappelle que le terme « entreprise » utilisé aux alinéas 4 à 6, doit être compris de la même manière que dans les articles 101 et 102 TFUE. Il s'agit donc d'une conception économique de l'entreprise qui peut être composée de plusieurs entités légales. Ces alinéas suivent le principe de la « responsabilité directe de l'entreprise ». Cela signifie que tous les actes et infractions commis par une personne physique autorisée à agir pour l'entreprise sont attribués et considérés comme réalisés par elle.

Finalement, le chiffre d'affaires à prendre en compte est celui de l'exercice de l'année précédant la décision d'amender l'entreprise.

5ème étape : Analyser si le montant final calculé répond aux exigences d'efficacité, de dissuasion et de proportionnalité ou si des ajustements supplémentaires du montant sont nécessaires

Chaque amende administrative prononcée doit respecter ces trois exigences. Cela signifie que le montant doit être adapté à l'infraction commise dans son contexte spécifique. Les autorités sont donc tenues d'augmenter ou de diminuer le montant de l'amende afin qu'elle remplisse les critères, tout en ne dépassant pas son maximum légal.

De manière générale, une amende est considérée comme effective lorsqu'elle atteint les objectifs pour lesquels elle a été imposée, soit le rétablissement du respect de la loi, la sanc-

tion de comportements illicites ou les deux.

Ensuite, le principe de proportionnalité requiert que les mesures adoptées soient appropriées et nécessaire pour atteindre les objectifs légitimes poursuivis. Cette proportionnalité passe aussi par la prise en compte de la gravité de l'infraction et de la taille de l'entreprise qui l'a commise.

Finalement, l'amende doit avoir un « véritable effet dissuasif ». Pour cela, elle doit réunir deux composantes : un effet général (décourager d'autres personnes à commettre la même infraction dans le futur) et un effet spécifique (décourager son destinataire à reproduire l'infraction). De surcroit, non seulement la nature et le niveau de l'amende sont décisifs, mais aussi la probabilité de se voir amender.

Une méthodologie reproduisible en Suisse ?

La nouvelle Loi fédérale sur la protection des données (nLPD) qui devrait entrer en vigueur à partir du 1er septembre 2023 a été alignée en grande partie sur le RGPD. Cependant, quelques différences subsistent, notamment par rapport aux sanctions. Tout d'abord, la nLPD introduit des amendes pénales et non administratives et ce, jusqu'à un maximum de CHF 250'000, bien loin des EUR 20 millions ou 4% du chiffre d'affaires mondial du RGPD. Elles visent cependant la personne responsable (directeur et/ou décideur) et non l'entreprise en tant que telle. Elles ne seront pas prononcées par le PFPDT, mais pas les autorités de poursuite pénale. La méthodologie adoptée par le CEPD ne paraît donc pas reproduisible en Suisse.

Pour une analyse détaillée des dispositions pénales de la nLPD, voir notre recension de l'article « *Die Strafbestimmungen des neuen DSG* » de David Rosenthal et Seraina Gubler (cf. https://swissprivacy.law/75/).

Proposition de citation : David Dias Matos, RGPD et amendes administratives : le CEPD présente ses lignes directrices, 29 juillet 2022 *in* www.swissprivacy.law/162