

## Lignes directrices du Comité européen de la protection des données sur le calcul des amendes

Retour sur l'adoption le 12 mai 2022 des lignes directrices du CEPD relatives aux amendes prononcées par les autorités de contrôle : une méthodologie de calcul des amendes en vue d'une harmonisation des pratiques.



### Si vous n'avez que 30 secondes

Le Comité européen de la protection des données (« CEPD ») a adopté le 12 mai 2022 des lignes directrices incluant une méthodologie harmonisée de calcul des amendes administratives en 5 étapes à mettre en œuvre par les autorités européennes de contrôle en matière de données personnelles (dont la CNIL). La détermination du montant des amendes étant à la discrétion de chacune des autorités de contrôle, ces lignes directrices participent à l'objectif recherché par le CEPD d'une équivalence des sanctions dans l'ensemble des États membres de l'Union européenne (« UE »).

L'autorité de contrôle devant procéder à cette évaluation de l'amende « *selon les caractéristiques propres à chaque cas* » (article 83 du RGPD), le risque est grand que chaque autorité de contrôle mette en œuvre ses propres modalités de calcul et que des divergences d'interprétation se fassent jour. Par ailleurs, tandis que le RGPD prévoit des plafonds d'amende (article 83 alinéa 4 à 6), le texte ne prévoit en revanche aucun montant minimum d'amende.

Par conséquent, ces nouvelles directrices peuvent permettre, le cas échéant, (i) aux autorités de contrôle d'harmoniser leurs pratiques ; (ii) aux responsables de traitement ou sous-traitants d'évaluer le risque financier d'une non-conformité au RGPD.

Si ces lignes directrices ont vocation à s'appliquer à l'ensemble des manquements sanctionnés par les autorités, elles seront tout particulièrement utiles dans les hypothèses où le mécanisme du guichet unique devant une autorité « chef de file » n'est pas applicable dès lors que le responsable de traitement ou le sous-traitant a son siège hors UE (notamment dans l'affaire Google, cf. CNIL, délib. de la formation restreinte n° SAN-2019-001, 21 janv. 2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC) et peut être attrait devant plusieurs autorités de contrôle pour un même traitement mis en œuvre dans plusieurs États membres de l'UE.

Néanmoins, leur apport demeure limité dans la mesure où le montant de l'amende est librement apprécié par l'autorité de contrôle, sous réserve des dispositions de l'article 83 du RGPD, et que ces lignes directrices n'ont bien sûr pas vocation à instaurer un barème d'amende qui lierait les autorités.

### Pour approfondir :

Ces lignes directrices, qui sont soumises à une consultation publique durant 6 semaines, à l'issue desquelles une version finale sera adoptée, viennent compléter celles sur l'application et la fixation des amendes administratives dans le cadre du RGPD adoptées le 3 octobre 2017 consacrées aux circonstances dans lesquelles infliger une amende.

Pour rappel, l'article 83 du RGPD liste quelques critères de détermination du montant des amendes.

Outre le fait qu'elles doivent être effectives, proportionnelles et dissuasives, le calcul de l'amende doit prendre en compte notamment :

- 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 ;
- Le fait que la violation a été commise délibérément ou par négligence ;
- Toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;
- 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 du RGPD ;
- Toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;
- 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 ;
- Les catégories de données à caractère personnel concernées par la violation.

Afin d'harmoniser les modalités de calcul des amendes, le CEPD propose une méthodologie très précise en 5 étapes, illustrées par de nombreux exemples :

### **1<sup>ère</sup> étape : les manquements au RGPD**

Il s'agit d'apprécier si les faits litigieux concernent un seul ou plusieurs manquements au RGPD, l'objectif étant de déterminer si l'ensemble des manquements doivent être sanctionnés ou non par une amende.

### **2<sup>ème</sup> étape : les bases de calcul de l'amende**

Trois facteurs sont à prendre en compte comme base de calcul de l'amende.

- i. La nature du manquement (article 83 al. 4 à 6 du RGPD).

Le RGPD prévoit deux catégories de manquements :

- Les manquements sanctionnés par l'article 83 al. 4 du RGPD, passibles d'une amende maximale de 10 millions d'euros ou de 2 % du chiffre d'affaires annuel de l'entreprise, le montant le plus élevé étant retenu (par exemple, le manquement à l'obligation de signer un contrat de traitement de données entre le responsable de traitement et le sous-traitant, le manquement à l'obligation de tenir un registre des activités de traitement, etc.) ;
- Et les manquements sanctionnés par l'article 83 al. 5 et 6 du RGPD, passibles d'une amende maximale de 20 millions d'euros ou de 4 % du chiffre d'affaires annuel de l'entreprise, le montant le plus élevé étant également retenu (par exemple, l'absence de base légale du traitement, le manquement à l'obligation d'information des personnes concernées, un manquement aux dispositions relatives aux transferts hors Union européenne, etc.).

- ii. La gravité du manquement (article 83 al. 2 du RGPD) appréciée en fonction de la nature et de la finalité du traitement, de sa durée, de son caractère intentionnel ou non intentionnel, des données à caractère personnel qui font l'objet du manquement, du nombre de personnes concernées.

- iii. Le chiffre d'affaires du responsable de traitement ou du sous-traitant, lequel fait fonction d'assiette de calcul de l'amende.

### **3<sup>ème</sup> étape : les facteurs aggravants ou atténuants du montant de l'amende**

L'autorité de contrôle doit prendre en compte les facteurs aggravants ou atténuants permettant d'ajuster le montant de l'amende, notamment en fonction des facteurs suivants (article 83 alinéa 2 du RGPD) :

- Les mesures prises par le responsable du traitement ou le sous-traitant pour atténuer les dommages subis par les personnes concernées ;
- Le degré de responsabilité du responsable de traitement ou du sous-traitant ;
- Les manquements antérieurs du responsable de traitement ou du sous-traitant ;
- Le degré de coopération avec l'autorité de contrôle afin de remédier au manquement et d'atténuer les éventuels effets négatifs du manquement
- Les conditions dans lesquelles le manquement a été porté à la connaissance de l'autorité de contrôle ;
- Toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telles que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

#### 4<sup>ème</sup> étape : le plafond légal de l'amende

L'autorité de contrôle doit veiller à ce que les plafonds susvisés ne soient pas dépassés.

#### 5<sup>ème</sup> étape : la validation finale du montant de l'amende

Il appartient enfin à l'autorité de contrôle de valider le montant final de l'amende au regard des exigences d'efficacité, de dissuasion et de proportionnalité prévues par le RGPD, l'autorité de contrôle pouvant, le cas échéant, ajuster le montant de l'amende à la hausse (si le montant est non dissuasif), comme à la baisse (risque d'insolvabilité du responsable de traitement ou sous-traitant).

L'apport de ces lignes directrices reste limité, car si elles permettent d'harmoniser le raisonnement mis en œuvre par l'autorité de contrôle pour calculer l'amende ; in fine, l'autorité de contrôle peut librement ajuster son montant pour tenir compte du contexte (comme l'illustre très bien l'étape n°5), et pour ainsi dire en équité.

## L'ÉQUIPE DROIT IT/IP/DATA DE LEXCASE



### Iliana BOUBEKEUR

Avocate associée

[iboubekeur@lexcase.com](mailto:iboubekeur@lexcase.com)



### Guillaume BUSSEUIL

Collaborateur

[gbusseuil@lexcase.com](mailto:gbusseuil@lexcase.com)



### Manon FAUCHER

Collaborateur

[mfaucher@lexcase.com](mailto:mfaucher@lexcase.com)

[www.lexcase.com](http://www.lexcase.com)

