n°36 Avril 2023
#36 April 2023

Lexing Insights

Le réseau Lexing® vous informe – The Lexing® network informs you

BILAN 2022 DES AMENDES PRONONCEES PAR LES APD

FINES BY DATA PROTECTION AUTHORITIES IN 2022

PANORAMA DES CONDAMNATIONS 2022

- Les 2 dernières années ont été marquées par un accroissement important de condamnations par les autorités en charge de protection des données, que ce soit à l'encontre des organismes privés, mais aussi, et de plus en plus, des organismes publics.
- Bien entendu, les grandes entreprises informatiques, dont Google ou Meta, ont été régulièrement condamnées, pour des montants souvent extrêmement importants, mais les entreprises plus modestes ou des organismes publics font aussi, et de plus en plus régulièrement, l'objet de poursuites.
- Par ailleurs, la pression exercée sur les autorités de protection des données par des associations ou groupes de consommateurs est un phénomène grandissant que les organisations ne devraient pas sous-estimer dans leur approche de mise en conformité.
- Enfin, la question des flux transfrontières vers les Etats-Unis reste, à ce jour, un sujet non totalement résolu pour les entreprises européennes et qui a déjà été l'occasion d'un certain nombre de sanctions, notamment, sur la question des cookies.
- Dans ce numéro, nous vous proposons un panorama des condamnations prononcées en 2022 par les autorités en charge de la protection des données en Afrique du Sud, Belgique, Chine, Espagne, Grèce et Hongrie.

OVERVIEW OF THE 2022 CONVICTIONS

- Over the last 2 years, there have been a significant increase in the number of convictions by data protection authorities against private organizations and, more and more, against public organizations as well.
- Of course, large IT companies, such as Google or Meta, have been regularly condemned, often for extremely large amounts, but smaller companies or public bodies are also prosecuted, more and more regularly.
- Furthermore, pressure on data protection authorities from consumer groups or associations is a growing phenomenon that organizations should not underestimate in terms of compliance.
- Finally, the matter of cross-border flows to the United States remains nowadays an unresolved issue for European companies. It has as well led to a certain number of sanctions, in particular, in respect of cookies.
- In this issue, we offer you an overview of the 2022 convictions by data protection authorities in, Belgium, China, Greece, Hungary, South Africa, and Spain.

Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leurs pays respectifs.

Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

https://lexing.network

FREDERIC FORSTER

Vice-président du réseau Lexing® et Directeur du pôle Industries et services informatiques, télécoms et bancaires du cabinet Lexing Alain Bensoussan-Avocats

VP of Lexing® network and Head of the Industries & IT, Telecoms and Banking Services division of Lexing Alain Bensoussan-Avocats

Bilan 2022 des amendes prononcées par les autorités en Afrique

▪ Les autorités chargées de la protection des données en Afrique ont commencé à infliger des amendes aux organisations qui ne respectent pas la législation en matière de protection des données. Cet article présente deux affaires récentes en Angola et au Kenya, et décrit les enseignements à en tirer pour les responsables du traitement.

Angola : l'opérateur de réseau mobile Africell condamné à une amende de 138 000 euros pour défaut d'autorisation préalable

▪ En janvier 2023, l'Agence nationale de protection des données (NDPA) d'Angola a infligé une amende de 150 000 dollars (environ 138 000 euros) à la société Africell car cette dernière n'avait pas obtenu l'autorisation préalable de la NDPA pour procéder au traitement des données personnelles de ses clients. En l'espèce, la NDPA a néanmoins fait preuve d'indulgence à l'égard d'Africell en lui imposant une amende moins élevée que prévue aux motifs que l'opérateur de réseau mobile :

- a pris des mesures immédiates pour garantir, à l'avenir, le respect de la loi sur la protection des données ;
- n'a pas précédemment commis de violation de la législation sur la protection des données. Il s'agissait, en effet, du premier incident enregistré pour ce contrevenant ;
- s'est montré très coopératif pendant l'enquête de la NDPA ;
- n'a pas obtenu d'avantage financier du fait de la violation.

Bilan et enseignements

▪ En Afrique, les lois sur la protection des données des différents pays **(1)** sont similaires à 80 % et l'obtention d'une autorisation préalable d'une autorité de protection des données avant de procéder au traitement de certains types de données personnelles est une exigence courante dans la plupart des pays africains. Les responsables du traitement peuvent donc éviter ce type d'amende en s'assurant de bien obtenir l'autorisation préalable d'une autorité de protection des données lorsque la loi concernée l'exige.

(1) https://www.michalsons.com/blog/data-protection-laws-in-africa/64458

Kenya : le constructeur de smartphones Oppo condamné à une amende de 39 000 euros pour ne pas s'être conformé à un avis d'exécution

▪ Une personne a déposé une plainte contre la société Oppo pour avoir publié sa photo sur la page d'un des réseaux sociaux de la société sans son consentement.

▪ Dans un premier temps, le bureau du commissaire à la protection des données du Kenya (ODPC) a prononcé un avis d'exécution mettant en demeure le

constructeur de smartphones de mettre en œuvre deux mesures : (1) obtenir le consentement des personnes concernées pour utiliser leurs données à caractère personnel à des fins commerciales ; et (2) mettre en place une procédure de réclamation interne pour permettre aux personnes concernées de formuler des plaintes directement auprès d'Oppo.

