Analysis of fines under GDPR

Mrežar, Filip

University of Zagreb

Faculty of Law

Department for Information Technology Law and Informatics

Filip Mrežar

ANALYSIS OF FINES UNDER GDPR AND THEIR FUTURE

Master's thesis

Mentor: Tihomir Katulić, Ph.D., Assoc. Prof.

Zagreb, February 2023

Sveučilište u Zagrebu

Pravni fakultet

Katedra za pravo informacijskih tehnologija i informatiku

Filip Mrežar

ANALIZA KAZNI ZBOG KRŠENJA GDPR-A I NJIHOVA BUDUĆNOST

Diplomski rad

Mentor: izv. prof. dr. sc. Tihomir Katulić

Zagreb, veljača 2023.

Declaration of Authenticity

I, Filip Mrežar, under full moral, material and criminal responsibility, herewith declare that I am the exclusive author of the master's thesis and that no unauthorised use of any part of other works (use without proper citation) was made and that I did not use any sources other than those listed herein.

Filip Mrežar, m.p.

_____

Izjava o izvornosti

Ja, Filip Mrežar, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristio drugim izvorima do onih navedenih u radu.

Filip Mrežar, v.r.

_____

Table of Contents

1. Introduction

The right to privacy emerged in international human rights law in the Universal Declaration of Human Rights[1], adopted in 1948, as one of the fundamental protected human rights. It was reaffirmed in the European Convention of Human rights[2], drafted in 1950. In regard to European Union law, data protection is affirmed in Article 16 of the Treaty of the Functioning of the EU[3], as well as in Article of 8 of the EU Charter of Fundamental Rights[4]. This led to the Data Protection Directive[5] in 1995, which was the first time data protection was regulated by EU law.[6]

Rapid technological advancements have forced the EU to adapt to the digital age with The General Data Protection Regulation[7] which became applicable in May 2018. In its Article 84, GDPR regulates general conditions for imposing administrative fines. Since then, over 1,500 fines have been issued, amounting to over 2 billion €. This work will explain the trends of fines, their amounts and reasons for issuing. It will analyse ten different sectors obligated to respect the GDPR, their history of fines and specific problems. Across the EU, it will show the most strict and lenient DPAs (Data Protection Authorities). Throughout it, 10 highest fines overall will be clarified and their importance highlighted. In the second half of this work, it will illustrate the new Guidelines on the calculation of administrative fines under the GDPR[8] (which aren't yet fully adopted but were given to public consultation in 2022) adding many insights, suggestions, and complaints by commentators.

[1] United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948.
[2] Council of Europe, European Convention of Human Rights, CETS NO. 005, 1950.
[3] EU, Consolidated version of the Treaty of the Functioning of the European Union, OJ 2012 C 326
[4] EU, Charter of Fundamental Rights of the European Union, OJ 2012 C 326.
[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal dana and on the free movement of such data, OJ 1995 L 281.
[6] European Union Agency for Fundamental Rights. et al., *Handbook on European Data Protection Law: 2018 Edition.* (2018), available at https://data.europa.eu/doi/10.2811/343461 (last visited 14 December 2022), p. 18.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); (hereinafter referred to as GDPR).
[8] *Guidelines 04/2022 on the Calculation of Administrative Fines under the GDPR*, version 1.0, available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en (hereinafter referred to as "Guidelines")

2. About GDPR enforcement tracking

Since coming into force in May 2018, GDPR has caused many discussions in real life and online. A lot of websites concerning it have popped up, in which lawyers, judges, members of DPAs and concerned citizens engage in conversation about understanding the legislation and its consequences. Looking at the practice and reasoning of different DPAs in relation to fines especially helps this cause. Thus, people have created several websites to track fines issued under the GDPR from all across the EU. One of those websites is GDPR enforcement tracker[9]. On its homepage, it clearly states that it "offers an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation". Since not all fines are made public, it offers a system to submit fines or offer corrections on the already reported ones. GDPR enforcement tracker is not the only one of its kind. For example, there is GDPRhub[10], an initiative by noyb, also supported by the contributions of volunteers. GDPR enforcement tracker, and its periodic executive summary is a project by CMS, a firm with offices in more than 40 countries and more than 5000 lawyers.[11]

3. GDPR enforcement tracker

The first half of the work is going to concentrate on analysing the data about fines and penalties available in the database on enforcement tracker[12]. A few words about the limitations of the database should be mentioned. It does not list any fines imposed under national/ non European laws, under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR laws.[13]

[9] https://www.enforcementtracker.com/ (last visited 19 December 2022).
[10] https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub (last visited 19 December 2022).
[11] https://cms.law/en/int/about-cms/about-us (last visited 19 December 2022).
[12] GDPR Enforcement Tracker, *op. cit.* (fn. 9).
[13] *Ibid.*

In some statistics, concerning time and date issued, there are inaccuracies because of incompleteness of entries.[14]

All data shown in next chapters was accurate on 29 November 2022 and was acquired from https://www.enforcementtracker.com/?insights.

3.1. Number and sum of fines (chronological statistics)

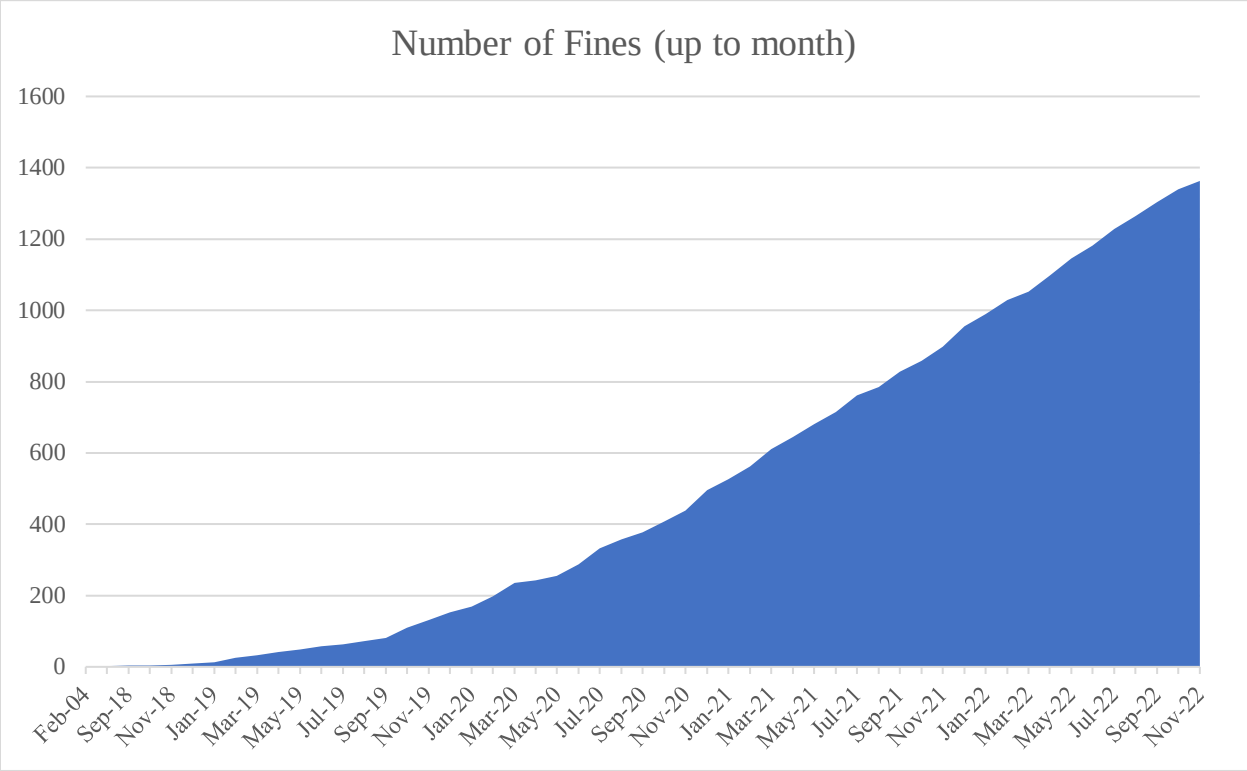

Figure 1: number of fines issued under the GDPR; data correct on 29 November of 2022 (https://www.enforcementtracker.com/?insights).

The data shows that in the first few months since the introduction of GDPR in May 2018, all the way to January 2019, there were relatively few fines issued at all, showing that data protection authorities allowed a period for the market, citizens, and others to adapt to and fully comprehend GDPR's obligations. Not counting the fine from 2004, there were only 9 fines issued until the end of 2018. To compare that to the first 6 months of 2019, when there were 47 issued fines, shows an

[14] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/methodology-and-contacts (last visited 19 December 2022).

increase of more than 5 times. Since 2018, the overall number of fines is constantly growing. The number of fines through different months shows great oscillations; for example, in April of 2020, there were issued only 8 fines, but in December of the same year there were 57, which is the highest number of fines in a month issued ever (December of 2021 shows the same number of fines issued). When looking at issued fines based on a year, the data shows 143 fines issued in 2019, 341 in 2020 and 459 in 2021 which shows constant growth through the years.

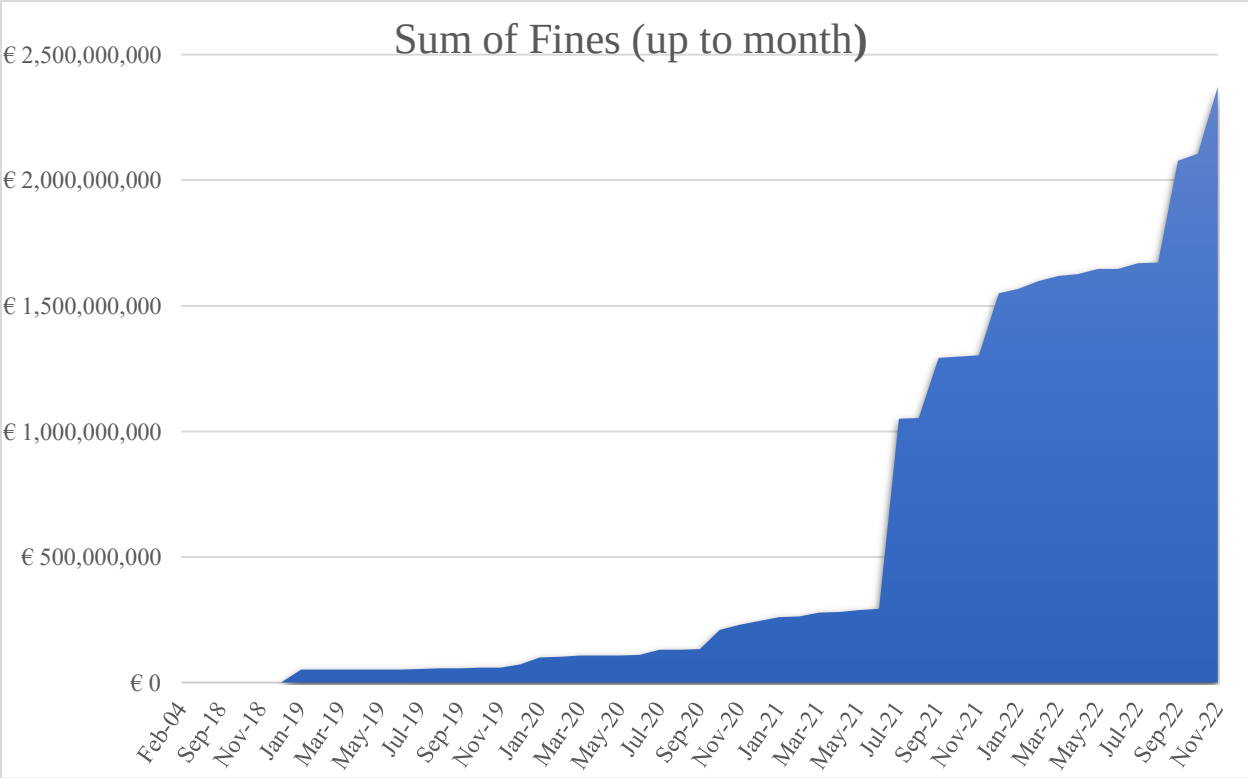

Figure 2: sum of fines issued under the GDPR; data correct on 29 November; (https://www.enforcementtracker.com/?insights).

Sum of fines is, logically, quite connected to the number of fines, but the data shows interesting significant increases related to massive fines. The situation is the same for the rest of 2018 in which those few fines caused very little financial impact. Through 2019 and 2020 there were a few outlier (meaning higher than usual) fines but little compared to 2021, when 5 out of 10 biggest fines were issued. The biggest jump in the statistics appears in July of 2021, when Luxembourg DPA issued

a 746,000,000 €[15] fine. There will be more words about this particular fine later in this work, but for the sake of transparency, it should be mentioned here that this decision was appealed and its appeal process is currently in progress. Next jump in the graph of Figure 2 in September of 2021 is related to a 225,000,000 €[16] fine by Ireland DPA. The end of 2021 was also marked by 3 other high amount fines by the France DPA, amounting to 210,000,000 €[17][18][19].

In 2022, there have been 2 particularly large fines, both issued by the Ireland DPA, one in September, and one in November. The first one amounts to 405,000,000 €[20] and takes the second place in the top 10 of the highest amount fines, just behind the aforementioned Luxembourg fine. The fine from November is smaller, "only" 265,000,000 €[21] and takes the third place in the top 10. They were both against the same controller, Meta Platforms. These two fines are the main reason for the significant increase at the end of the graph of Figure 2.

