SROUJI AVOCATS
AVOCATS A LA COUR

www.sroujiavocats.com

Overview of recent data protection fines in the European Union

September 2022

Executive Summary

The number of EU data protection-related fines continued to increase in 2022, with GDPR fines hitting record levels to date for 2022.

Most media attention has gone to the impressive fines imposed on the technology giants Google, Meta (Facebook) and Amazon. And just recently, the Irish Data Protection Commission (DPC) levied a staggering € 405 million fine on Meta for failures in processing minors' data.

Personal health data continues to be a hot topic for regulatory scrutiny, as demonstrated from the French Data Protection Authority's (CNIL) aggressive fine due to security weaknesses that led to a data breach of medical data concerning nearly 500,000 individuals.

The use of new technologies – notably facial recognition and artificial intelligence – is also front and center for regulators. Several EU Supervisory Authorities fined the US-based company Clearview Al (specialized in facial recognition) with fines amounting to € 20 million.

A significant number of fines continue to result from non-compliance of general data processing rules, such as the lawfulness of data processing principle set forth in the GDPR (Articles 5 and 6) as well as the security of processing (Article 32). Moreover, EU regulators remain sensitive to non-compliance when obtaining valid consent of data subjects (Article 7).

Overview of data protection fines in EU (as of September 2022)

Austria

- *REWE International – 14 January 2022*

An Austrian food retailer company, REWE International, received a fine of € 8 million for non-compliance with the GDPR. The company's customer loyalty and rewards program was non-compliant with the GDPR since it collected users' data without their consent and used it for marketing purposes.

This is not the first time the company failed to comply with the GDPR. The subsidiary was fined € 2 million in 2021 for the unlawful collection of millions of bonus club members' data and the subsequent sale to third parties.

Croatia

- *Telecommunications company*– 21 July 2022

The Croatian Supervisory Authority imposed an administrative fine of HRK 2.15 million (around € 286,000) on a telecommunications company for failing to take appropriate technical and organizational security measures for the processing of personal data, which led to the unauthorized processing of personal data of approximately 100,000 respondents.[1] According to the competent authority, the company did not take the necessary measures to achieve an adequate security measure in accordance with the existing foreseeable risks, breaching Articles 25 paragraph 1 and Article 32 of GDPR.

The authority found an aggravating circumstance given the fact that the company is one of the leading companies providing telecommunications services in Croatia. Several factors to determine the fine were taken into account, such as the cost of implementation and the nature, scope, context and purposes of processing, as well as risks of different levels of probability and severity for the rights and freedoms of individuals arising from data processing.

Denmark

- *Gyldendal A/S*– 22 June 2022

The Danish Supervisory Authority reported an online bookstore, Gyldendal A/S, to the police and recommended a fine of DKK 1 million (approximately € 201,663), for not deleting personal data of its unsubscribed book club members. After a physical inspection, the Danish authority found that information about approximately 685,000 unsubscribed members of Gyldendal's book clubs was kept for longer than needed. The controller stored data in a so-called "passive database" and had no procedures or guidelines for deleting it. The non-compliance relates to two basic principles: "storage limitation" and "responsibility."[2]

France

- *Dedalus Biologie – 15 April 2022*

[1] Personal Data Protection Agency of Croatia, July 21 2022, https://azop.hr/izrecene-dvije-upravne-novcane-kazne-u-ukupnom-iznosu-218-milijuna-kuna/

[2]Datatilsynet Press Release, 22 June 2022, https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jun/gyldendal-indstilles-til-boede

On April 2022, the French DPA ("CNIL") levied a fine of € 1.5 million on Dedalus Biologie, a company selling software solutions for medical analysis laboratories. Dedalus acts as a data processor on behalf of its clients. This sanction was justified by several issues of non-compliance with the GDPR, in particular the obligation to ensure the security of personal data.

On February 23, 2021, a massive data leak concerning private health information on nearly 500,000 people was revealed in the press, which implicated the company DEDALUS. Sensitive health data (such as medical conditions or treatments) as well as other types of personal data, were disclosed on the Internet.