▪ Dans un second temps, compte tenu du non-respect de cette mise en demeure par Oppo, l'ODPC a, en décembre 2022, prononcé, dans son premier avis de sanction **(2)**, une amende d'un montant de 5 millions de shillings kenyans (environ 39 000 euros) à son encontre.

(2) https://twitter.com/ODPC_KE/status/1605615980616351744

Bilan et enseignements

▪ Un avis d'exécution (*enforcement notice*) émanant d'une autorité de protection des données a pour objet de vous mettre en demeure de faire ou de ne pas faire certaines actions. Il contient une liste d'actions qu'un responsable du traitement doit mettre en œuvre, dans un délai prescrit, pour assurer sa mise en conformité à la réglementation en matière de protection des données. Si vous recevez un tel document d'une autorité de protection des données, ne l'ignorez pas, prenez le temps d'examiner ce que l'autorité vous demande de faire et mettez en œuvre les mesures adéquates et nécessaires. Veillez également à respecter le délai prescrit afin d'éviter toute condamnation qui pourraient par la suite être prononcées dans le cadre d'un avis de sanction (*penalty notice*).

Conclusion

▪ Bien que les autorités africaines de protection des données n'aient infligé que trois amendes au cours de l'année 2022, les sanctions pécuniaires devraient se multiplier en 2023. L'autorité sud-africaine de protection des données (*Information Regulator*) enquête actuellement sur des plaintes et a déjà saisi sa formation restreinte à l'encontre d'un ministère **(3)**. La prochaine amende d'une autorité africaine devrait donc émaner d'Afrique du Sud.

(3) https://www.michalsons.com/blog/regulator-refers-the-department-of-health-to-enforcement-committee/64137

SHAMAA SHEIK

south-africa@lexing.network

Administrative fines by the African data protection authorities in 2022

▪ Data protection authorities in Africa have begun fining organisations for non-compliance with data protection laws. In this article, we highlight two recent case studies in Angola and Kenya. We also provide insights into what organisations can learn from the fines that the authorities issued.

Angola: Africell fined $150 000 for failing to get prior authorisation

▪ In January 2023, the National Data Protection Agency (NDPA) fined Africell $150 000 because Africell did not get prior authorisation from the NDPA when they processed their customers' personal data. The NDPA showed some leniency towards Africell by imposing a lower fine on them because they:

- took immediate steps to ensure compliance with data protection law in the future.
- did not violate data protection laws in the past. This was their first incident on record.
- were very cooperative during the NDPA's investigation.
- did not gain economically despite processing their customer's personal data without prior authorisation.

Key takeaways from this case study

▪ The Data Protection Laws of Africa **(1)** are 80% similar. For example, getting prior authorisation from a data protection authority to process certain types of personal data is a common requirement in most African countries. Organisations can avoid this type of fine altogether by ensuring that they obtain prior authorisation from a data protection authority if the law requires them to do so.

Kenya: Oppo fined KES 5 million for not complying with an enforcement notice

▪ A data subject lodged a complaint against Oppo because they published the data subject's photo on Otto's social media page without the data subject's consent. In December 2022, the Office of the Data Protection Commissioner (ODPC) issued its first penalty notice **(2)** (or enforcement notice in other jurisdictions) against Oppo for KES 5 million because they did not comply with the ODPC's enforcement notice.

▪ In the enforcement notice, the ODPC instructed Oppo to implement two policies: (1) to get consent from data subjects to use their personal data for commercial purposes; and (2) an internal complaints process to enable data subjects to complain to Oppo directly.

(1) https://www.michalsons.com/blog/data-protection-laws-in-africa/64458

(2) https://twitter.com/ODPC_KE/status/1605615980616351744

Key takeaways from this case study

▪ An enforcement notice from a data protection authority contains a list of actions that a controller should take, within a prescribed period, to rectify their non-compliance with the data protection law. If you receive an enforcement notice from a data protection authority do not ignore it. Take the time to look at what the authority is asking you to rectify and do it. Make sure that you complete the order in the enforcement notice within the prescribed time period to avoid non-compliance.

Conclusion

▪ Although there were only three fines from African data protection authorities over the last year, we expect to see many more fines in 2023. South Africa's data protection authority, the information regulator, is investigating complaints and has already referred a government department to the enforcement committee for investigation (3). It's therefore likely that the next fine will be from South Africa.

(3) https://www.michalsons.com/blog/regulator-refers-the-department-of-health-to-enforcement-committee/64137