3.2. Countries with highest fines (sum and number of fines)

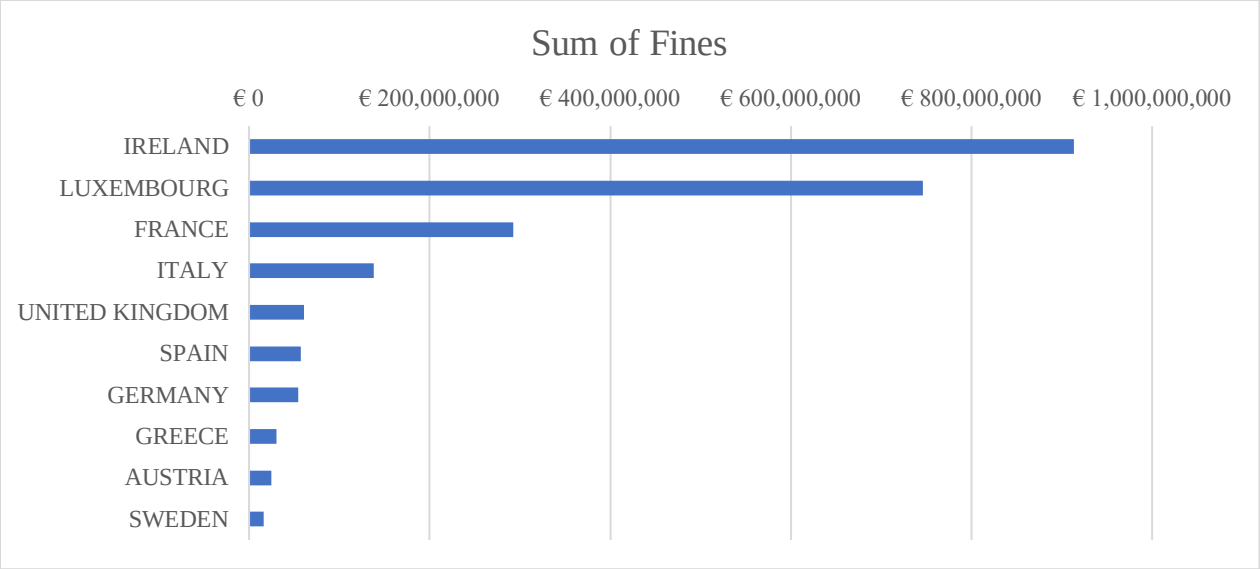

Figure 3: countries in relation to the sum of fines they issued; data correct on 29 (November 2022; https://www.enforcementtracker.com/?insights).

[15] https://www.enforcementtracker.com/ETid-778 (last visited 8 December 2022).
[16] https://www.enforcementtracker.com/ETid-820 (last visited 9 December 2022).
[17] https://www.enforcementtracker.com/ETid-978 (last visited 9 December 2022).
[18] https://www.enforcementtracker.com/ETid-979 (last visited 9 December 2022).
[19] https://www.enforcementtracker.com/ETid-980 (last visited 9 December 2022).
[20] https://www.enforcementtracker.com/ETid-1373 (last visited 8 December 2022).
[21] https://www.enforcementtracker.com/ETid-1502 (last visited 8 December 2022).

It appears that Ireland has issued the highest sum of fines, at over 900,000,000 €, but this is a quite new turn of events. In the fall of 2022, Ireland has overtaken Luxembourg for the first place because of already mentioned two very hefty fines. Luxembourg held the lead all the way from July of 2021, when the 746,000,000€ fine was issued. However, the possible correlation that Ireland and Luxembourg have also issued the most fines, is completely wrong. Luxembourg has issued only 23 fines, and it does not enter into top 10 countries with the highest number of fines. Ireland has issued even less, only 17. Therefore the two top countries on the list are not there because of a consistent high number of severe fines but mostly because of single, massive fines, which are definitely outliers in their usual practice, especially in the case of Luxembourg.

The third country with the highest sum of fines is France, but it is far from the top 2, not even reaching the threshold of 300,000,000€. Though France has issued 31 fines, which has them take 10th place by the number of fines, 4 of those are in the top 10 highest fines which is why France, with a relatively low number of fines still has the 3rd highest sum.

4th place is secured by Italy, which is the first country that shows strong correlation between the amount of fines and their sum. The data shows that Italy with 195 fines managed to issue 138,440,096 € worth of fines. Combine that with the fact that one of those enters the hall of fame of the top 10 highest fines and it appears that Italy has probably one of the most severe DPA's in the EU. Comparing Italy to Spain, which holds the first place for the total number of fines at 532[22], its sum of fines amounts to "only" 57,284,890€. That means while having 337 more fines, they amount to about 81 million € less than Italy's sum.

On both lists, Germany takes its place after Italy and Spain, coming in 6th by the sum of fines and 3rd by the number of fines. Even though Germany is no rival to Spain by the sheer number of fines at 115 fines, their total sum amounts to not even 3 million less than Spain's (57,284,890). This shows that Spain indeed has issued far more fines than any other country, but their fines are much less severe than Italy's, and even Germany's.

[22] Perhaps it should come as no surprise that Spain's AEPD (Agencia Española de Protección de Datos) is the most active DPA since it is historically known as such. See: Artemio Rallo Lombarte, *'The Spanish Experience of Enforcing Privacy Norms: Two Decades of Evolution from Sticks to Carro*ts' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), p. 123

UK accrued 5th highest sum at around 60 million € with only 12 fines. This is largely because of two fines of around 20 million € in October of 2020. The list of top 10 countries with the highest sum of fines ends in Greece at 8th, Austria in 9th, with Sweden coming in to finish the top 10.

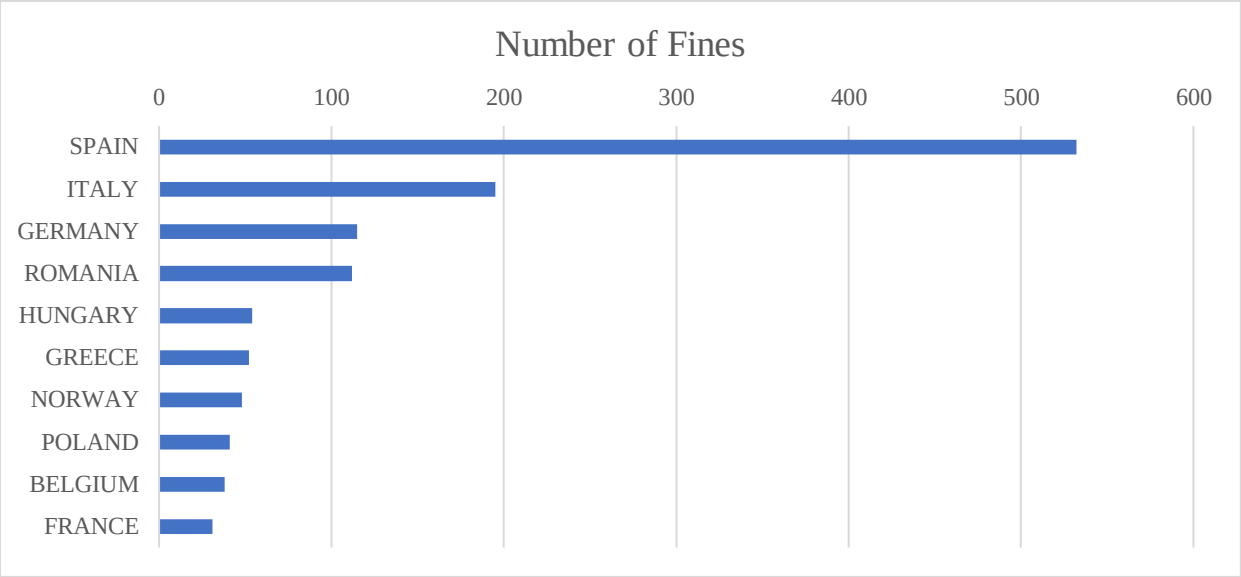

Figure 4: countries in relation to the number of fines they issued; data correct on 29 November; (https://www.enforcementtracker.com/?insights).

Only Spain, Italy, Germany and Romania have imposed over 100 fines. Hungary and Greece are barely over 50, while everyone else is under. The numbers show that Spain is by far leading the race by the number of fines, while Italy might be the most consistently severe. Ireland and France are frontrunners in the fines against "Big Tech", and if that continues, they will only further their lead against others with massive fines issued to this sector.

Figure 5: list of the highest fine from each country issued under the GDPR

Country	Highest fine(€)
Luxembourg	746,000,000
Ireland	405,000,000
France	90,000,000
Germany	35,258,708
Italy	27,800,000
United Kingdom	22,046,000
Greece	20,000,000
Spain	10,000,000
Austria	9,500,000
Norway	6,300,000
Sweden	5,000,000
The Netherlands	3,730,000
Bulgaria	2,600,000
Denmark	1,300,000
Portugal	1,250,000
Poland	1,000,000
Cyprus	925,000
Hungary	634,000
Finland	608,000
Belgium	600,000
Croatia	285,000
Isle of Man	202,000
Latvia	150,000
Romania	150,000
Czech Republic	118,500
Lithuania	110,000
Estonia	100,000
Malta	65,000
Iceland	51,000
Slovakia	50,000
Liechtenstein	4,100

Figure 6: all countries in relation to the number of fines issued under the GDPR

Country	Number of fines
Spain	532
Italy	195
Germany	115
Romania	112
Hungary	54
Greece	52
Norway	48
Poland	41
Belgium	38
France	31
Sweden	27
Cyprus	26
Czech Republic	25
Denmark	25
Luxembourg	23
Bulgaria	21
The Netherlands	20
Austria	19
Ireland	17
Finland	14
United Kingdom	12
Iceland	9
Slovakia	9
Croatia	8
Lithuania	8
Estonia	6
Portugal	6
Latvia	5
Isle of Man	3
Malta	2
Liechtenstein	1

3.3. Fines by type of violation (sum and number of fines)

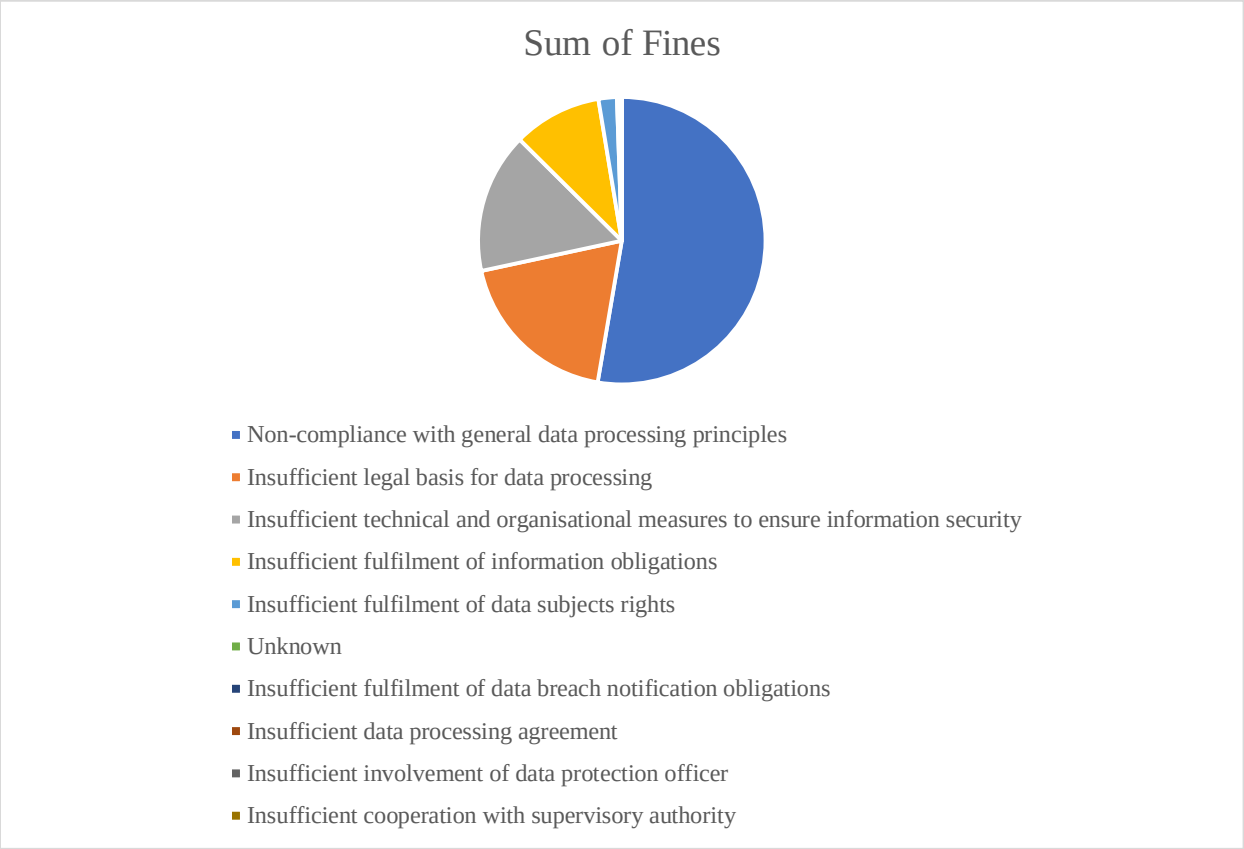

Figure 7: sum of fines in relation to the type of violation for which they were issued; data correct on 29 November 2022; (https://www.enforcementtracker.com/?insights).

Data shows that by far the biggest part of the total sum of fines is due to non-compliance with general data processing principles. That violation has cost offenders 1,253,259,499 €, encompassing 337 fines. Only one of those, amounts to 746,000,000 €, which is the already mentioned Luxembourg fine. Since one fine contains about 60% of the total sum for this violation, it actually isn't the usually most severe punished as it would appear at first. If we add just one more fine, from September of 2022 by the Ireland DPA totalling 405,000,000€ it shows that only 2 fines amount to astounding 92%. There are a lot of fines due to this violation though, it is the 2nd most common violation, behind only insufficient legal basis for data processing at 453 fines.

Those 453 fines amount to about 450 million € which is significantly less than over 1.2 billion € for non-compliance with general data processing principles. When looking at the top 10 highest

fines, all fines from 5th to 10th are issued because of this violation, the highest (5th) being 90,000,000 € and the lowest (10th) 27,800,000 €.

Third violation in the complete sum of fines is insufficient technical and organizational measures to ensure information security amounting to 375,717,219 €. That is mostly because of one already mentioned fine, made by Ireland DPA in November of 2022 at 265,000,000 € (3rd from top 10 highest fines). There have been 265 fines issued for this violation, making it 3rd by the number of fines and by the sum.

Insufficient fulfilment of information obligations has the 4th highest sum at 237,002,475 € with 121 fines issued for this violation. Even though it takes 5th place by the number of fines issued, the main reason it has such a high sum is because of a single fine from September of 2021, by the Ireland DPA for 225,000,000 € (4th highest fine). That single fine is responsible for 95% of the total sum for this violation.

Insufficient fulfilment of data subjects rights is in 5th accruing 49,193,070 €, the first violation for which there isn't a single fine issued that enters the 10 highest. The significant decrease from the 4th to 5th violation is best seen on the graph (Figure 7), overall sum going from over 200 million to very close to 50 million €. Even with more than 150 million € less, there are still 13 fines more issued for insufficient fulfilment of data subjects rights (134) than for insufficient fulfilment of information obligations (121).

About 9 million belong to 7 fines for unknown violations, followed by insufficient fulfilment of data breach notification obligations at nearly 1.5 million € encompassing 25 fines. The last violation that reaches a million is insufficient data processing agreement at 1,048,610 € formed by 9 fines.