The issues of GDPR non-compliance are summarized as follows: the obligation for the processor to comply with the instructions of the controller (Article 29 of the GDPR); the obligation to ensure the security of personal data (Article 32 of the GDPR); the obligation to regulate by a formalized legal act the processing carried out on behalf of the data controller (Article 28 of the GDPR). The significant amount of this fine was decided in view of the seriousness of the breaches identified.

- *TotalEnergies Electricité et Gaz France* – 23 June 2022

The CNIL imposed a fine of € 1 million on *TotalEnergies Electricité et Gaz France*.[3]

Violations were as follows:

- Under French Law, a breach of the obligation to allow people to opt-out of commercial prospecting;
- Under GDPR, breaches of the obligation to provide information and comply with the exercise of data subject rights; the obligation to inform persons targeted by telemarketing (Article 14 of the GDPR); breach of the right of access to data (Article 15 of the GDPR) and the right to opt-out (Article 21 of the GDPR). In regards to the non-compliance with data subject rights (Article 12 of the GDPR), the company did not respond to data subject requests within the period provided for by GDPR.[4]

- UBEEQO International – 7 July 2022

The CNIL imposed a fine of € 175,000 on UBEEQO International, a company specialized in short-term car rentals, for privacy infringements due to the geolocalisation of its customers.[5] In particular, the company collected data relating to the geolocation of the rented vehicle when the vehicle was moving, and when the engine was switched on and off. The company kept records longer than needed.

The CNIL fines focused on the following areas of non-compliance:
- Failure to comply with the obligation to ensure data minimization (Article 5.1 c GDPR)
- Failure to define and respect a proportionate data retention period (Article 5.1 e GDPR)
- Failure to inform individuals (Article 12 GDPR)

[3]CNIL Press Release, https://www.cnil.fr/fr/prospection-commerciale-et-droits-des-personnes-sanction-de-1-million-deuros-lencontre-de
[4] CNIL decision, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000045975295?init=true&page=1&query=San-2022-011&searchField=ALL&tab_selection=all
[5] CNIL decision, 7 July 2022, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046070924?init=true&page=1&query=%2A&searchField=ALL&tab_selection=cnil

- *Accor SA* - 3 August 2022

The CNIL imposed a € 600,000 fine on Accor SA Company for insufficient fulfilment of data subjects rights.[6] In particular, the fine focused on the company's commercial prospecting without the consent of the data subjects and for not having respected the rights of customers and prospects.

The CNIL identified four areas of GDPR non-compliance, notably the company's failure to obtain the consent of the data subject when processing their data for commercial prospecting purposes.[7]

The company's GDPR non-compliance can be summarized according to the following failures:

- the obligation to inform data subjects (Articles 12 and 13 GDPR);
- the obligation to respect the right of access of individuals to data concerning them (art. 12 and 15 of the GDPR), since the company did not respond to the requests made by a complainant within the deadlines;
- the obligation to respect the right of to opt-out (art. 12 and 21 of the GDPR) ;
- the obligation to ensure the security of personal data (Art. 32 of the GDPR), because the company allowed the use of insufficiently strong passwords.

The CNIL took into account several elements to determine the penalty, such as the number of non-compliance issues noted, the fact that these issues relate to several fundamental principles of the protection of personal data and that they constituted a substantial violation of the rights of individuals, as well as the number of data subjects and the financial situation of the company. [8]

Germany

- *unidentified German company - 20 September 2022*

The Berlin Supervisory Authority fined the subsidiary of a Berlin-based retail group € 525,000 because of a conflict of interest involving the company's Data Protection Officer ("DPO").[9]

Under Article 38 (6) GDPR, any such tasks and duties fulfilled by the DPO must not result in a conflict of interests.

In this case, the DPO had to monitor compliance with data protection law by the service companies operating within the scope of the commissioned processing, which were managed by himself as managing director.