SHAMAA SHEIK

south-africa@lexing.network

Bilan 2022 des amendes prononcées par l'APD en Belgique

- À l'heure du bilan de l'année 2022 et des amendes prononcées par l'autorité belge de protection des données (APD), nous constatons que l'APD accélère encore le rythme. Après avoir pris 143 décisions en 2021 **(1)**, la chambre contentieuse a battu son record en publiant pas moins de 178 décisions en 2022.
- Sur ces 178 décisions, seulement 12 décisions ont débouché sur l'imposition d'amendes administratives. Bien que ce chiffre puisse paraître dérisoire à première vue, il convient de garder à l'esprit les circonstances suivantes :
  - la loi belge ne permet pas à l'APD d'infliger des amendes administratives aux autorités publiques **(2)** ;
  - la somme des douze amendes administratives prononcées en 2022 atteint 738.900€, ce qui représente plus du double de ce qui avait été comptabilisé en 2021 (301.000€) ;
  - l'APD a notamment condamné IAB Europe au paiement de 250.000 euros pour avoir manqué à ses obligations dans la mise en œuvre du « Transparency & Consent framework » **(3)** ;
  - l'emploi de caméras thermiques pendant la crise covid a également causé la condamnation de deux aéroports belges au paiement de 220.000 euros (aéroport de Bruxelles) **(4)** et 100.000 euros (aéroport de Charleroi) **(5)**. Ces amendes ont néanmoins été diminuées par la Cour des Marchés, autorité de recours des décisions de l'APD, en raison de l'absence de prise en compte de certaines circonstances atténuantes **(6)**.
- L'année 2022 marque également l'apparition d'une nouvelle pratique au sein de la chambre contentieuse : la transaction :
  - depuis sa création, l'APD peut proposer des transactions pour mettre fin à une procédure et ce, sans qu'un examen sur le fond de l'affaire n'ait lieu **(7)**. À notre connaissance, cette faculté n'a pourtant été utilisée pour la première fois qu'en 2022 ;
  - en réalité, l'APD a eu recours à la transaction à dix reprises pour clore des procédures relatives à l'utilisation de cookies. L'intérêt accru de l'APD pour le respect des règles applicables aux cookies ressort de sa stratégie 2020-2025 **(8)**. Pour atteindre ses objectifs, l'APD a missionné le service d'inspection pour réaliser une enquête d'envergure sur le respect des réglementations sur les cookies par les médias d'information belges ; suite à ce rapport, l'APD a condamné deux éditeurs de presse à une amende de 50.000 EUR **(9)** chacun. Au regard du grand nombre de dossiers similaires en attente d'être examinés entraînant de longs délais de traitement pour la totalité des dossiers, l'APD a proposé une transaction aux dix autres éditeurs de sites. Ces éditeurs ont tous accepté de payer le montant transactionnel de 10.000 euros afin d'éviter une condamnation sur le fond par la chambre contentieuse **(10)**.

REFERENCES

(1) Rapport annuel

(2) Article 83.7 du RGPD et article 221, §2 de la loi du 30 juillet 2018.

(3) Décision quant au fond 21/2022 du 2 février 2022

(4) Décision quant au fond 48/2022 du 4 avril 2022

(5) Décision quant au fond 47/2022 du 4 avril 2022

(6) Arrêts 2022/AR/560&564, et 2022/AR/556 de la Cour des marchés du 7 décembre 2022,

(7) Article 95 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données

(8) Plan stratégique 2020-2025

(9) Décisions quant au fond 85/2022 du 25 mai 2022 et 103/2022 du 16 juin 2022

(10) Décision quant au fond de transaction 150/2022 du 21 octobre 2022, décision 151 du 21 octobre 2022, décisions 153, 154, 155, 156, 157 du 4 novembre 2022 et décisions 168, 169 et 170 du 22 novembre 2022

VICTORIA RUELLE

belgium@lexing.network

Administrative fines by the Belgian data protection authority in 2022

- As we look back at 2022 and the fines issued by the Belgian Data Protection Authority (DPA), we see that the DPA is picking up the pace again. After issuing 143 decisions in 2021 **(1)**, the litigation chamber broke its record by issuing no less than 178 decisions in 2022.
- Among these 178 decisions, only twelve resulted in the imposition of administrative fines. Although this number may seem derisory at first glance, the following circumstances should be kept in mind:
  - Belgian law does not allow the DPA to impose administrative fines on public authorities **(2)**;
  - the sum of the twelve administrative fines imposed in 2022 amounts to €738,900, which is more than twice what was imposed in 2021 (€301,000);
  - in particular, the DPA ordered IAB Europe to pay €250,000 for failing to comply with its obligations when implementing the "Transparency & Consent framework" **(3)**;
  - the use of thermal cameras during the Covid crisis also led to two Belgian airports being fined €220,000 (Brussels Airport) **(4)** and €100,000 (Charleroi Airport) **(5)**. These fines were nevertheless reduced by the Market Court, the appeal authority for DPA decisions, due to the failure to take into account certain mitigating circumstances **(6)**.
- The year 2022 also marks the appearance of a new practice within the litigation chamber: the transaction:
  - since its creation, the Belgian DPA has the ability to propose settlements or transactions in order to put an end to a proceeding, without any examination of the merits of the case **(7)**. To the best of our knowledge, however, this faculty was only used for the first time in 2022;
  - in fact, the DPA has used the transaction on ten occasions to close proceedings related to the use of cookies. The DPA's increased focus on cookie compliance is reflected in its Strategy for 2020-2025 **(8)**. To achieve its objectives, the DPA commissioned the inspection service to conduct a major investigation on the compliance by the Belgian news media with cookie regulations. Based on the findings on this report, the DPA fined two media publishers €50,000 each **(9)**. Due to the large number of similar cases awaiting review before the DPA, resulting in long processing times for all cases, the DPA proposed a transaction to the remaining ten publishers. These publishers all agreed to pay the settlement amount of €10,000 in order to avoid a conviction on the merits by the litigation chamber **(10)**.