The last two violations come to a million euros only when their sum is combined, first being insufficient involvement of data protection officers more than doubling with 875,600 € the last, insufficient cooperation with supervisory authority at 309,029 €. Even though their sum is pretty low compared to others, there were 58 fines issued due to insufficient cooperation with supervisory authority, showing that DPAs didn't hesitate to practice their GDPR given rights. 13 fines were issued for insufficient involvement of data protection officer, which shows that some controllers put too little responsibility in the hands of people that should be the most responsible.

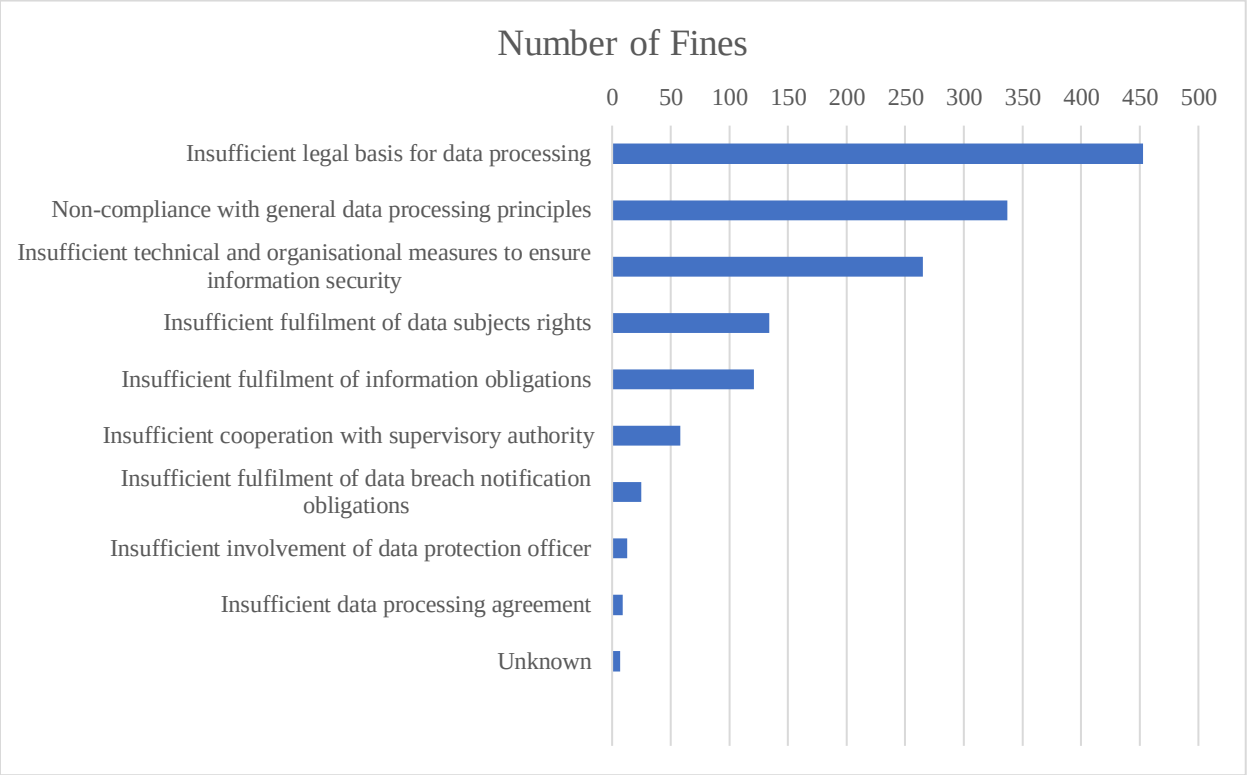

Figure 8: number of fines in relation to the type of violation for which they were issued; data correct on 29 November 2022; (https://www.enforcementtracker.com/?insights)

3.4. Fines by sectors (sum and number of fines)

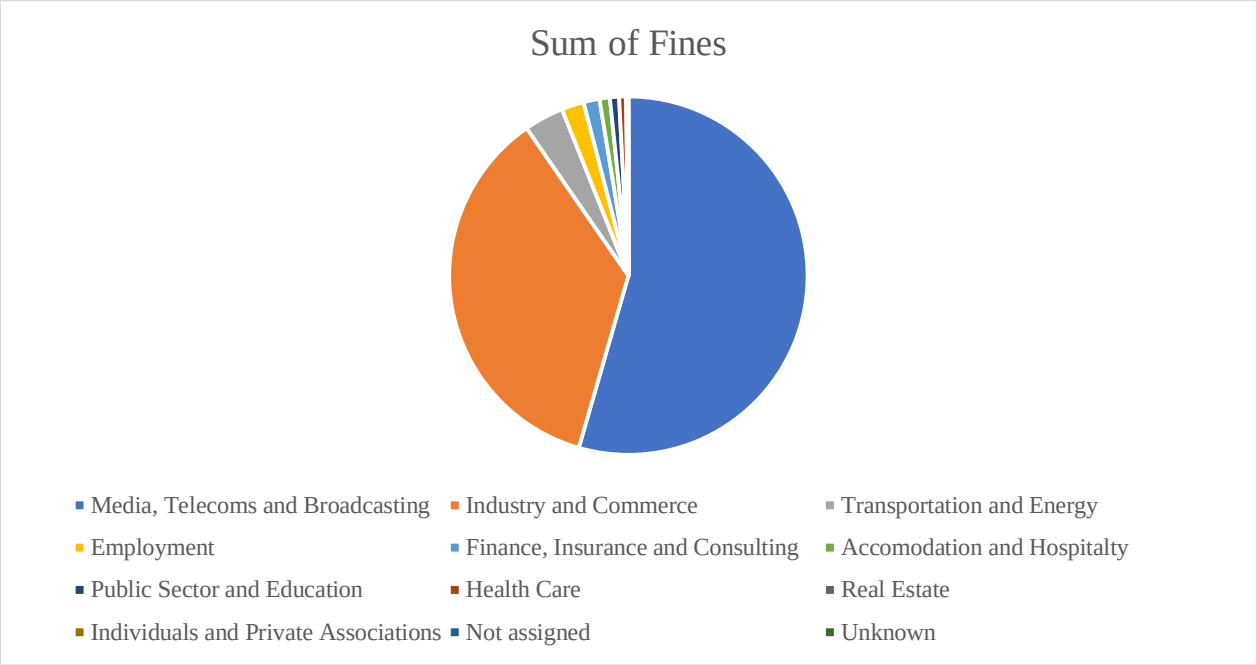

Figure 9: sum of fines in relation to the sector in which they were issued; data correct on 29 November 2022; (https://www.enforcementtracker.com/?insights).

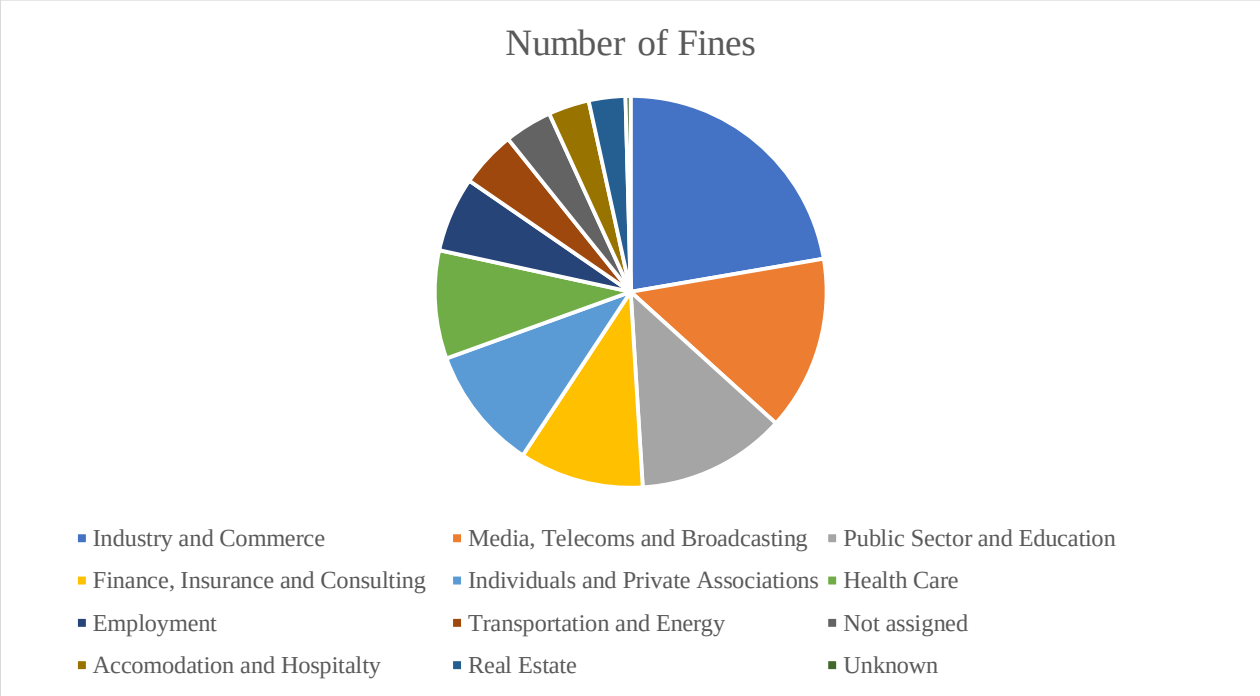

Figure 10: number of fines in relation to the sector in which they were issued under; data correct on 29 November 2022; (https://www.enforcementtracker.com/?insights).

Each sector will be looked at with more detail later in the work. Here is only a general overview.

The sector with the most fines is "Industry and Commerce" with 317 fines amounting to a staggering 854,287,397 €. This number shows a skewed picture of the sector though, and it has to be noted that the biggest fine of 746 million € issued by Luxembourg DPA to Amazon belongs in this sector. Without that massive fine, the sum is around 108 million € spread on 316 fines, and it would put the entire sector only third by the sum of fines, while maintaining the top spot with the most fines. With those numbers, it can be concluded that a 746 million € fine is quite extraordinary for this sector, with other fines being relatively much smaller (excluding the Amazon fine, the average is around 340,000 €).

"Media, Telecoms and Broadcasting" is second in number of fines, but first in the total sum amounting to almost 1.3 billion (1,295,557,541) € with 205 fines. This sector took the lead quite recently mainly because of two massive fines in the fall of 2022, made by the Ireland DPA that combined equalled to 670,000,000 €, meaning that more than half of the total sum is in these two fines. The data shows that this sector has more high amount fines than any other. This means, that if one decided to ignore only one Amazon fine, this sector would have by far the highest sum of fines, towering over with 1.3 billion to only about 108 million € ("Industry and Commerce") in 2nd place. It should also be noted that 8 out of 10 highest fines are issued to companies in this sector. Therefore this sector is crucial and definitely one of the most important ones, which is logical considering the type of work and data used in this sector.

"Transportation and Energy" has the third highest sum of fines, with a relatively quite low amount of 66 fines. It owes its high placement partly to two fines of around 26 and 22 million € by Italy and UK.

"Employment" is fourth, followed by "Finance, Insurance, and Consulting", "Accommodation and Hospitality", "Public Sector and Education", "Health Care", "Real Estate" and the list of known sectors ends in "Individuals and Private Associations". Out of these, "Employment" and "Accommodation and Hospitality" show a relatively small number of fines compared to the sum, "Employment" being the last mentioned sector to have a fine in the top 10 highest partially explaining the discrepancy.

"Accommodation and Hospitality" has a similar situation, with one fine exceeding 20 million. "Individuals and Private Associations" seems to be the biggest outlier, with 117 fines amounting to just under 1.5 million. In comparison, "Health Care" has accrued just one more fine but with a total sum of about nearly 15 million. This discrepancy is completely logical, considering that fines for individuals should be a lot lower.

Interestingly enough, the new EDPB guidelines don't mention the fines issued to individuals explicitly saying that the guidance set out "applies to all types of controllers and processors according to Article 4(7) and (8) GDPR except natural persons when they do not act as undertakings."[23]

3.5. Enforcement tracker executive summary

This work will further analyse the enforcement tracker report (ET Report) made available at CMS website which contains more details about certain sectors. When talking about the 2022 Report, it covers all fines from 2018 to 1 March 2022. When mentioning the difference from 2021 ET Report, it relates to the fines issued between March of 2021 to March of 2022. If the ET Report is mentioned but not specified, it refers to the 2022 Report.

In 2021 for the first time since May 2018, the total number of cases recorded exceeded one thousand, and the total sum of GDPR fines exceeded one billion euros. Up to March 2022, overall number of cases, including those with limited/no detail information, was 1088.[24]

Comparing that to the number of fines available in the database at the time of writing this (November 2022), which is 1507, shows an increase of 419 fines in about 8 months. That number shows a slight raise comparing it to the increase that occurred between the 2021 GDPR Enforcement Tracker Report and the 2022 version.[25]

[23] EPDB, *op. cit.* (fn. 8), p. 6.
[24] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/executive-summary (last visited 19 December 2022).
[25] https://www.enforcementtracker.com/?insights (last visited 8 December 2022).

Till March of 2022, the total sum of fines amounted to around 1.581 billion € with huge fines issued and reported in 2021. The data shows an increase of 1.319 billion from 2021 ET Report, mainly because of fines against "Big Tech".[26] In November of 2022, the overall sum of fines is around 2.3 billion €.[27]

It is worth noting again that the fines reported do not present all fines issued. "There are probably many more unfamiliar fines, exceeding even the numbers of fines available in the database. Even though those fines do not reach big numbers, their importance should not be ignored."[28]

One of the main takeaways from this report was "that there is hardly an area of European data protection law (still) shaped more by national laws and official practice than the GDPR fines. The administrative / sanctions law environment as well as position, personnel and equipment, and finally an authority's self-confidence/understanding of its own role appear to vary significantly between European countries - anything but fully harmonized."[29]

Therefore in 2022, the European Data Protection Board (EDPB) published its new "Guidelines on calculation on fines"[30] (version for public consultation), in efforts to make the practice of DPAs more equal across the European Union.

The constantly growing number of fines, and the fact that the fines issued in 2021 against "Big Tech" continued in 2022, shows a firm stance from DPAs. In the reporting period 2018 - March of 2022, the average fine was around 1,533,910 € across all countries, but that number is largely skewed by massive fines issued against "Big Tech" in 2021.[31]

4. Sectors in more detail

4.1. Finance, Insurance and Consulting

[26] CMS, *op. cit.* (fn. 24).
[27] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[28] CMS, *op. cit.* (fn. 24).
[29] *Ibid.*
[30] EPDB, *op. cit.* (fn. 8).
[31] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures (last visited 7 December 2022).