[6] CNIL Decision, 3 August 2022, https://www.cnil.fr/sites/default/files/atoms/files/deliberation_de_la_formation_restreinte_no_san-2022-017_du_3_aout_2022_concernant_la_societe_accor_sa.pdf
[7] Article L. 34-5 du Code des postes et des communications électroniques
[8] CNIL Press Release, https://www.cnil.fr/fr/prospection-commerciale-et-droits-des-personnes-sanction-de-600-000-euros-lencontre-daccor
[9] Decision of 20 September 2022, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2022/20220920-BlnBDI-PM-Bussgeld-DSB.pdf

- *Hannoversche Volksbank – 28 July 2022*

A German Bank was fined € 900,000 by the Lower Saxony Supervisory Authority for infringing Article 6 (1) of the GDPR.[10] The company evaluated data from active and former customers without their consent, identifying customers with an increased inclination for digital media and to use electronic communication channels in order to better target them for advertising purposes.

- *Volkswagen – 26 July 2022*

On July 2022, Lower Saxony Supervisory Authority imposed a fine of € 1.1 million on Volkswagen for GDPR violations, relying on Article 83 GDPR that provides for the imposition of administrative fines.

The high fine was justified by data protection violations in connection with the use of a service provider for research trips for a driver assistance system to avoid traffic accidents. A test vehicle from the company was stopped for a traffic check by the Austrian police near Salzburg in 2019. The vehicle was used to test and train the functionality of a driver assistance system to avoid traffic accidents. The traffic situation around the vehicle was recorded, for error analysis. Among the violations, the company was not compliant with Article 13 since it failed to inform the data subjects that their data were being processed.

The company remedied these violations and cooperated fully with the authority. While the authority deemed these violations to have a low level of severity, the high amount of the fine demonstrates that even violations of a *relatively low severity* can lead to substantial fines.

Greece

- *Clearview Al Inc.– 13 July 2022*

The Greek Supervisory Authority imposed a fine of € 20 million, finding that the Clearview Al Inc company, which trades in personal identification services, violated the principles of legality and transparency (art. 5 GDPR) as well as those arising from the provisions of of Articles 12, 14, 15 and 27 of the GDPR.

In addition, the Authority addressed a compliance order to the company to satisfy the request for access to personal data of the complainant, while imposing on the company a ban on the collection and processing of personal data of data subjects located in Greece, using methods involved in the facial recognition service. Finally, the Authority ordered the company to delete the personal data of the data subjects located in Greece.[11]

This significant fine follows another one imposed by the Italian Supervisory Authority on February 2022 amounting to € 20 million euros. The French CNIL also fined the company on December 2021. The personal data held by the company, including biometric and geolocation information, were deemed to have been processed unlawfully without an appropriate legal basis. Additionally, the

[10] Lower Saxony State Chancellery Press Release, 28 July 2022
https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/900-000-euro-bussgeld-gegen-kreditinstitut-wegen-profilbildung-zu-werbezwecken-213925.html
[11] See Decision, 13 July 2022, https://www.dpa.gr/sites/default/files/2022-07/35_2022%20anonym_0.pdf

company infringed on several fundamental principles of the GDPR, such as transparency, purpose limitation, and storage limitation. [12]

Italy

- *Unicredit S.p.A – 16 June 2022*

The Italian Supervisory Authority (Garante) announced on 16 June 2022 a fine up to € 70,000 on the bank Unicredit S.p.A. following the request of one of its employees to access their data. The company asked the data subject to submit the access request by filling out a specific form. The data subject did not reply or fill out the form on the portal, but instead filed a complaint with the Garante. The data subject claimed that their right to access was not granted by the controller. After the company was notified of the complaint by the Garante, it granted the access request.

According to the Garante, the controller still had a duty to respond to data subject requests communicated through different means. The Garante further noted that the form in question did not cover the full content of the data subject's right of access under Article 15 GDPR.[13]

The Garante observed that the considerable amount of paper documentation sent belatedly to the data subject after the complaint had been made before the Authority was not provided in such a way as to facilitate access request and understanding by the data subject as required by Article 12 GDPR.

- *Clearview Al Inc - 20 February 2022*

In addition to other European Supervisory Authorities, the Garante imposed on the 20 February 2022 a fine up to € 20 million on Clearview and imposed a ban on data collection and processing.[14] The findings revealed that the personal data held by the company, including biometric and geolocation data, were processed illegally without an adequate legal basis.

Ireland

- *Meta Platforms Ireland Limited – 15 September 2022*

The Irish Data Protection Commission (DPC) concluded an inquiry on Meta Platforms Ireland Ltd (Instagram) and announced the imposition of a record fine for failures to comply with the GDPR related to the processing the personal data of minors. The imposed fine totaled € 405 million, including a fine of €20 million for the infringement of Article 6(1) that concerns the lawfulness of processing.