REFERENCES

(1) Annual report

(2) Article 83.7 of the GDPR and Article 221, §2 of the Law of July 30, 2018.

(3) Decision on the merits 21/2022 of February 2, 2022

(4) Decision on the merits 48/2022 of April 4, 2022

(5) Decision on the merits 47/2022 of April 4, 2022

(6) Decisions 2022/AR/560&564, and 2022/AR/556 of the Market Court of December 7, 2022

(7) Article 95 of the Law of December 3, 2017 establishing the Belgian Data Protection Authority

(8) Strategic Plan 2020-2025

(9) Decisions on the merits 85/2022 of May 25, 2022 and 103/2022 of June 16, 2022

(10) Decision on the merits 150/2022 of October 21, 2022, decision 151 of October 21, 2022, decisions 153, 154, 155, 156, 157 of November 4, 2022 and decisions 168, 169 and 170 of November 22, 2022.

VICTORIA RUELLE

belgium@lexing.network

Bilan 2022 des amendes prononcées en Chine

▪ La violation de la loi sur la protection des informations personnelles (PIPL) de la République populaire de Chine peut entraîner l'imposition de sanctions administratives tant à l'encontre des entreprises responsables du traitement que de leur dirigeants personnes physiques :

- (a) les sanctions administratives à l'encontre du responsable du traitement contrevenant vont de l'application de mesures correctives à l'avertissement, en passant par la confiscation des revenus illicites et la suspension des activités de l'entreprise contrevenante ;
- (b) les responsables du traitement qui ne se mettent pas en conformité en n'adoptant pas de mesures correctives s'exposent à une amende allant jusqu'à un million de yuans (environ 133 000 euros) ;
- (c) une amende allant de 10 000 à 100 000 yuans (entre 1 300 et 13 300 euros) peut être imposée aux dirigeants et collaborateurs directement tenus pour responsables des actes de violation identifiés ; et
- (d) en cas de violations graves, les autorités compétentes au niveau provincial ou national peuvent ordonner l'application de mesures correctives, la confiscation des revenus illicites et imposer, cumulativement, une amende pouvant aller jusqu'à 50 millions yuans (environ 6,6 millions d'euros) ou jusqu'à 5 % du chiffre d'affaires réaliser par le responsable du traitement au cours de l'année précédente, ainsi qu'une suspension temporairement ou permanente de l'activité commerciale ou le retrait la licence commerciale dont bénéficie le responsable du traitement. Les dirigeants personnes physiques ou toutes autres personnes directement tenues pour responsables de la violation s'exposent à une amende allant de 100 000 à 1 million de yuans (entre 13 300 et 133 000 euros) et peuvent se voir interdire d'occuper certaines fonctions (telles que des postes de direction dans le domaine de la protection des données personnelles) pendant une certaine période.

▪ Depuis l'entrée en vigueur de la PIPL le 1er novembre 2021, les autorités chinoises ont infligé des amendes administratives à un certain nombre d'entreprises et de personnes ayant enfreint cette loi.

▪ A titre d'illustration, le 21 juillet 2022, l'Administration du cyberespace de Chine a imposé une amende de 8,026 milliards de yuans (1,2 milliards d'euros) à DiDi Global Inc., le principal opérateur de VTC du pays. En outre, M. Cheng Wei (Président et PDG de DiDi Global Inc.) et Mme Liu Qing (Présidente de DiDi Global Inc.) ont chacun écopé d'une amende de 1 million de yuans (environ 133 000 euros), en application de la PIPL ainsi que de la loi sur la cybersécurité, de la loi sur la sécurité des données et de la loi sur les sanctions administratives. La décision a été motivée, entre autres, par le traitement excessif effectué par DiDi de données personnelles concernant les passagers et les conducteurs.

JUN YANG

china@lexing.network

Administrative fines by the Chinese data protection authority in 2022

▪ Breach of the PRC Personal Information Protection Law (PIPL) may result in administrative sanctions under PIPL for both corporate processors in question and the person in charge:

- (a) administrative sanctions against breaching processor range from order of rectification, warning, confiscation of illegal revenues to the suspension of breaching app;
- (b) for those breaching processor resisting rectifying, a fine up to one million RMB may be concurrently imposed;
- (c) a fine ranging from RMB10k to 100k may be imposed on the person in charge and those directly held accountable for the breaching acts identified; and
- (d) in case of serious circumstances, the competent authorities at provincial or national level may issue order of rectification, confiscation of illegal revenues and concurrently impose a fine up to RMB50M or up to 5 percent of the processor's business turnover in preceding year plus order to suspend the business operation or withdrawal of operation or business license of the processor. The persons in charge or other persons directly held accountable may be fined in an amount ranging from RMB100K to RMB1M and barred from assuming position such as director, senior manager or person in charge of personal information protection within certain time period.

▪ The Chinese regulatory authorities have imposed administrative fines to a number of breaching enterprises and individuals since the PIPL took effect on November 1, 2021.

▪ To just quote the following for illustrative purpose, on July 21, 2022, the Cyberspace Administration of China imposed a fine of RMB 8.026 billion on DiDi Global Inc., the leading taxi-hailing platform operator in the country and a fine of RMB 1 million on Mr. CHENG Wei (Chairman and CEO of DiDi Global Inc.) and Ms. LIU Qing (President of DiDi Global Inc.) respectively in application of PIPL as well as Cyber-security Law, Data Security Law, Administrative Penalty Law. The administrative decision was motivated, among others, by DiDi's excessive processing of personal data involving both passengers and drivers.