Till March of 2022, 19 DPAs have imposed 108 fines on banks and other companies in the finance, insurance and consulting sector amounting to a total of 29.19 million €. Among the countries, Spain is the leader both in the number and amount of fines imposed. It has issued 34 fines, 4 of which range between 1 – 6 million €.[32]

The largest group of fines based both on number (43 fines, more than twice as much compared to 21 in 2021) and on the aggregated amount (11,107,455 €, almost twice the amount compared to 6,383,970 € in 2021) were issued due to an insufficient legal basis for data processing. In the majority of these cases, advertising messages were sent to data subjects without their consent. 29 fines were issued because of insufficient technical and organizational measures to ensure information security. This highlights the fact that data security is a key issue in the highly regulated financial and insurance sectors.[33]

The insurance sector is especially exposed to the risks described by GDPR, since all insurance companies collect, maintain and store both private and special category data not only for serving their customers, but also the potential gain this data can return to the company. "For example, it is a common practice for insurance companies and their business partners to exchange personal data for their customers, even as regularly as on a daily basis. An insurer may exchange data with hospitals, car garages, claims management companies, fraud detection services, sales networks such as agencies and brokers, external contact centres for road assistance or legal protection, e-shops for marketing activities etc."[34]

The situation isn't completely bleak for the sector though, Cyber Insurance is definitely a business growth opportunity with unique risks.[35]

Such relatively new insurance products could include coverage for the following:[36] "liability risk, which provides compensation and legal support in the event of third-party claims resulting from

[32] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/finance-insurance-and-consulting (last visited 7 December 2022).
[33] *Ibid.*
[34] Liapakis, '*A GDPR Implementation Guide for the Insurance Industry:*', 7 International Journal of Reliable and Quality E-Healthcare (2018) 34 , available at http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJRQEH.2018100103 (last visited 13 September 2022) , p. 35.
[35] *Ibid.*, p. 36.
[36] This is a rather rare case, usually „modern privacy legislation does significantly improve the position of individuals concerning their rights and freedoms, but at the cost of possibly impeding business opportunities and preventing service providers from offering new services to their customers."; N. Parlov, Ž. Sičaja, T. Katulić i R. Luša,

loss of personal and/or business data; crisis costs to undertake forensic investigations, reputational public repair, customer notification costs, credit monitoring, IT services, and cyber incident response services; fines for research costs, legal assistance, and administrative fines; digital media breach to cover compensation and defence costs related to third-party claims against you arising out of your multimedia activities (e.g. defamation, allegation, or plagiarism); cyber extortion, including ransomware; network interruption, loss of revenues, or net profits associated with network downtime."[37]

Highest fine of 6 million € within the sector wasn't connected to insurance though, it was imposed on a Spanish bank mainly due to an insufficient legal basis for data processing[38]. Customers of the bank were supposed to accept new privacy policies allowing the controller to transfer the customers' personal data to all companies within the banks group. However, the data subjects were not given the option of specifically not consenting to this transfer. The Spanish DPA[39] concluded that the customers' consent did not meet the requirements of an effective consent and, as a result, the data was unlawfully transferred to other companies within the bank's group.[40]

Additionally, the DPA determined that the bank had violated its information obligations as set out in Article 13 and 14 GDPR[41]. "This case shows the importance of establishing and implementing comprehensive internal compliance processes before transferring data to other entities, even within the same group of companies."[42]

Since the highest 4 fines in this sector have all been imposed due to a lack of adequate internal compliance measures to ensure a sufficient legal basis for the processing of customer data, it is advised for companies to "implement comprehensive processes to ensure a clear legal basis for each data processing activity."[43]

"Information security and the lawful interception of communications through telecom service providers infrastructure: advanced model system architecture", *Policija i sigurnost*, vol.30, br. 1/2021, p. 112-130, 2021,p.128.

[37] Ouwerkerk, '*Beware of GDPR - Take Your Cyber Risk Responsibility More Seriously*', in The InsurTech Book (2018) 175, p. 178.

[38] https://www.enforcementtracker.com/ETid-522 (last visited 5 December 2022).

[39] *Agencia Española de Protección de Datos | AEPD*, available at https://www.aepd.es/es (last visited 5 December 2022).

[40] CMS, *op. cit.* (fn. 32).

[41] Article 13 relates to information to be provided where personal data are collected from the data subject and Article 14 to information to be provided where personal data has not been obtained from the data subject.

[42] CMS, *op. cit.* (fn. 32).

[43] *Ibid.*

The second highest reason for which significant fines were issued were insufficient data security measures. "Not only do they cause financial pains, they might lead to considerable reputational damage[44]. Accordingly, companies should focus on strong data security measures."[45]

At the time of writing this, in November of 2022, the number of fines is 146 and they amount to 34,403,108 €, which is 38 and a bit over 5 million € more than approximately 8 months prior. The average in the last 8 months is around 137,187 €, which is almost a half from before, the data gathered till March of 2022, when it was approximately 270,278 €.[46]

4.2. Accommodation & Hospitality

Till March of 2022, 9 DPAs have imposed 37 fines on restaurants, hotels and other companies in the accommodation and hospitality sector, amounting to a total of 21,487,707 €. The overall average of fines in this sector was 631,903 €, but this number was skewed by one fine of above 20 million € by the British ICO[47]. Without that fine in the equation, the average was just under 30,000 €.[48]

The Spanish DPA issued the most fines (21), followed by Germany (9). The majority of the fines in the accommodation and hospitality sector were imposed due to illegal video surveillance (26 cases). "The activity of DPAs in this sector is not only on "big players", but also on small restaurants, stores or hotels, which is why the actual fines are comparatively low with a few exceptions."[49]

Highest fine by far in this sector was issued in 2020: the British ICO imposed a fine of 20.45 million € on Marriott International, Inc.[50] based on a cyber incident originating from a vulnerability

[44] "Even though immaterial damages such as loss of reputation due to a mention in an activity report or a high-damage claim can be more painful for an enterprise in certain cases, technically administrative fines and criminal penalties are to be regarded as the most severe sanctions for data protection violations."; Sebastian J. Golla, *Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR*, 8 (2017) JIPITEC 70 para 1., p.71
[45] CMS, *op. cit.* (fn. 32).
[46] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[47] https://ico.org.uk/ (last visited 8 December 2022).
[48] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/accommodation-and-hospitality (last visited 7 December 2022).
[49] *Ibid.*
[50] https://www.enforcementtracker.com/ETid-60 (last visited 5 December 2022).

in the IT systems[51] of the Starwood hotels group which was acquired by Marriott in 2016. This vulnerability led to the exposure of personal data from approximately 339 million guest records.[52]

Even though the majority of fines in this sector were issued for unlawful use of CCTV systems, the 26 fines only amount to 91,400 €. Spanish DPA imposed most of them (19), ranged between 900 and 6,000 €.[53]

At the time of writing this, in November of 2022, the number of fines is 48, which is 11 and about 620,000 € more issued in the last 8 months. So, the average from the last 8 months is around 56 000 €, which looked at the average before (ignoring the outlier 20 million € fine by the British ICO) is an increase of around 26 000 €.[54]

4.3. Health Care

Till March of 2022, 25 DPAs have imposed 94 fines for data protection violations by hospitals, pharmacies, physicians and medicine suppliers. In this sector, more fines have been issued in the past year alone than in the previous reporting periods taken together. The sum of fines amounts to more than 12.7 million € which is an increase of 3 million € compared to last year. The numbers show an interesting trend, the number of fines is more than doubled than last year, but the absolute amount only increased by less than 25%, indicating that the average amount of fines was lower in 2021 than in recent years.[55]

"This could be interpreted to mean that in 2021, the authorities did not only consider major landmark cases but have widened the scope of their supervisory activities and also address less prominent cases."[56]

[51] "Since most of personal data collection, processing and storing is done through information systems an appropriate level of security of those systems is required to ensure the security of personal data."; T. Katulić and N. Protrka, "Information Security in Principles and Provisions of the EU Data Protection Law," *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, p. 1219, Opatija, Croatia, 2019, pp. 1219-1225
[52] CMS, *op. cit.* (fn. 48).
[53] *Ibid.*
[54] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[55] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/health-care (last visited 7 December 2022).
[56] *Ibid.*

The main reason for the fines was lack of sufficient technical and organizational data protection measures (38 fines with a total amount of 9.6 million €). In the last year there were 17 cases which added 0,7 million €.[57]

For this sector it is important that GDPR presents and defines a new concept named "data concerning health". "This concept aggregates all personal data of a patient that discloses information about their past, present or future physical and mental health. It also includes all the administrative information collected by medical units during a hospital episode or during a simple general practitioner visit such as registration number, unique identification number, all data derived from laboratory test, laboratory results, etc."[58][59]

There was a case in Sweden that concerned Sweden's central telephone hotline offering advice on health-related topics. Recordings of the phone calls were available on a web server with no password protection or other security measures due to a misconfiguration. The main provider responsible for setting up and organizing the telephone service was fined 1.2 million €[60]; the provider who hosted the data was fined 64,500 €[61].[62]

"It is clear that privacy regulation such as GDPR and privacy rules related to collection, sharing and transferring of personal and sensitive information is significantly impacting governments and businesses. These rules and limitations will impact both new and existing applications and may require significant modifications to existing systems and data flows. This has especially been true for crisis times in health care, like the COVID-19 pandemic."[63]

---

[57] *Ibid.*

[58] Stan and Miclea, '*New Era for Technology in Healthcare Powered by GDPR and Blockchain*', in S. Vlad and N. M. Roman (eds.), 6th International Conference on Advancements of Medicine and Health Care through Technology; 17–20 October 2018, Cluj-Napoca, Romania vol. 71 (2019) 311, p. 312,313.

[59] "The categorization of sensitive data presents advantages, as it accounts for the need for additional caution when dealing with health-related data. It can be efficient to prevent unconsented secondary uses, but this special category can also act as a disincentive for researchers, especially given the high sanctions they incur in case of sensitive data breach."; Forcier et al., '*Integrating Artificial Intelligence into Health Care through Data Access: Can the GDPR Act as a Beacon for Policymakers?*', 6 Journal of Law and the Biosciences (2019) 317 , available at https://academic.oup.com/jlb/article/6/1/317/5570026 (last visited 20 January 2023) , p. 9.

[60] https://www.enforcementtracker.com/ETid-718 (last visited 10 December 2022).

[61] https://www.enforcementtracker.com/ETid-719 (last visited 10 December 2022).

[62] CMS, *op. cit.* (fn. 55).

[63] Larrucea et al., '*Towards a GDPR Compliant Way to Secure European Cross Border Healthcare Industry 4.0*', 69 Computer Standards & Interfaces (2020) 103408, available at https://linkinghub.elsevier.com/retrieve/pii/S0920548919304544 (last visited 13 September 2022), p. 2.

GDPR brought some big changes to national health services because of its recital 47 which states; in reference to the legitimate interests of a controller as legal basis for processing a data subjects personal data; "Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks". "This in effect means that processing personal data using legitimate interests as a basis is no longer an option for, for example, National Health Service England and primary care in particular."[64]

"The key causes of fines in the health care sector continue to originate from technical and organizational data protection deficiencies[65] and in particular inappropriate setup (or lack of) access restrictions and access management systems."[66]

"The COVID-19 pandemic showed that the existing digital data processing structures were not yet ready to meet newly arising needs. New systems had to be set up rather quickly which led to the use of readily available, but inappropriate tools and lack of further organizational measures."[67]

At the time of writing this, in November of 2022, there are 127 fines given to this sector, so 33 new fines that amount to about 2.2 million € have been issued since March of 2022.[68]

4.4. Industry & Commerce

Till March of 2022, 24 DPAs have imposed 233 fines on a variety of different enterprises including utility companies, global retailers, grocery store chains and food-delivery services, with a total fine volume of 776 million € (an increase of 769 million € in comparison to the 2021 ETR). Meaning

[64] Shu and Jahankhani, '*The Impact of the New European General Data Protection Regulation (GDPR) on the Information Governance Toolkit in Health and Social Care with Special Reference to Primary Care in England*', in 2017 Cybersecurity and Cyberforensics Conference (CCC) (2017) 31, p. 35.
[65] Health care, while constantly improving with technology, can also suffer from it: "In 2017, the US Food and Drug Administration (FDA) confirmed that certain medical devices had vulnerabilities that could allow hackers to access the devices such as pacemakers and defibrillators used to monitor and control patients' heart functions and prevent heart attacks. Because of the vulnerability of the transmitter, hackers could control the shocks, manage the incorrect pacing, and drain the battery."; Vojković, Milenković and Katulić, '*IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law*', 11 Business Systems Research Journal (2020) 167, p. 177, available at https://www.sciendo.com/article/10.2478/bsrj-2020-0033
[66] CMS, *op. cit.* (fn. 55).
[67] *Ibid.*
[68] GDPR Enforcement Tracker, *op. cit.* (fn. 25).

that in the last year the number of fines more than doubled, and those new 120 fines amount to 99% of the total fine volume.[69]

The average amount of fines in this sector was roughly 3.53 million €, but that number was heavily impacted by the extraordinary fine from Luxembourg DPA against Amazon for the amount of 746 million €[70].[71]

Main reasons for fines were: insufficient legal basis for data processing (67), insufficient fulfilment of information obligations (48) and insufficient technical and organizational measures (37). Spanish DPA was the most active, imposing more than 45% of all fines in this sector (106), followed by the authorities in Italy (21) and Romania (20).[72]

As already mentioned, the biggest fine in the past year was the 746 million € penalty imposed on Amazon Europe Core S.a.r.l. by the Luxembourg DPA[73] (CNPD). Amazon has already stated that it plans to appeal this decision. Specifics of the case have not been publicly disclosed as the CNPD is bound to professional secrecy by Luxembourg laws until the appeal process is completed. This fine is the largest GDPR fine across all sectors thus far. Till March of 2022 it exceeded the total of the other 9 of the top 10 highest fines in all sectors by about 150 million € and represented nearly half of the amount of all fines across all sectors combined since the GDPR came into effect[74]. That is no more the case. In November of 2022 it accounts for about 31% of all fines, and although it is still the largest fine, its lead is significantly smaller. 2nd and 3rd highest fines combined come up to 670 000 000 €, only 76 000 000 € less. If one adds in the 4th, the number is 895 million €, 149 000 000 € more than the Amazon fine, achieved only in 3 other fines. That is to say, from March of 2022, there have been a few quite high amount fines that make the Amazon fine not completely alone and untouchable at the top of the highest fines as before.[75]

[69] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/industry-and-commerce (last visited 7 December 2022).
[70] GDPR Enforcement Tracker, *op. cit.* (fn. 15).
[71] CMS, *op. cit.* (fn. 69).
[72] *Ibid.*
[73] https://cnpd.public.lu/en.html (last visited 5 December 2022).
[74] CMS, *op. cit.* (fn. 69).
[75] GDPR Enforcement Tracker, *op. cit.* (fn. 25).