The Netherlands

- *Dutch tax authorities – 7 April 2022*

[12] GPDP Decision, 10 February 2022, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362 ; CNIL Press release, 16 December 2021, https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet
[13] GPDP Decision, 16 June 2022, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9795350
[14] GPDP Decision, 10 February 2022, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362

The Dutch Supervisory Authority imposed a fine of € 3.7 million on the Dutch tax authorities due to the unlawful processing of personal data in their Fraud Signaling Facility.[15]

The tax authorities had no legal basis for processing the personal data which constitutes a breach of Article 6 GDPR. The authorities also registered incorrect personal data, leading people to be wrongly registered as possible fraudsters. This fine is the highest the Authority has ever imposed due to the seriousness of the violations, the impact on large numbers of people and the duration of the violations.

Spain

- *Google LLC – 18 May 2022*

The Spanish Supervisory Authority (AEPD), imposed a fine of € 10 million on Google LLC for two serious infringements of GDPR.[16] The AEPD found that Google transferred data to third parties without legal basis to do so and hindered citizens' right to erasure (respectively Articles 6 and 17 of the General Data Protection Regulation).

- *DKV Seguros y Reaseguros, S.A.E. – 13 July 2022*

The AEPD imposed a fine of € 220,000 on a health insurance company DKV Seguros y Reaseguros following a complaint lodged by an individual.[17] The complainant had received several emails with private health data of unknown individuals from company such as personal data relating to names, surnames, and test data although the complainant had repeatedly brought the situation to the attention of the insurance company and no action was taken.

The Authority deemed that DKV Seguros y Reaseguros' technical and organisational security measures were not adequate, taking into consideration that the data in question was sensitive.

- *Amazon Road Transport Spain, S.L. – 11 February 2022*

On February 2022, the AEPD issued a fine of € 2 million against Amazon Road Transport Spain, a logistics company responsible for managing deliveries for Amazon.[18] For the contractor hiring, company required the contractors to provide certificates of absence of a criminal record.

The AEPD ordered the company to cease requiring the certificate of absence of a criminal record from applicants as it did not comply with the processing of personal data relating to criminal convictions within the meaning of Art. 10 GDPR. Such data processing would therefore only be permissible under the control of official authority and with the consent of individuals. The AEPD also compelled the company to delete all the information of the certificates already provided, and adapt its processing in accordance to the requirements of Article 6(1) of the GDPR.

[15] Autoriteit Persoonsgegevens Decision, 7 April 2022, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_belastingdienst_fsv.pdf https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_belastingdienst_fsv.pdf
[16] AEPD Decision, 18 May 2022, https://www.aepd.es/es/documento/ps-00140-2020.pdf
[17] AEPD Decision, 13 July 2022, https://www.aepd.es/es/documento/ps-00080-2022.pdf
[18] AEPD Decision, 11 February 2022, https://www.aepd.es/es/documento/ps-00267-2020.pdf

Sweden

- *Klarna Bank AB – 28 March 2022*

The Swedish Supervisory Authority (IMY) issued a fine of SEK 7,500,000 (around € 689.000) against Klarna Bank AB for non-compliance with the GDPR.[19] Klarna failed to ensure that its processing of personal data was accurate and as complete as possible.

The company also provided incomplete and misleading information about who was the recipient of personal data when information was shared with Swedish and foreign credit reporting companies.

United Kingdom
(N.B. we have opted to include the UK in our EU scope, for the time being, given the historical alignment with other EU Supervisory Authorities)

- *Clearview Al Inc.– 23 May 2022*

In line with penalties imposed by other EU Supervisory Authorities, the UK Information Commissioner's Office (ICO) fined Clearview for non-compliance with UK data protection obligations. On 23 May 2022, the ICO fined Clearview AI Inc £7,552,800 for using images of people in the UK that were collected from the web and social media to create a global online database that could be used for facial recognition.[20]

[19] IMY Decision, 28 March 2022, https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-klarna.pdf
[20] ICO Press Release, 23 May 2022 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/