JUN YANG

china@
lexing.network

Bilan 2022 des amendes prononcées en Espagne

▪ Les infractions les plus courantes au RGPD en Espagne ont trait aux thématiques suivantes :

- Manque de transparence : ne pas fournir d'informations claires et concises aux personnes concernées sur la manière dont leurs données personnelles seront traitées, ou fournir ces informations dans une langue qui ne leur est pas compréhensible ;
- Mesures de sécurité inadéquates : ne pas mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données personnelles, par exemple ne pas procéder au chiffrement d'informations sensibles ou ne pas maintenir les logiciels à jour ;
- Défaut de recueil du consentement : ne pas obtenir le consentement valide et explicite des personnes concernées pour le traitement de leurs données personnelles, ou ne pas leur donner un moyen clair et facile de retirer leur consentement ;
- Non-respect des droits des personnes concernées : ne pas répondre aux demandes des personnes concernées d'exercer leurs droits d'accès, de rectification ou de suppression concernant leurs données à caractère personnel, ou ne pas donner suite à ces demandes dans les délais requis ;
- Violations de données : ne pas informer l'autorité compétente et les personnes concernées d'une violation de données à caractère personnel dans les délais requis, ou ne pas prendre de mesures adéquates pour prévenir de futures violations.

▪ Florilège des amendes les plus notables imposées en Espagne pour violation du RGPD :

- Telefónica - 11,8 millions d'euros : plusieurs violations du RGPD, dont mise en place de mesures de sécurité inadéquates et absence de recueil d'un consentement valide pour le traitement des données personnelles ;
- Google - 10 millions d'euros : plusieurs violations du RGPD, et notamment transfert de données à des tiers sans base légale et entrave à l'exercice du droit à l'oubli ;
- Vodafone - 8,15 millions d'euros : plusieurs violations du RGPD, dont mise en place de mesures de protection des données insuffisantes et de procédures de consentement inadéquates ;
- Banco Santander - 2 millions d'euros : violation des principes de transparence et de confidentialité ;
- CaixaBank - 6 millions d'euros : violation des principes de transparence et de consentement ;

- Iberdrola - 6 millions d'euros : violation du principe de transparence ;
- BBVA - 5 millions d'euros : violation des principes de transparence et de consentement ;
- Facebook - 1,2 million d'euros : violation des principes de transparence et de consentement ;
- Equifax - 1 million d'euros : défaut d'obtention d'un consentement valide pour le traitement des données à caractère personnel et mesures de sécurité inadéquates ayant conduit à une violation de données affectant des millions de citoyens espagnols.

▪ Les amendes ainsi prononcées dans les affaires décrites ci-dessus soulignent l'importance de se conformer aux principes et aux exigences du RGPD, ainsi que les conséquences financières importantes qui peuvent résulter, en Espagne, en cas de non-conformité.

MARC GALLARDO

spain
@lexing.network

Administrative fines by the Spanish data protection authority in 2022

▪ The most common infringements of GDPR in Spain are related to the following areas:

- Lack of transparency: This includes failing to provide clear and concise information to individuals about how their personal data will be processed, or providing this information in a language that is not easily understood;
- Inadequate security measures: This includes not implementing appropriate technical and organizational measures to ensure the security of personal data, such as failing to encrypt sensitive information or not keeping software up to date;
- Failure to obtain consent: This includes not obtaining valid and explicit consent from individuals for the processing of their personal data, or not giving them a clear and easy way to withdraw their consent;
- Failure to honor data subject rights: This includes not responding to data subject requests to access, rectify, or delete their personal data, or not doing so within the required timeframe;
- Data breaches: This includes not notifying the competent authority and affected individuals of a personal data breach within the required timeframe, or not taking adequate measures to prevent future breaches.

▪ Some of the most notable GDPR fines imposed in Spain for these infringements include:

- Telefónica - €11.8 million: For several GDPR violations, including inadequate security measures and not obtaining valid consent for processing personal data;
- Google - €10 million: For several GDPR violations, including transferring data to third parties with no legal basis and for obstruct the exercise of the right to be forgotten;
- Vodafone - €8.15 million: For several GDPR violations, including insufficient data protection measures and inadequate consent procedures;
- Banco Santander - €2 million: for violating GDPR's principles of transparency and confidentiality;
- CaixaBank - €6 million: For violating GDPR's principles of transparency and consent;
- Iberdrola - €6 million for violating GDPR's transparency principle;
- BBVA - €5 million: For violating GDPR's transparency and consent principles;

- Facebook - €1.2 million: for violating GDPR's principles of transparency and consent;
- Equifax - €1 million: For failing to obtain valid consent for processing personal data and for inadequate security measures that led to a data breach affecting millions of Spanish citizens.

▪ These fines highlight the importance of complying with GDPR's principles and requirements, as well as the significant financial consequences that can result from non-compliance in Spain.