"In particular, non-compliance with general data protection principles and insufficient data security measures resulted in severe fines for companies in the industry and commerce sector. In terms of general data protection principles, authorities are closely examining the necessity of data processing and the length of storage periods."[76]

At the time of writing this, in November of 2022, the number of fines increased by 84 to 317, and the sum by around 78 million €. This high number of new fines combined with a quite high number of old ones puts "Industry and Commerce" firmly in 1st place by the number of fines, having 112 fines more than the next sector, "Media, Telecoms & Broadcasting". It is crucial to emphasize the importance of this sector: it has more fines than any other, it's 2nd by the sum of fines because 36% of the sum of all fines issued since the introduction of GDPR in 2018 belong to this sector (31% is the already mentioned Amazon fine).[77]

4.5. Real Estate

Till March of 2022, 30 fines from 11 DPAs have been imposed on data controllers in the Real Estate sector. The fines amount to 524,470 €. 16 out of 30 fines in this sector, meaning the majority, have been issued for non-compliance with general data processing principles. 6 out of 30 have been for insufficient legal basis for data processing.[78]

Since the majority of data controllers in this sector are small businesses or homeowner associations, the fines are comparatively small and range from 500 to 29,500 €. There are a few outliers, though. One was a fine issued by the French Data Protection Authority at 400,000 €[79](for a lack of basic security measures and excessive data storage). [80]

This sector, just as "Accommodation and hospitality" has issues with video surveillance. Sometimes data subjects have not been informed of the surveillance measures or provided information did not meet requirements of Article 13 GDPR[81]. "There are also no justifications for

[76] CMS, *op. cit.* (fn. 69).
[77] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[78] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/real-estate (last visited 7 December 2022).
[79] https://www.enforcementtracker.com/ETid-24 (last visited 7 December 2022).
[80] CMS, *op. cit.* (fn. 78).
[81] Article 13 relates to information to be provided where personal data are collected from the data subject.

CCTV systems to record audio, and the data recorded has to be sufficiently against unauthorized access. It seems that the biggest issue with CCTV surveillance is placement of the cameras, since the majority of fines were issued because of that. CCTV surveillance should not capture images from public property such as public streets or footpaths or inside of private apartments."[82]

The Real Estate sector "requires the processing of sensitive data, as prospective tenants provide landlords with information such as ID-documents and detailed financial information and data processors may collect and process data by using CCTV systems to protect their property against theft, vandalism and similar inconveniences. Adequate technical and organizational measures must be in place to ensure adherence to GDPR with a special focus on general processing principles such as data minimization or storage limitation."[83]

At the time of writing this, in November of 2022, there are 43 fines assigned to this sector, which is an increase of 13. Even though there were only 13 new fines, the total sum in this sector increased to 2,577,570 € meaning an increase of over 2 million €. This shows that there is/are definitely outlier fines but it's hard to pinpoint exactly because GDPR Enforcement Tracker website doesn't allow search by sectors.[84]

4.6. Media, Telecoms & Broadcasting

Till March of 2022, 18 DPAs have issued 177 fines amounting to 596 million €. Since the overall amount of fines was about 1,6 billion € across all sectors, this sector alone contributed to more than a third.[85]

In November of 2022, this sector can only be seen as even more important than before. It used to be more than a third, now it is more than a half of all fines. With 205 fines, still notably less than "Industry and Commerce" with 317, this sector accrued almost 1.3 billion € in fines (1,295,557,541). The data shows that in the last 8 months with 28 fines, the overall sum increased by around 700 million €, meaning it more than doubled. The main culprits for this are two fines

[82] CMS, *op. cit.* (fn. 78).
[83] *Ibid.*
[84] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[85] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/media-telecoms-and-broadcasting (last visited 7 December 2022).

from the Ireland DPA issued in September and November of 2022, against Meta Platforms, Inc. (405 million €), and Meta Platforms Ireland Limited (265 million €). Together they amount to 670 million € which put "Media, Telecoms & Broadcasting" in the lead over long time leading "Industry and Commerce".

This sector features 8 out of 10 of overall top 10 fines. 2nd highest fine since the introduction of GDPR is already mentioned fine against Meta Platforms, Inc[86] by the Ireland DPA for 405 000 000 €. Irish DPA discovered that on Instagram business accounts of minors, their cell phone numbers and email addresses were publicly displayed. Also, the settings for the underage user's accounts were set to "public" by default. Their initial draft proposed a fine of 30 – 50 million €, but because the draft was submitted to other affected European supervisory authorities, of which 6 stated objections, it led to a dispute resolution procedure at the European Data Protection Board. The EDPB requested the Ireland DPA to increase the proposed fine.[87]

In November of 2022, 3rd highest fine was issued, again by the Irish DPA. Meta Platforms Ireland Limited was fined for 265 000 000 €, after an investigation started by the media reports that indicated a dataset containing personal data from Facebook had been made available on a hacking platform. The data leak affected up to 533 million users with their data such as phone numbers and email addresses.[88]

Irish DPA also imposed the 4th highest fine of 225 million €[89] against WhatsApp Ireland LTD for violation of the data transparency principle. WhatsApp failed to provide users information on the data processing operations such as the data sharing with Facebook in an intelligible and easily accessible manner, including towards children.[90]

[86] U.S. companies were expected to struggle with complying with the GDPR especially because „rights afforded dana subjects in the EU are not rights that American data subjects have nor that U.S. companies have been operating under."; Houser, Kimberly and Voss, W. Gregory, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?* (July 11, 2018). Working Paper, 25 Rich. J. L. & Tech. 1, 2018 Forthcoming, Available at SSRN: https://ssrn.com/abstract=3212210
[87] GDPR Enforcement Tracker, *op. cit.* (fn. 20).
[88] GDPR Enforcement Tracker, *op. cit.* (fn. 21).
[89] GDPR Enforcement Tracker, *op. cit.* (fn. 16).
[90] CMS, *op. cit.* (fn. 85).

At the end of 2021, France DPA issued the 5th (90 000 000 €[91] against Google LLC), 6th (60 000 000 €[92] against Facebook Ireland Ltd.), 7th (60 000 000 €[93] against Google Ireland Ltd.), and back in 2019 the 8th (50 000 000 €[94] against Google LLC) highest fine. The last one was imposed for lack of transparency, insufficient information and lack of legal basis concerning the creation of a Google account during the configuration of a mobile phone using the Android operating system.[95][96] The three other fines relate to the companies' unlawful use of cookies on Google, YouTube and Facebook. The companies offered clear buttons to accept cookies, but there was no equivalently easy option to reject cookies, therefore they violated the French Law on Informatics and Freedoms.[97]

In 2020, Italian DPA imposed a fine of 27 800 000 €[98] against TIM (telecommunications operator) for, among other things, lack of consent for marketing activities, addressing of data subjects who asked not to be contacted with marketing offers, invalid consents collected in TIM apps, lack of appropriate security measures to protect personal data and lack of clear data retention periods.[99] This is the 10th highest fine.[100]

4.7. Public Sector & Education

Till March 2022, 22 DPAs have imposed 136 fines on representatives of local governments (such as mayors), police officers, schools, universities and other public bodies or educational institutions amounting to a total of more than 14,1 million €. In comparison to the 2021 ETR, this is a 9,1 million € increase in only 58 new fines.[101]

[91] GDPR Enforcement Tracker, *op. cit.* (fn. 17).
[92] GDPR Enforcement Tracker, *op. cit.* (fn. 19).
[93] GDPR Enforcement Tracker, *op. cit.* (fn. 18).
[94] https://www.enforcementtracker.com/ETid-23 (last visited 9 December 2022).
[95] *Ibid.*
[96] In 2019, this fine represented „around two-thirds of the daily profits of the firm's parent company Alphabet."; *Google is first company hit with major GDPR fine*, Computer Fraud & Security (2019), p. 3., available at http://www.magonlinelibrary.com/doi/10.1016/S1361-3723%2819%2930013-2
[97] CMS, *op. cit.* (fn. 85).
[98] https://www.enforcementtracker.com/ETid-189 (last visited 9 December 2022).
[99] *Ibid.*
[100] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[101] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/public-sector-and-education (last visited 7 December 2022).

There were 47 fines related to insufficient legal bases for data processing and 42 for insufficient technical and organizational measures. That means these 2 causes cover the reasons for the majority of fines (89 out of 136). After these, there were 22 fines for non-compliance with general data processing principles.[102]

During the Covid-19 pandemic, the use of digital products (e.g. messenger apps or video conferences tools) by universities or schools, in particular for holding online classes and examinations, has increased significantly.[103] This has led to a lot of debate on which software exactly should be used with different criteria from different teachers and professors. One of the most important ones was security. "For example, when conducting a conference call for lecture, the teacher may want to know that security concerns like unwelcome guests, Zoombombing[104], and camera hacking are reduced, if not eliminated entirely. People need to feel secure in the technology they use on a daily basis when joining an online class."[105]

In this context, the Italian DPA imposed a fine of 200,000 €[106] on Bocconi University for the use of a remote monitoring software in online examinations. "The software was able to monitor the behaviour of the students through video recordings and snapshots taken at random intervals. In addition, the exam was audio-visually recorded and a photograph was taken of each examinee at the beginning of the exam. In its investigation the DPA found that students were not properly informed of the processing of their personal data (e.g. no information about the audio visual recordings). It also found that the university had processed the personal data without a valid legal basis. In light of the health risks in the pandemic, the obtained consents of the students could not be considered voluntary as the in-person exam was the only proposed alternative to the online exams."[107]

[102] *Ibid.*
[103] *Ibid.*
[104] Lorenz, '*'Zoombombing': When Video Conferences Go Wrong*', The New York Times (2020) , available at https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html (last visited 8 December 2022).
[105] Cavus and Sekyere-Asiedu, '*A Comparison of Online Video Conference Platforms: Their Contributions to Education during COVID-19 Pandemic*', 13 World Journal on Educational Technology: Current Issues (2021) 1180 , available at https://un-pub.eu/ojs/index.php/wjet/article/view/6329 (last visited 13 September 2022) , p. 1174.
[106] https://www.enforcementtracker.com/ETid-876 (last visited 5 December 2022).
[107] CMS, *op. cit.* (fn. 101).

The number of fines regarding the processing of health data has also increased: for example, the Lithuanian DPA[108] (VDAI) imposed a fine of 12,000 €[109] on the Lithuanian National Health Service (NVSC) regarding the use of a quarantine app in the spring of 2020. The DPA found that the controller had not taken sufficient technical and organizational measures and had not carried out a data protection impact assessment, although this would have been necessary. Further, the controller had provided non-transparent and incorrect information in the app's privacy policy.[110]

Covid-19 apps[111] in general have been a cause of a lot of discussion, from a legal, technical and ethical perspective. "Some of the best solutions for this type of apps use the Bluetooth connection of mobile phones to determine contacts between people and therefore the probability of contagion, and then suggested related measures."[112]"Legally, there were concerns on how to make use of those apps comply with the GDPR, but it is considered that privacy concerns can be seriously mitigated, and that there are other more pressing, ethical difficulties."[113]

The apps also "had to be in line with the thinking of the Ethics Advisory Group, which was established by the European Data Protection Supervisor, in order to analyse the new ethical challenges posed by digital developments and current legislation, especially in relation to the GDPR."[114] Ethics Advisory group published a report[115] that can be useful in this case as guidance. At the time of writing this, there are 120 contact tracing mobile apps available in 71 countries.[116] In some other countries, there are very questionable behaviours concerning gathered data in aforementioned apps. "In China, where Alipay and WeChat hosted the Health Code app used to track coronavirus exposure, those companies have asserted rights contractually to keep the data

[108] *State Data Protection Inspectorate*, available at https://vdai.lrv.lt/en/ (last visited 8 December 2022).
[109] https://www.enforcementtracker.com/ETid-571 (last visited 5 December 2022).
[110] CMS, *op. cit.* (fn. 101).
[111] *COVID-19 Apps*, *Wikipedia*, 24 August 2022, available at https://en.wikipedia.org/w/index.php?title=COVID-19_apps&oldid=1106470205 (last visited 14 September 2022).
[112] Luciano, '*Mind the App—Considerations on the Ethical Risks of COVID-19 Apps*', 33 Philosophy & Technology (2020) 167 , available at https://link.springer.com/10.1007/s13347-020-00408-5 (last visited 14 September 2022) , p. 1.
[113] *Ibid.*, p. 2.
[114] Floridi, '*Soft Ethics, the Governance of the Digital and the General Data Protection Regulation*', 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences (2018) 20180081 , available at https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0081 (last visited 14 September 2022).
[115] *Burgess, J.P., Floridi, L., Pols, A. and van Den Hoven, J., 2018. Towards a Digital Ethics: EDPS Ethics Advisory Group.*, available at https://philpapers.org/archive/BURTAD-3.pdf (last visited 14 September 2022).
[116] https://www.top10vpn.com/research/covid-19-digital-rights-tracker/ (last visited 14 September 2022).

once the crisis is over."[117]"In view of privacy rights, GDPR requires a general lawful basis and special category exemption lawfully to collect and analyse data concerning health. Additionally, any use of data, which exceeds what is necessary for the stated lawful basis, is prohibited by the GDPR unless it is covered by a separate permissible basis."[118]

Highest fine in the public and education sector till March of 2022 was issued by the Dutch Supervisory Authority for Data Protection[119] (AP), which sanctioned the Dutch Minister of Finance with a fine of 2.75 million €[120] for the processing of dual citizenship data of 1.4 million people in the context of childcare benefit applications, although the data on dual nationality of Dutch citizens would not have been necessary when assessing an application for childcare benefits. The data was also used – without any legal basis – to combat organized fraud and automatic classification in the authority's risk system.[121]

"Public authorities have a special position of trust that requires particularly strict compliance with data protection laws and an outstandingly high level of data security."[122]

It should be noted that in Croatia, if an administrative fine is imposed against a legal person with public authority or against a legal person performing a public service, the imposed administrative fine must not jeopardize the performance of such public authority or public service (Article 44(2))[123], and an administrative fine may not be imposed on a public authority (Article 47)[124].

[117] *Joint Webinar - Beyond the Exit Strategy: Ethical Uses of Data-Driven Technology in the Fight against COVID-19*, The Nuffield Council on Bioethics, available at https://www.nuffieldbioethics.org/news/joint-webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19 (last visited 14 September 2022).
[118] Bradford, Aboy and Liddell, '*COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes*', 7 Journal of Law and the Biosciences (2020) lsaa034 , available at https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsaa034/5848138 (last visited 14 September 2022) , p. 12.
[119] https://www.autoriteitpersoonsgegevens.nl/en (last visited 5 December 2022).
[120] https://www.enforcementtracker.com/ETid-946 (last visited 5 December 2022).
[121] CMS, *op. cit.* (fn. 55).
[122] *Ibid.*
[123] *Zakon o Provedbi Opće Uredbe o Zaštiti Podataka, NN 42/2018*, available at https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html (last visited 10 December 2022).
[124] *Ibid.*

The number of fines in the public sector for violations of data protection law with regard to the processing of sensitive data, profiling and tracking or surveillance of individuals has increased over recent years. It seems likely that this trend will continue in the future.[125]

At the time of writing this, in November of 2022, there are 175 fines from this sector which shows an increase of 39 fines that amount to around 5.4 million €. This increase occurred in a time frame of around 8 months, which compared to a year that passed between 2021 ET report and 2022 ET report that showed an increase of 58 fines affirms that fines in this sector so far were issued at a stable rate. This is somewhat surprising since there were expectations that a lot more COVID-19 related violations will be registered and sanctioned in the coming years, and that increase has not yet occurred.[126][127]

4.8. Transportation & Energy

Till March 2022, 14 DPAs have imposed 47 fines that amount to more than 81 million €. The average of fines in this sector is around 1,82 million €. The 5 highest fines are all above 3 million €. The most common reason for fines was insufficient legal basis.[128]

"Italian DPA imposed a 26.5 million €[129] fine on a gas and electricity supplier for various breaches. The DPA found that the controller illegally processed the personal data of millions of users for telemarketing purposes. The users received unsolicited promotional calls even though no consent was given, or the users had already requested the controller to delete their personal data or had objected to their processing for advertising purposes. Furthermore, the controller failed to sufficiently provide data subjects with the required and timely feedback on their requests to exercise their rights of access and objection. Finally, from the DPA's perspective the controller did not cooperate sufficiently with the DPA during the extensive investigation."[130]

[125] CMS, *op. cit.* (fn. 101).
[126] *Ibid.*
[127] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[128] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/transportation-and-energy (last visited 7 December 2022).
[129] https://www.enforcementtracker.com/ETid-1005 (last visited 5 December 2022).
[130] CMS, *op. cit.* (fn. 128).

Most noteworthy is the heaviest fine of 2020 (that had already been announced in 2019): The British ICO imposed a fine of 22 million €[131] on the British Airways airline based on insufficient technical and organizational security measures. In 2018, British Airways had been the target of a major cyberattack (personal data of around 500,000 customers including login, payment card and travel booking details, as well as name and address information). The ICO's investigation concluded that poor security measures were at least one reason why the attack was successful and why it had remained undetected for two months.[132]

Despite fines in the transportation and energy sector being quite high, they are still comprised of the same criteria: the amount of data subjects involved, the severity of the single violations, and the willingness to cooperate with the respective DPA.[133]

At the time of writing this, in November of 2022, the data shows that in the last 8 months there have been 19 new fines that put the total sum of this sector to 84,854,214 € meaning it is the 3rd highest sector by the sum of fines. It has more than 10 times less than the 2nd "Industry and Commerce" and about 37 million € more than 4th place "Employment". This clearly illustrates how much higher the fines issued to "Media, Telecoms and Broadcasting" and "Industry and Commerce" are compared to every other sector. With that being said, "Transportation and Energy" definitely has very high fines, considering that in total it has only 66 fines. These new 19 fines added around 4 million € to the total sum.[134]

4.9. Individuals & Private Associations

Till March 2022, 15 DPAs have imposed 96 fines to private individuals, homeowner associations, individual entrepreneurs, private sport associations and leagues for the total amount of 1,424,746 €.[135]

[131] https://www.enforcementtracker.com/ETid-58 (last visited 5 December 2022).
[132] CMS, *op. cit.* (fn. 128).
[133] *Ibid.*
[134] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[135] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/individuals-and-private-associations (last visited 7 December 2022).

The highest fine of 525,000 €[136] was issued against the Royal Dutch Tennis Association for selling contact details of 350,000 members without permission to sponsors who contacted them for direct marketing purposes via phone and email. All fines above 20,000 € were imposed on sports associations and other big non-profit organizations, while against private individuals usually didn't go over 2,000 €. The lowest fine of 48€[137] was imposed on an Estonian police offer who accessed personal data in a police database for private research.[138]

It appears that DPAs tend to treat bigger non-profit organizations like similarly sized businesses, which is an interesting development, seeing as to the new guidelines indicate that the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) is also relevant.[139]

DPAs in this sector focus heavily on illegal video surveillance, nearly half of all fines were imposed for that reason. Dashcams especially seem to be an issue.[140]

Europe in general has a lot of diversity when it comes to dash cams. In Russia, almost all citizens own and employ dash cams, due to significant police corruption, high rates of accidents, and unsafe road conditions. In Portugal, Luxembourg and Austria, the use of dash cams or recording devices in public is illegal, while they are perfectly legal in Spain and the UK. In France and Belgium dash cams are legal only for private use, and it is illegal to upload footage publicly online, which is an interesting adaption to respecting privacy.[141]

At the time of writing this, in November of 2022, there are 145 fines related to this sector, meaning 49 new fines in the last 8 months. These amount to 107,370 €, so the average of the last 8 months is around 2 200 €.[142]

[136] https://www.enforcementtracker.com/ETid-218 (last visited 5 December 2022).
[137] https://www.enforcementtracker.com/ETid-384 (last visited 5 December 2022).
[138] CMS, *op. cit.* (fn. 135).
[139] EPDB, *op. cit.* (fn. 8), p. 17.
[140] CMS, *op. cit.* (fn. 135).
[141] Helena, *Dash Cams around the World*, 26 August 2020, VIA Technologies, Inc., available at https://www.viatech.com/en/2020/08/dash-cams-around-the-world/ (last visited 13 September 2022).
[142] GDPR Enforcement Tracker, *op. cit.* (fn. 25).

4.10. Employment

Till March of 2022, DPAs have imposed a total of 74 fines in connection with the processing of employee data. The data shows 32 new fines compared to 2021 ETR which increased the overall amount in this only by about 0.5 million €, bringing it to almost 48 million €. The average fine was halved from 2021(1.2 million to 0.6 million €), and the highest fine issued by Italian DPA amounted to 84,000 €.[143]

By far the largest fine in this sector was imposed in 2020 by the German DPA, against H&M Hennes & Mauritz Online Shop A.B. & Co. KG (fashion company) for 35,258,708 €[144] due to excessive storage of employee data with an insufficient legal basis. Supervisors compiled dossiers on employees over several years, including health data obtained in return-to-work interviews and hearsay relating to family problems and religious beliefs. They used the dossiers to evaluate employee work performance and make employment decisions.[145]

Already mentioned, the highest new fine from the issuing of 2021 ETR, was imposed by the Italian DPA against the City of Bolzano/Bozen for 84 000 €[146] due to, broadly said, unlawful behaviour centred around or involving CCTV as a means for employee monitoring. There have been a decent amount of cases this nature across Europe, enough to make it significant in this sector. Usually, the employers had reasons to operate CCTV, but did not take the employee's interests sufficiently into account.[147]

In recent years, employers have had to justify their data protection compliance not only to DPAs but also to trade unions and/or works councils. Employees may be more likely to raise complaints with a DPA, especially in case of conflict situations.[148] An initial analysis of employee data-related fines indicates that because of a structural imbalance between employers and employees, employee

[143] https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/employment (last visited 9 December 2022).
[144] https://www.enforcementtracker.com/ETid-405 (last visited 10 December 2022).
[145] CMS, *op. cit.* (fn. 143).
[146] https://www.enforcementtracker.com/ETid-747 (last visited 10 December 2022).
[147] CMS, *op. cit.* (fn. 143).
[148] *Ibid.*

consent is problematic. The best choice for employers may be relying on a statutory legal basis (e.g. contract performance).[149]

From March to November of 2022, this sector acquired 14 new fines but its total amount still remains just under 48 million €. Notably, it is the 4th sector by the overall sum, just behind "Transportation and Energy", which clocks in also under 100 million.[150]

5. Guidelines on the calculation of administrative fines

There are two main guidelines made by the EDPB in relation to fines under GDPR.

One of them is "Guidelines on the application and setting of administrative fines" which addresses "the circumstances in which an administrative fine would be an appropriate tool and interpret the criteria of Article 83 GDPR in this respect"[151][152], which was adopted in 2018. The other is "Guidelines on the calculation of administrative fines"[153] which addresses the methodology for the calculation of administrative fines. The latter is not yet fully adopted, but it was given to public consultation from 16th of May 2022 to 27th of June 2022. This work will further focus on it and on the comments given in relation to it. "The two sets of Guidelines are applicable simultaneously and should be seen as complementary."[154]

5.1. Scope

"According to Article 83(7) GDPR, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State and these Guidelines do apply to the calculation of the fine to be imposed on

[149] *Ibid.*
[150] GDPR Enforcement Tracker, *op. cit.* (fn. 25).
[151] EPDB, *op. cit.* (fn. 8), p. 5.
[152] *Guidelines on the Application and Setting of Administrative Fines for the Purpose of the Regulation 2016/679, WP253 (Hereinafter Referred to as "Guidelines WP253")*
[153] EPDB, *op. cit.* (fn. 8).
[154] *Ibid.*, p. 5.

public authorities and bodies, with the exception of a chapter 4.4.[155] concerning using annual turnover to create a starting amount."[156]

Paragraph 6 of the Guidelines states: "These Guidelines can be seen as following a step-by-step approach, though supervisory authorities are not obliged to follow all steps if they are not applicable in a given case, nor to provide reasoning surrounding aspects of the Guidelines that are not applicable."[157]

This has been criticized arguing that "above wording implies that DPAs are obliged to follow the steps described in the Guidelines if they are applicable in that particular case. However, under Article 70(1)(k), the EDPB can only provide recommendations on the application of fines."[158]

5.2. Methodology for calculating the amount of the fine

"The calculation of the amount of the fine is at the discretion of the supervisory authority. The GDPR requires that the amount of the fine shall in each individual case be effective, proportionate and dissuasive (Article 83(1) GDPR). Moreover, when setting the amount of the fine, supervisory authorities shall give due regard to a list of circumstances that refer to features of the infringement (its seriousness) or of the character of the perpetrator (Article 83(2) GDPR). The quantification of the amount of the fine is therefore based on a specific evaluation carried out in each case, taking account of the parameters included in the GDPR."[159]

"Guidelines propose that in certain circumstances the supervisory authority may consider that certain infringements can be punished with a fine of a predetermined, fixed amount. It is at the discretion of the supervisory authority to establish which types of infringements qualify as such, based on their nature, gravity and duration. The supervisory authority cannot make such a determination if this is prohibited or would otherwise conflict with the national law of the Member State."[160]

---

[155] This chapter is not marked in the document.
[156] EPDB, *op. cit.* (fn. 8), p. 6.
[157] *Ibid.*
[158] Foreign Investors Council, *FIC Position on EDPB Guidelines 4.2022*, p. 2, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/FIC%20Position%20on%20EDPB%20Guidelines%204.2022.pdf (last visited 26 August 2022).
[159] EPDB, *op. cit.* (fn. 8), p. 7.
[160] *Ibid.*, p. 8.

"Fixed amounts can be established at the discretion of the supervisory authority, taking into account – inter alia – the social and economic circumstances of that particular Member State, in relation to the seriousness of the infringement as construed by Article 83(2)(a), (b) and (g) GDPR. It is recommended that the supervisory authority communicates the amounts and circumstances for application beforehand."[161]

This idea has proven to be quite controversial. Some argue that "it is not fully correct" and that in their view "it could be contrary to the requirements of the GDPR set out in Article 83 (2) (the requirements to take into account the circumstances of each individual case)."[162]

Others say that "it is not comprehensible as it cannot be derived from the GDPR", also pointing out that "one of the most important tasks of the EDPB is to ensure uniform application."[163]Even further, for some "it is inconsistent with GDPR's requirement for each individual case to be subject to an effective, proportionate and dissuasive administrative fine (Article 83(1) of the GDPR)."[164]

Some have pointed out that "the consequence is to (re)create a distortion between Member States as: some headquarters fall under the supervision of authorities that are stricter in their control policy; non-European players choose to locate their headquarters in Member States[165] where these authorities have a reputation for being particularly lenient."[166]

---

[161] *Ibid.*

[162] V. Rámiš, A. Selby and F. Nonnemann, *2022_06_27_SpOOU_EDPB_Guidelines_calculations_fines (EN)_final*, p. 4, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2022_06_27_SpOOU_EDPB_Guidelines_calculations_fines%20%28EN%29_final.pdf (last visited 26 August 2022).

[163] R. Weiß, *20220627_Bitkom Position Paper Administrative Fines GDPR*, p. 3, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/20220627_Bitkom%20Position%20Paper%20administrative%20fines%20GDPR.pdf (last visited 26 August 2022).

[164] M. Raphael, *CEN-CLC JTC 13 WG5 Consultation Task Force Feedback on EDPB Guidelines 042022 on the Calculation of Administrative Fines under the GDPR*, p. 3, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/CEN-CLC%20JTC%2013%20WG5%20Consultation%20Task%20force%20feedback%20on%20EDPB%20Guidelines%20042022%20on%20the%20calculation%20of%20administrative%20fines%20under%20the%20GDPR.pdf (last visited 26 August 2022).

[165] Referring to "the state of data protection in the first decade of this century, where transposition measures of the Data Protection Directive resulted in a heterogenous patchwork of national laws allowing Big Data to choose places of establishment in Europe based on stringency of Member State laws and especially national supervisory bodies."; T. Katulić, *"Towards the Trustworthy AI: Insights from the Regulations on Data Protection and Information Security"*, Medijska istraživanja, vol.26, br. 2, p. 9-28, 2020., p. 15.