MARC GALLARDO

spain
@lexing.network

Bilan 2022 des amendes prononcées par la HDPA en Grèce

▪ Tout d'abord, la HDPA a imposé une amende record de 20 000 000 euros à la société Clearview AI, spécialisée dans la reconnaissance faciale, pour plusieurs violations de la législation sur la protection des données et lui a interdit de collecter et de traiter les données à caractère personnel de citoyens grecs (1). Clearview AI s'est également vue enjointe de supprimer toutes les données déjà collectées. Cette décision fait suite à une plainte déposée en mai 2021 par l'ONG de défense des droits de l'homme « Homo Digitalis » et s'inscrit dans le cadre d'une série d'amendes prononcées par plusieurs autorités européennes de protection des données (en Italie et en France notamment) contre Clearview.

▪ En outre, la HDPA a infligé à des fournisseurs grecs de services de communication des amendes allant jusqu'à 150 000 euros, sanctionnant ainsi l'absence de mesures techniques et organisationnelles appropriées pour protéger la sécurité des services qu'ils fournissent (2). Un groupe de fournisseurs de services de communication a écopé, quant à lui, d'une amende administrative de 9 250 000 euros pour plusieurs manquements : la violation des principes de licéité et de transparence, la fourniture d'informations peu claires et incomplètes aux abonnés, la mise en œuvre de mesures de sécurité inadéquates, la mauvaise application de procédures d'anonymisation et l'absence d'identification et de répartition claires des responsabilités en matière de traitement entre les sociétés du groupe. L'inadéquation des mesures de sécurité en place en cas d'incident de violation de données lui a également été reprochée (3).

▪ Dans d'autres décisions, qui ont mené à des amendes de montants beaucoup moins élevés, la HDPA sanctionné des institutions bancaires (4), un établissement d'enseignement privé (5), un centre de diagnostic médical (6), un prestataire de services postaux (7), ou encore une agence de rencontres (8). Les amendes administratives imposées vont de 15 000 euros (installation illégale de systèmes de vidéosurveillance en violation des principes de limitation des finalités et de responsabilité) à 60 000 euros (non-respect par le responsable du traitement des droits d'accès et d'effacement en violation du principe de responsabilité).

▪ Enfin, on peut relever qu'un certain nombre d'affaires examinées par l'autorité grecque concernaient des communications non sollicitées émanant de personnalités politiques. Dans ce cadre, la HDPA a imposé des amendes administratives allant de 1 000 à 5 000 euros, et a notamment pris en compte la récidive d'un responsable du traitement, la possibilité offerte aux personnes concernées d'exprimer un refus ou encore le respect du droit à l'effacement (9).

▪ En résumé, en 2022, l'autorité hellénique de protection des données a traité de nombreuses affaires visant des thématiques et des secteurs d'activité variés et a prononcé des amendes administratives record, témoignant de son application rigoureuse de la législation sur la protection des données.

REFERENCES

(1) HDPA, décision n°35/2022

(2) HDPA, décisions n°38/2022 et 39/2022

(3) HDPA, décision n°4/2022

(4) HDPA, décisions n°52/2022 et 53/2022

(5) HDPA, décision n°50/2022

(6) HDPA, décision n°36/2022

(7) HDPA, décision n°40/2022

(8) HDPA, décision n°16/2022

(9) A titre indicatif, HDPA, décisions n° 48/2022, 17/2022, et 26/2022

GEORGE A. BALLAS
&
NIKOLAOS PAPADOPOULOS

greece@lexing.network

Administrative fines by the Greek data protection authority in 2022

▪ This high-level analysis focuses on the fines issued by the Hellenic Data Protection Authority (HDPA) during the year 2022.

▪ In a landmark decision, the HDPA imposed a fine of EUR 20.000.000 on Clearview AI due to data protection legislation violations and banned the facial recognition company from collecting and processing Greeks' personal data (1). Clearview AI was also ordered to delete any data already collected. The decision originates from a May 2021 complaint by the human rights advocacy group "Homo Digitalis" and forms part of a series of fines imposed by European Data Protection Authorities on Clearview AI (in Italy and France, as well).

▪ Moreover, the HDPA imposed fines on Greek communication services providers of up to EUR 150.000 for the lack of appropriate technical and organizational measures to protect the security of the services they provide (2). Another group of communications service providers faced an administrative fine of EUR 9.250.000 (in total) due to the infringement of the principles of legality and transparency, as well as due to unclear and incomplete information provided to subscribers, inadequate security measures, incorrect implementation of anonymizing procedures, and failure to identify and allocate processing roles between the companies of the group. Further, the Decision deemed the security measures in place to be inadequate, with regard to the infrastructure used in connection with a data breach incident (3).

▪ On a lower scale, the HDPA handled cases submitted against bank institutions (4), private educational institutions (5), medical diagnostics centres (6), post-service providers (7), and even dating agencies (8). The administrative fines imposed range between EUR 15.000 in cases of illegal installation of CCTV, infringing the purpose limitation and accountability principles, to EUR 60.000 (in total) in cases where the data controller failed to satisfy the right to data access, the right to data deletion and infringed the accountability principle.

▪ On a separate note, a number of cases examined by the HDPA referred to unsolicited communication from politicians. In such cases, the HDPA imposed administrative fines ranging from EUR 1.000 to EUR 5.000, taking into account whether the data controller was a repeated offender, whether an opt-out option was presented to data subjects, and whether the right to data deletion was satisfied (9).

▪ To conclude, during the past year, the HDPA examined a number of interesting cases and imposed record administrative fines, demonstrating a rigorous approach to data protection and privacy legislation violations.