[166] E. Flament-Mascaret and A. Fontaine, *EDPB Guidelines on the Calculation of Administrative Fines under the GDPR - AFEP - June 2022*, p. 2, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/EDPB%20guidelines%20on%20the%2

5.3. One sanctionable conduct

"The relevant sanctionable behaviour needs to be assessed and identified on a case-by-case basis. For example, in a certain case 'the same or linked processing operations' might constitute one and the same conduct. The term 'linked' refers to the principle that a unitary conduct might consist of several parts that are carried out by a unitary will and are contextually (in particular regarding identity in terms of data subject, purpose and nature), spatially and temporally related in such a close way that an outside observer would consider them as one coherent conduct."[167]

"However, if the circumstances of the case form one and the same conduct, but this conduct gives rise to not only one, but multiple infringements, it must be established whether the attribution of one infringement precludes attribution of another infringement or can they be attributed alongside each other."[168]

It has been recommended including a provision to the Guidelines that "takes account of breaches to the supply chain, and in such cases identify which party carries the larger share of responsibility. The nature of market, opinion and social research activities can result in supply chains which involve a number of different processors."[169]

"For example, activities such as translations, transcriptions, data processing, scripting, data collection, etc. are often outsourced and fieldwork is frequently outsourced to third-party sources. Presently the Guidelines do not cover details on shared liabilities, and the responsibility of said liabilities beyond the controller and processor."[170]

5.4. Concurrence of offences

"Concurrence occurs already on the abstract level of statutory provisions. This could either be on grounds of the principle of specialty, subsidiarity or consumption, which often apply where

0calculation%20of%20administrative%20fines%20under%20the%20GDPR%20-%20AFEP%20-%20June%202022.pdf (last visited 26 August 2022).

[167] EPDB, *op. cit.* (fn. 8), p. 11.

[168] *Ibid.*, p. 12.

[169] K. Kolawole and C. Gennaro, *EFAMRO ESOMAR Response to Consultation 422_EDPB*, p. 2, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/EFAMRO%20ESOMAR%20response%20to%20consultation%20422_EDPB.pdf (last visited 26 August 2022).

[170] *Ibid.*

provisions protect the same legal interest. In such cases, it would be unlawful to sanction the offender for the same wrongdoing twice."[171]

5.4.1. Principle of specialty

"The principle of specialty *(specialia generalibus derogant*) is a legal principle that means that more specific provision (derived from the same legal act or different legal acts of the same force) supersedes a more general provision, although both pursue the same objective. The more specific infringement then is sometimes considered a "qualified type" to the less specific one."[172]

Commentators asked for a specific example by EDPB of such cases. "The only example provided by EDPB is for the case where the objectives of the provisions are not congruent i.e., the data protection principles in Article 5 of the GDPR versus the provisions that are a concretization of such principle."[173]

Notably, "The Irish DPA(DPC) with its decision against WhatsApp IE of 20.08.2021[174] issued a separate fine for the infringement of the overarching transparency principle and separate fines for infringing Articles 13 and 14 information obligations (and other specific transparency obligations) towards users and non-users."[175]

"It was stated by the DPC that it is possible to find an infringement of transparency obligations independently from the infringement of transparency principle in light of the gravity and the overarching nature and impact of the infringements. It stems from the above reasoning that the DPC does not consider all violations of GDPR provisions that concretize data protection principles to be simultaneously finable violations of such principles."[176]

5.4.2. Principle of subsidiarity

[171] EPDB, *op. cit.* (fn. 8), p. 12.
[172] *Ibid.*, p. 13.
[173] Raphael, *op. cit.* (fn. 164), p. 3.
[174] GDPR Enforcement Tracker, *op. cit.* (fn. 16).
[175] Raphael, *op. cit.* (fn. 164), p. 3.
[176] *Ibid.*

"It applies where one infringement is considered subsidiary to another infringement. This could be either because the law formally declares subsidiarity or because subsidiarity is given for material reasons."[177]

5.4.2. Principle of consumption

"The principle of consumption applies in cases where the infringement of one provision regularly leads to the infringement of the other, often because one infringement is a preliminary step to the other."[178]The provisions in the Guidelines on specialty, subsidiary and consumption would "greatly benefit from more clarity and some more concrete examples of these concepts in the direct context of GDPR infringements."[179]

5.5. Starting point for calculation

"The identification of harmonized starting points in these Guidelines does not and should not preclude supervisory authorities from assessing each case on its merits. The fine imposed upon a controller/processor can range from any minimum fine until the legal maximum of the fine, provided that this fine is effective, dissuasive and proportionate. The existence of a starting point does not prevent the supervisory authority from lowering or increasing the fine (up to its maximum) if the circumstances of the case so require."[180]

It has been argued that "considering that Article 83 of GDPR does not set any categories or starting points for calculating fines, by setting such a starting point for the calculation of the fines, the Guidelines derogate from the provisions of the GDPR. The provisions of a non-binding document, such as the Guidelines, cannot derogate or add to the provisions of a Regulation."[181] Therefore, commentators proposed amending the Guidelines by "removing the paragraphs regarding the setting of starting points for calculation of the amount of fines."[182]

---

[177] EPDB, *op. cit.* (fn. 8), p. 13.
[178] *Ibid.*
[179] B. Bellamy, M. Heyder and N. Gerlach, *CIPL Response to the EDPB Guidelines 04 2022*, p. 5, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/CIPL%20Response%20to%20the%20EDPB%20Guidelines%2004%202022%20.pdf (last visited 26 August 2022).
[180] EPDB, *op. cit.* (fn. 8), p. 15.
[181] Foreign Investors Council, *op. cit.* (fn. 158), p. 3.
[182] *Ibid.*

Others have, maybe less harshly, pointed out that they "miss the legal basis of the minimum amount of fine concept newly introduced by the Guidelines where the minimum level of fine is derived primarily from the turnover of the breaching organization."[183] They also "consider such an approach lacking a legal basis in the GDPR to be rather controversial."[184]

Yet another commentator mentioned that "the focus on turnover contradicts the regulations and values of the GDPR, because it uses the turnover of the affected company as the upper limit, but not as the lower limit of the sanction."[185]

"The EDPB considers three elements to form the starting point for further calculation: the categorization of infringements by nature under Articles 83(4)–(6) GDPR, the seriousness of the infringement pursuant to Article 83(2) GDPR and the turnover of the undertaking as one relevant element to take into consideration with a view to imposing an effective, dissuasive and proportionate fine, pursuant to Article 83(1) GDPR."[186]

5.5.1. Categorization of infringements under Articles 83

"Essentially, there are two categories; those punishable under Article 83(4), and those punishable under Article 83(5) and (6). The first category is punishable by a fine maximum of 10 million or 2% of the undertaking's annual turnover, whichever is higher. The second category is punishable by a fine maximum of 20 million or 4% of the undertaking's annual turnover, whichever is higher.[187] With this distinction, the legislator provided a indication of the seriousness of the infringement."[188]

5.5.2. Nature, gravity and duration of the infringement

"The GDPR requires the supervisory authority to give due regard to the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing

[183] Rámiš, Selby and Nonnemann*op. cit.* (fn. 162), p. 2.
[184] *Ibid.*
[185] Weiß, *op. cit.* (fn. 163), p. 2.
[186] EPDB, *op. cit.* (fn. 8), p. 16.
[187] In other words, „any non-compliant activity has the potential to bankrupt a company."; Ziegler, Evequoz and Huamani, '*The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities*', in A. Aagaard (ed.), Digital Business Models (2019) 201 , p. 221.
[188] EPDB, *op. cit.* (fn. 8), p. 16.

concerned, as well as the number of data subjects affected and the level of damage suffered by them (Article 83(2)(a) GDPR)."[189]

5.5.2.1. The nature of the infringement

"The supervisory authority may review the interest that the infringed provision seeks to protect and the place of this provision in the data protection framework. In addition, the supervisory authority may consider the degree to which the infringement prohibited the effective application of the provision and the fulfilment of the objective it sought to protect."[190]

5.5.2.2. The gravity of the infringement

1. "The nature of the processing, including the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) and all the characteristics of the processing."[191]

   For some, the very nature of the activity (e.g. „business activity", „non-profit", „political party", etc.) should not play a significant role. "It is not clear, for example, why unauthorized processing should be evaluated more strictly (or otherwise), e.g. in the context of processing health data for research purpose carried out by entrepreneurs or non-profit organizations."[192] In their opinion, "the overall impact on the rights of data subjects should be more important and this distinction is also not supported by and goes beyond the text of GDPR."[193]

2. "The scope of the processing local, national or cross-border scope; The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor."[194]

   Commentators have argued against this, pointing out that "the GDPR supports the free movement of data within the EU, as an integral part and condition of the free movement of

[189] *Ibid.*
[190] *Ibid.*
[191] *Ibid.*, p. 17.
[192] Rámiš, Selby and Nonnemann, *op. cit.* (fn. 162), p. 2.
[193] *Ibid.*, p. 3.
[194] EPDB, *op. cit.* (fn. 8), p. 17.

goods, services and capital, so the indication of making cross-border processing an aggravating circumstance is contrary to both the GDPR and the basic principle of the European Union."[195] They consider "the implication that the reason for the stricter approach to cross-border processing is the difficulty on the part of supervisory authorities in investigating and sanctioning misconduct in such processing as very unfortunate especially when the GDPR contains a set of mechanisms designed to promote and unify cooperation between supervisory authorities across the European Union."[196]

3. "The purpose of the processing; The supervisory authority may also consider whether the purpose falls within the so-called core activities of the controller. The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be."[197] "Since it gives no example for this it would be desirable for the guidelines to clarify what is meant by "core business"."[198]The Guidelines though do give an example for "circumstances in which the processing of personal data is further removed from the core business, but significantly impacts the evaluation nonetheless (processing concerning personal data of workers where the infringement significantly affects those workers' dignity)."[199]

4. "The number of data subjects concretely but also potentially affected. The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor."[200]

   In this regard, some have asked "for more clarity for larger group of companies where a number of smaller entities belong to a parent company. In which relation should they stand (e. g. sharing a common IT infrastructure) in order the infringement within a smaller

[195] Rámiš, Selby and Nonnemann, *op. cit.* (fn. 162), p. 3.
[196] *Ibid.*
[197] EPDB, *op. cit.* (fn. 8), p. 17.
[198] Flament-Mascaret and Fontaine, *op. cit.* (fn. 166), p. 4.
[199] EPDB, *op. cit.* (fn. 8), p. 17.
[200] *Ibid.*

company to be considered as the one affecting the parent company and thus increasing the number of affected data subjects?"[201]

5. "The level of damage suffered and the extent to which the conduct may affect individual rights and freedoms. The level of damage suffered refers to physical, material or non-material damage."[202]

5.5.2.3. The duration of the infringement

"Meaning that a supervisory authority may generally attribute more weight to an infringement with longer duration."[203]

5.5.3. Intentional or negligent character of the infringement

"In case of an intentional infringement, the supervisory authority is likely to attribute more weight to this circumstance. Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral."[204]

Some have called for the EDPB to state "that 'negligence' shall be interpreted broadly in a way that it encompasses acts or omissions of the controller or processor that may not be negligent per se i.e., purely negligent but also those that may be the result of carelessness or, even, those that may not be intentional but are not negligent either. This may be the case of a controller or processor that exercised diligence and care to safeguard that the processing operations comply to the GDPR, however the interpretation or the application of the legislation or guidelines was considered by the supervisory authorities to be inappropriate or misguided."[205]

[201] E. Ostwald, *Statement Re. Draft to Guidelines_RWE SE*, p. 1, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Statement%20re.%20Draft%20to%20Guidelines_RWE%20SE.pdf (last visited 26 August 2022).
[202] EPDB, *op. cit.* (fn. 8), p. 18.
[203] *Ibid.*
[204] EPDB, *Ibid.*, p. 19.
[205] Raphael, *op. cit.* (fn. 164), p. 4.

Others ask at least that the Guidelines should "clearly state that any risk assessment performed by the controller in good faith in order to assess the risk and identify the measures necessary to mitigate that risk should not lead to being considered as an intentional infringement of the GDPR. This could be the case where the DPA disagrees with the analysis of the controller and decides to fine such controller where the risk analysis has led to breaching GDPR."[206]

5.5.4. Classifying the seriousness of the infringement and identifying the appropriate starting amount

"Based on the evaluation of already mentioned factors, the supervisory authority may find the infringement to be of a low, medium or high level of seriousness."[207]

Level of seriousness	Starting amount for further calculation
LOW	Between 0-10% of the applicable legal maximum
MEDIUM	Between 10-20% of the applicable legal maximum
HIGH	Between 20-100% of the applicable legal maximum

The Guidelines proceed to give an example for each level.[208]

Some critics don't see "where the 3 levels (low/medium/high) derive from and perceive such a concept to be too narrow to account for the variety of infringements."[209]

In the aforementioned examples, the Guidelines start the analysis by categorizing whether it is an infringement under Article 83(4) or 83(5) of GDPR which influenced the decision of classifying the infringement under low, medium or high level of seriousness. Commentators have pointed out that "the actual level of seriousness of an infringement and the level of damage (material or non-material) that is capable of inflicting on individuals is not necessarily lower for infringements

[206] Federation of European Data and Marketing, , p. 4, *FEDMA_Answer to EDPB Consultation_Guidelines on GDPR Fines*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/FEDMA_Answer%20to%20EDPB%20Consultation_Guidelines%20on%20GDPR%20fines.pdf (last visited 26 August 2022).
[207] EPDB, *op. cit.* (fn. 8), p. 19.
[208] *Ibid.*, p. 20,21,22.
[209] Weiß, *op. cit.* (fn. 163), p. 4.

under Article 83(4) of the GDPR in comparison to infringements under Article 83(5) of the GDPR."[210]

"For example, infringements relating to security of processing are listed in Article 83(4) and, therefore enjoy a lower legal maximum, however, such infringements can cause significant and grave damages to a significant number of individuals and society which may be greater than the damage inflicted when the controller omits to include in its privacy notice information on data retention, an infringement covered under Article 83(5) of the GDPR."[211]

For some, this "results in an unjustified discrimination between two controllers purely on the basis of when the supervisory authority imposed its fine – before or after finalization of the guidelines – as the controller fined before finalization of such Guidelines may be subject to a far more favourable fining approach than the one fined afterwards."[212]

5.6. Turnover of the undertaking with a view to imposing an effective, dissuasive and proportionate fine

Annual turnover of an undertaking	Basis of a sum down of the identified starting amount
≤€2m	0.20%
≤€10m	0.40%
≤€50m	2%
€50m-€100m	10%
€100m-€250m	20%
≥€250m	50%

[210] Raphael, *op. cit.* (fn. 164), p. 5.
[211] *Ibid.*
[212] K. Skogen Lund and A. Caulier, *European Tech Alliance - Response to the Public Consultation of the European Data Protection Board*, p. 3, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/European%20Tech%20Alliance%20-%20Response%20to%20the%20public%20consultation%20of%20the%20European%20Data%20Protection%20Board.pdf (last visited 26 August 2022).