REFERENCES

(1) Decision 35/2022 of the Hellenic Data Protection Authority

(2) Decisions 38/2022 and 39/2022 of the Hellenic Data Protection Authority

(3) Decision 4/2022 of the Hellenic Data Protection Authority

(4) Decisions 52/2022 and 53/2022 of the Hellenic Data Protection Authority

(5) Decision 50/2022 of the Hellenic Data Protection Authority

(6) Decision 36/2022 of the Hellenic Data Protection Authority

(7) Decision 40/2022 of the Hellenic Data Protection Authority

(8) Decision 16/2022 of the Hellenic Data Protection Authority

(9) Indicatively, Decisions 48/2022, 17/2022, and 26/2022 of the Hellenic Data Protection Authority

GEORGE A. BALLAS
&
NIKOLAOS PAPADOPOULOS

greece@lexing.network

REFERENCES

Bilan des amendes prononcées par la NAIH en Hongrie

▪ Un examen des 134 décisions **(1)** rendues au cours des trois dernières années par l'autorité nationale de protection des données, la NAIH, fait apparaitre que les violations les plus courantes au RGPD concernaient les thématiques suivantes :

▪ **Information transparente :** la plupart des affaires étaient liées à l'article 12 du RGPD. Dans plus de la moitié des cas, l'autorité a déclaré que l'entreprise n'avait pas fourni, à la personne concernée, d'informations transparentes sur le traitement des données.

▪ **Licéité, loyauté et transparence :** dans de nombreuses affaires, l'autorité a imposé une amende à des organismes en raison de la violation de l'article 5, paragraphe 1, point a), du RGPD, relatif aux principes de licéité, de loyauté et de transparence.

▪ **Finalité du traitement :** une violation fréquente du RGPD par les responsables du traitement des données concernent l'absence de fourniture, aux personnes concernées, d'informations sur la finalité du traitement prévue à l'article 13, paragraphe 1, point b) du RGPD.

▪ **Accès aux données :** l'autorité a spécifiquement infligé des amendes aux entreprises qui n'ont pas permis à la personne concernée d'exercer son droit d'accès aux données à caractère personnel la concernant. Cette obligation est fondée sur l'article 15 du RGPD.

▪ **Limitation des finalités :** aux termes de l'article 5, paragraphe 1, point b) du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes. Dans de nombreuses affaires dont elle a été saisie, l'autorité hongroise a constaté que les entreprises n'avaient pas respecté cette obligation.

Le montant des amendes imposées par la NAIH pour violation du RGPD varie de 50 000 HUF (130 EUR) à 250 millions HUF (650 000 EUR).

Bilan des amendes les plus importantes prononcées par la NAIH :

▪ **Budapest Bank :** l'amende la plus élevée (250 millions HUF – 650 000 EUR) a été infligée à la Budapest Bank pour avoir utilisé, pendant des années, une intelligence artificielle cachée dans son service clientèle téléphonique afin d'établir le profil émotionnel des clients et, ainsi, identifier les clients à rappeler en priorité. L'autorité a estimé que l'entreprise avait enfreint les articles 5, 6, 12, 13, 21 et 24 du RGPD.

▪ **DIGI Távközlési és Szolgáltató Kft :** l'autorité a imposé une amende de 100 millions de HUF (260 000 EUR) pour violation des principes de limitation des finalités et de limitation de la conservation. En effet, la société disposait d'une base

(1) https://www.naih.hu/hatarozatok-vegzesek

de données de test qui n'était pas supprimée après utilisation et dont le contenu était accessible au public sur son site web.

- **UPC Hongrie :** l'autorité a imposé une amende de 60 millions de HUF (156 000 EUR) au motif que la société a procédé à des enregistrements vocaux dans le cadre de services à la clientèle sans avoir identifié la finalité du traitement et sans avoir mis en balance les différents intérêts en cause.

- **Amplifon :** l'autorité a imposé une amende de 80 millions HUF (200 000 EUR) à Amplifon pour l'envoi de lettres dans le cadre d'une opération de prospection commerciale. L'autorité a constaté que la société avait induit en erreur environ 300 000 à 400 000 personnes concernées sur les finalités du traitement et illégalement utilisé le consentement comme base juridique.

- **Groupe TV2 Media :** l'autorité a prononcé une amende de 10 millions de HUF (25 650 EUR) à l'encontre de ce fournisseur de médias, notamment pour ne pas avoir correctement informé les personnes concernées du traitement de leurs données sur ses sites web via des cookies, et pour avoir utilisé de manière confuse le terme « intérêt légitime » sans lien avec sa signification dans le cadre du RGPD. Cette affaire est particulièrement notable car la NAIH n'avait, jusqu'alors, jamais encore contrôlé les paramètres des cookies.

ILDIKÓ MÓRICZ
&
KATARINA PETROV

hungary@
lexing.network

Administrative fines by the Hungarian data protection authority

We examined 134 decisions **(1)** from the last three years, where the most common infringements of GDPR were related to the following areas

- **Transparent information**: Most of the cases were related to Article 12 of the GDPR. In more than half of the cases the Authority has stated that the company has not given transparent information to the data subject about the data processing.
- **Lawfulness, fairness, and transparency**: In a lot of cases, the Authority imposed a fine on companies due to the violation of Article 5 (1) a) of the GDPR, i.e. the principles of lawfulness, fairness and transparency.
- **The purpose of the processing**: A frequent violation of the GDPR by data controllers is that they do not inform the data subjects of the purpose of the processing pursuant to Article 13 (1) b).
- **Access to personal data:** The Authority specifically fined those companies that did not properly enable the data owner to exercise their right of access to their personal data. This obligation is based on Article 12 of the GDPR.
- **Purpose limitation:** Article 5 (1) b) of GDPR provides that personal data can be collected for specified, explicit and legitimate purposes. The Hungarian Authority stated in a lot of cases that the companies did not comply with this obligation.
- The amount of the fines imposed for breaches of the GDPR range from HUF 50,000 (EUR 130) to HUF 250 million (EUR 650,000).

The most significant fines were in these cases:

- **Budapest Bank:** The highest fine (HUF 250 million – EUR 650,000) was imposed on Budapest Bank because it used hidden artificial intelligence in its telephone customer service for years to profile the emotion of customers, and based on this, made decisions on customer call-backs. The Authority found that the company had infringed Articles 5, 6, 12, 13, 21, 24 of the GDPR.
- **DIGI Távközlési és Szolgáltató Kft:** The Authority imposed a fine of HUF 100 million (EUR 260,000) for the infringement of purpose limitation and storage limitation. The company had a test database which was not deleted after use, and the content was accessible publicly through the company's website.
- **UPC Hungary:** The Authority imposed a fine of HUF 60 million (EUR 156,000) for the reason that the company performed voice recording in personal customer services, and failed to identify the purpose for the processing and to prepare an adequate balancing test.

(1) https://www.naih.hu/hatarozatok-vegzesek

▪ **Amplifon:** The Authority imposed a HUF 80 million (EUR 200,000) fine on Amplifon for sending direct marketing letters. The company mislead approximately 3-400.000 data subjects about the purposes of processing and unlawfully used consent as a legal basis.

▪ **TV2 Media Group:** The Authority fined the media provider HUF 10 million (EUR 25,650) for, among other things, failing to properly inform data subjects about the processing on its websites related to the use of cookies, and for confusingly using the term "legitimate interest" without referring to its meaning under the GDPR. This case is outstanding because the Authority never inspected the cookie settings before.

ILDIKÓ MÓRICZ
&
KATARINA PETROV

hungary@
lexing.networ

LEXING NETWORK

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne *Germany*	Mercatorius	Guido Imfeld	+49(0)241 / 946 21-0	germany@lexing.network
Australie *Australia*	Gadens	Dudley Kneller	+61 438 363 443	australia@lexing.network
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Brésil *Brazil*	Andrea Filomeno Faria	Andrea Filomeno Faria	+55 11 2189 0061	brazil@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Antoine Rancourt	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Congo (RDC) *Congo (DRC)*	KMC & ASSOCIES	Coco Kayudi Misamu	+243(0)99 872 72 22 +243(0)81 508 07 71	dcr@lexing.network
Côte d'Ivoire *Ivory Coast*	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Estonie *Estonia*	Hedman	Merlin Seeman	+372 66 452 50	estonia@lexing.network
États-Unis (côte est) USA (West Coast)	Mulligan, Banham & Findley	Janice F. Mulligan	+1 619.238.8700	westusa@lexing.network
États-Unis (côte est) *USA (East Coast)*	The Beckage Firm, PLLC	Jennifer A. Beckage	+1 223-253-4762	eastusa@lexing.network
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Hong Kong *Hong Kong*	Tanner de Witt	Pádraig Walsh	+852 2573 5000	hk@lexing.network
Hongrie *Hungary*	OPL gunnercooke	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde *India*	Poovayya & Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
Lettonie *Latina*	Hedman	Merlin Seeman	+372 66 452 50	estonia@lexing.network
Lituanie *Lithuania*	Hedman	Merlin Seeman	+372 66 452 50	estonia@lexing.network
Luxembourg *Luxembourg*	Emmanuelle Ragot Lawyers & Associates	Emmanuelle Ragot	+ 352 661 84 4250	luxembourg@lexing.network
Maroc *Morocco*	Elkhatib Lawfirm	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De González Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège *Norway*	Advokatfirmaet Føyen AS	Knut Fiane	+47 21 93 10 00	norway@lexing.network
Philippines *Philippines*	Calleja Peralta Jimenez San Luis Uy & Ulibas (Calleja Law Office)	Anthony B. Peralta	+6336113 +6352307	philippines@lexing.network
République tchèque *Czech Republic*	Rowan Legal	Michal Nulicek Josef Donat	+420 224 216 212	czechrepublic@lexing.network
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Sénégal *Senegal*	SCP Faye & Diallo	Mamadou Seye	(+221) 33 823 60 60	senegal@lexing.network
Slovaquie *Slovakia*	Rowan Legal	Michal Nulicek Josef Donat	+420 224 216 212	slovakia@lexing.network
Suède *Sweden*	Eris Law Advokatbyrå	Katarina Bohm Hallkvist	+46 (0) 70 646 6768	sweden@lexing.network
Suisse *Switzerland*	Lexing Switzerland	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan.
Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier Diffusée uniquement par voie électronique – gratuit- ISSN 1634-0701
Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/