"The supervisory authority is under no obligation to apply this adjustment if it is not necessary from the point of view of effectiveness, dissuasiveness and proportionality to adjust the starting amount of the fine."[213]"These turnover figures are inspired by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises."[214]

This decision by the Guidelines has been heavily criticized. Commentators say that the Guidelines "misinterpret the limitation on fines under Article 83 (4) and (5) of the GDPR not as the highest possible amount of the fine (upper limit), but as the upper limit of the usual interval in which the fine is to be imposed."[215]

Critics have also warned that "calculating the fine according to the model presented in the Guidelines can lead to disproportionate consequences for companies. Even minor violations can result in substantial fines due to the consideration of the worldwide group turnover."[216]In addition, "the direct link to the total turnover puts companies with high turnover but low profits at a disadvantage compared to industries with smaller turnover but high profits."[217]It would, for some commentators, "be much more appropriate to base the treatment on the values of cartel law, which are primarily based on the financial advantage achieved by an infringement."[218]

Further arguments against include the opinion that "the turnover of an undertaking cannot be regarded as an aggravating or a mitigating factor, due to the fact that an infringement of the fundamental right of natural persons regarding the protection of their personal data cannot be reasonably regarded as more or less serious, based on the pre-existing financial situation of the undertaking which violated such right."[219]

Some critics say that the Guidelines, in general, "over-emphasize the importance of the size and turnover of organizations when calculating fine levels. Worldwide turnover of the wider undertaking is not the appropriate starting point, and for them applying total turnover of the

[213] EPDB, *op. cit.* (fn. 8), p. 23.
[214] *Ibid.*
[215] Rámiš, Selby and Nonnemann, *op. cit.* (fn. 162), p. 2.
[216] Confederation of German Employers' Associations, *Opinion to the Guidelines for the Calculation of Fines*, p. 1, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Opinion%20to%20the%20Guidelines%20for%20the%20calculation%20of%20fines.pdf (last visited 26 August 2022).
[217] *Ibid.*
[218] *Ibid.*
[219] Foreign Investors Council, *op. cit.* (fn. 158), p. 2.

undertaking at the outset would be legally incorrect, as it would produce a disproportionate and excessive fine."[220]"Even in competition law, which was the inspiration for the GDPR fines, the turnover calculation is linked to the relevant market in line with proportionality considerations."[221]

5.7. Aggravating and mitigating circumstances

"The adoption of appropriate measures to mitigate the damage suffered by the data subjects may be considered a mitigating factor, decreasing the amount of the fine."[222]

"The measures adopted must be assessed, in particular, with regard to the element of timeliness, i.e. the time when they are implemented by the controller or processor, and their effectiveness. In that sense, measures spontaneously implemented prior to the commencement of the supervisory authority's investigation becoming known to the controller or processor are more likely to be considered a mitigating factor, than measures that have been implemented after that moment."[223]

"Only in exceptional circumstances, where the controller or processor has gone above and beyond the obligations imposed upon them, will this be considered a mitigating factor."[224]

Other critics argued that "asking the controller or processor to go 'above and beyond' what is required by the law is excessive. Instead, the final Guidelines could be changed to simply say that it is possible that compliance with Article 25 and 32 of GDPR can exceptionally constitute a mitigating circumstance."[225]

5.7.1. Previous infringements by the controller or processor

5.7.1.1. Time frame

[220] Weiß, *op. cit.* (fn. 163), p. 5.
[221] Bellamy, Heyder and Gerlach, *op. cit.* (fn. 179), p. 3.
[222] EPDB, *op. cit.* (fn. 8), p. 25.
[223] *Ibid.*
[224] *Ibid.*, p. 26.
[225] A. Di Felice and B. Ericson, *DIGITALEUROPE Response to the EDPB Consultation on the Draft Guidelines on the Calculation of Administrative Fines*, p. 3, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/DIGITALEUROPE%20response%20to%20the%20EDPB%20consultation%20on%20the%20draft%20Guidelines%20on%20the%20calculation%20of%20administrative%20fines.pdf (last visited 26 August 2022).

"According to Article 83(2)(e) GDPR, any relevant previous infringements committed by the controller or processor must be considered when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine."[226]

Critics say that to "take into account actions covered by a different legal framework would be contrary to the principle of nonretroactive application of law."[227]

5.7.2. Degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement

"Lack of cooperation may lead to the application of the fine provided for in Article 83(4)(a) GDPR. It should therefore be considered that the ordinary duty of cooperation is mandatory and should therefore be considered neutral (and not a mitigating factor)."[228]

"However, where cooperation with the supervisory authority has had the effect of limiting or avoiding negative consequences for the rights of the individuals that might otherwise have occurred, the supervisory authority may consider this a mitigating factor in the sense of Article 83(2)(f) GDPR, thereby decreasing the amount of the fine."[229]

"The EDPB refers to the socio-economic context in which the controller or processor operates, and the legal and market contexts as possible factors. Critics would like to add to that list the cessation or termination of the infringement as soon as the supervisory authority intervenes."[230]

"Whilst 'any action taken by the controller or processor to mitigate the damage suffered by data subjects' is already considered a mitigating factor as per Article 83(2)(c) in the sense that it repairs or compensates damage already caused, the mere cessation of the infringement is not. Granting mitigating effects to that action would align EDPB's guidance with bodies of administrative sanctions where such mitigation is contemplated."[231]

---

[226] EPDB, *op. cit.* (fn. 8), p. 26.
[227] Di Felice and Ericson, *op. cit.* (fn. 225), p. 5.
[228] EPDB, *op. cit.* (fn. 8), p. 28.
[229] *Ibid.*
[230] E. Velázquez, *We Are at Your Disposal for Any Questions.*, p. 1, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Final%20ACCIS%20Letter%20on%20Guidelines%2004%3A2022%20on%20the%20calculation%20of%20administrative%20fines%20under%20the%20GDPR.pdf.
[231] *Ibid.*

Other commentators have just asked for more clarity as to "how exactly the controllers and processors can achieve a mitigating factor."[232]

Other faultfinders think that "in the absence of clear guidelines on how to balance different fundamental rights, DPAs should acknowledge the complexity for companies to balance these different rights appropriately by considering the need to comply with other fundamental rights as a mitigating factor in the calculation of a fine."[233]

5.7.3. Adherence to approved codes of conduct or approved certification mechanisms

"Approved codes of conduct will, according to Article 40(4) GDPR, contain 'mechanisms which enable the (monitoring) body to carry out mandatory monitoring of compliance with its provisions.'"[234]

"Although the supervisory authority can take into account previously imposed sanctions pertaining to the self-regulatory scheme, the powers of the monitoring body are 'without prejudice to the tasks and powers of the competent supervisory authority', which means that the supervisory authority is not under an obligation to take into account any sanctions by the monitoring body."[235]

"On the other hand, if failure to comply with the codes of conduct or certification is directly relevant to the infringement, the supervisory authority may consider this an aggravating circumstance."[236]

It is the opinion of the critics that "adherence to codes of conduct as a mitigating factor and, where appropriate, payment of any sanctions imposed by the supervisory body set out in the Code should be taken into account by the competent supervisory authority." Differently, "one may be sanctioned several times for the same thing, and the essence of adherence to the Code as a

[232] Ostwald, *op. cit.* (fn. 201), p. 2.
[233] Federation of European Data and Marketing, *op. cit.* (fn. 206), p. 5.
[234] EPDB, *op. cit.* (fn. 8), p. 29.
[235] *Ibid.*
[236] *Ibid.*

compliance mechanism could be undermined, and also because the Code is also subject to approval by the supervisory authority."[237]

Yet again, some have just asked that references made to the legal benefits of codes of conduct are "made clearer and more detailed."[238] Others have pointed out that these provisions from the Guidelines would "undermine the incentive for codes of conduct and certification mechanisms as important tools for data protection compliance and accountability."[239]

"In light of the investments needed from both code owners and code signatories and to encourage the further adoption of code of conducts and other certified mechanisms", some commentators believe that "adherence to these tools should represent a constant mitigating factor."[240]

5.8. Determining an undertaking and corporate liability

Recital 150 GDPR states: "Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes."

"In line with settled CJEU case law the term undertaking in Articles 101 and 102 TFEU can refer to a single economic unit (SEU), even if that economic unit consists of several natural or legal persons. Whether several entities form a SEU depends largely on whether the individual entity is free in its decision-making ability or whether a leading entity, namely the parent company, exercises decisive influence over the others."[241]

However, it is the opinion of some commentators that "recital 150 contradicts the definitions in Article 4(18) and (19) of the GDPR and a Recital has no normative effect. The aforementioned definitions in Article 4, on the other hand, have binding effect. They distinguish between undertakings, groups of undertakings and groups of undertakings engaged in a joint economic

---

[237] *Comments on the Guidelines 04-2022*, p. 2, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Comments%20on%20the%20Guidelines%2004-2022..pdf (last visited 26 August 2022).
[238] J. Casella, *Guidelines 04/2022 on the Calculation of Administrative Fines*, p. 4, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Comments%20on%20Guidelines%2004%202022%20on%20the%20calculation%20of%20administrative%20fines.pdf.
[239] Bellamy, Heyder and Gerlach, *op. cit.* (fn. 179), p. 6.
[240] Kolawole and Gennaro, *op. cit.* (fn. 169), p. 3.
[241] EPDB, *op. cit.* (fn. 8), p. 34.

activity. Accordingly, the term 'undertaking', as distinct from the separately defined group of undertakings, would have to be seen in relation to the legal entity (that committed the infringement), i.e. the individual legal person."[242]

"In the specific case where a parent company holds 100% of shares or almost 100% of shares in a subsidiary which has infringed Article 83 GDPR and therefore is able to exercise decisive influence over the conduct of its subsidiary, a presumption arises that the parent company does in fact exercise this decisive influence over the conduct of its subsidiary (so-called Akzo[243] presumption)."[244]

"However, the Akzo presumption is not an absolute one, but can be rebutted by other evidence. In order to rebut the presumption, the company(ies) must provide evidence relating to the organizational, economic and legal links between the subsidiary and its parent company which are apt to demonstrate that they do not constitute a SEU despite holding 100% or almost 100% of shares."[245]

Critics find that "this makes it difficult for organizations with a large number of subsidiaries or with complex corporate/data protection structures to quantify the risk of being fined by the authorities for GDPR breaches in subsidiaries, over which the parent company does not have a decisive influence, especially for stock corporations."[246]

For some it is "not clear which kind of influence of the parent company is meant, e.g. if a smaller company makes its own decisions concerning privacy, data processing, etc., but in economic aspects stays under the influence and/or in strong cooperation with/of the parent company – would this company be considered as free in its decision making and will it be solely responsible for data protection infringements?"[247]

---

[242] R. Schön, *Stellungnahme Der WKÖ Amtssigniert*, p. 1, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Stellungnahme%20der%20WK%C3%96%20amtssigniert.pdf (last visited 26 August 2022).
[243] ECJ, *Akzo Nobel NV and Others v Commission of the European Communities*, Case C-97/08 P, 10 September 2009, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62008CJ0097 (last visited 20 September 2022).
[244] EPDB, *op. cit.* (fn. 8), p. 35.
[245] *Ibid.*
[246] Schön, *op. cit.* (fn. 242), p. 2.
[247] *Ibid.*

In this sense, critics argue, "it should be excluded the possibility of quantifying a sanction against a company only by virtue of an economic control by another company, which does not also translate into a control, by the parent company, over the data processing activities of the said company."[248]

"If the parent company does not hold all or almost all of the capital", the Guidelines proceed, "additional facts must be evidenced by the supervisory authority to justify the existence of a SEU."[249]

German commentators have found issue with the assumption that fines can be addressed directly to companies. "This is contrary to German administrative offenses law, for example, which does not require proof of a breach of supervisory duty by a company manager that has become causal for the data protection violation. This can be viewed critically, particularly since this has already been viewed in a differentiated manner by German courts."[250]

In addition, according to the Guidelines, "there is no possibility of exculpation for the responsible company if the data protection violation to be sanctioned is attributable to an employee who behaves contrary to existing and monitored conduct instructions."[251]

"In line with the SEU doctrine, Article 83(4)–(6) GDPR follow the principle of direct corporate liability, which entails that all acts performed or neglected by natural persons authorized to act on behalf of undertakings are attributable to the latter and are considered as an act and infringement directly committed by the undertaking itself."[252]Commentators concluded from that paragraph that

[248] *Comments Guidelines in Consultation 270622*, p. 3, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/comments%20guidelines%20in%20consultation%20270622.pdf (last visited 26 August 2022).
[249] EPDB, *op. cit.* (fn. 8), p. 35.
[250] D. Pfau, *Statement BVDW Guidelines 042022 on the Calculation of Administrative Fines under the GDPR*, p. 2, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/statement%20BVDW%20Guidelines%2004%3A2022%20on%20the%20calculation%20of%20administrative%20fines%20under%20the%20GDPR.pdf (last visited 26 August 2022).
[251] Confederation of German Employers' Associations, *op. cit.* (fn. 216), p. 2.
[252] EPDB, *op. cit.* (fn. 8), p. 35.

"neither the members of the management board nor the data protection officers are liable for the data protection violations of an undertaking under Article 83 GDPR."[253]

"The question of the prerequisites for corporate liability in the event of violations of the GDPR is currently the subject of ongoing proceedings before the European Court of Justice (ECJ, Case C-807/21)."[254]

The Higher Regional Court Berlin (KG Berlin) referred the following questions:

"1) Is Article 83(4) to (6) of the GDPR to be interpreted as incorporating into national law the functional concept of an undertaking and the principle of an economic entity, as defined in Articles 101 and 102 TFEU, as a result of which, by broadening the principle of a legal entity underpinning Paragraph 30 of the Gesetz über Ordnungswidrigkeiten (Law on administrative offences; 'the OWiG'), proceedings for an administrative fine may be brought against an undertaking directly and a fine imposed without requiring a finding that a natural and identified person committed an administrative offence, if necessary, in satisfaction of the objective and subjective elements of tortious liability?"[255]

"2) If Question 1 is answered in the affirmative: Is Article 83(4) to (6) of the GDPR to be interpreted as meaning that the undertaking must have intentionally or negligently committed the breach of an obligation vicariously through an employee (see Article 23 of Council Regulation (EC) No 1/2003 1), or is the objective fact of breach caused by it sufficient, in principle, for a fine to be imposed on that undertaking ('strict liability')?"[256]

[253] Dacuro GmbH, *Dacuro GmbH's Comments to Draft EDPB 042022 Guidelines*, p. 2, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/dacuro%20GmbH%27s%20comments%20to%20draft%20EDPB%20042022%20Guidelines.pdf (last visited 26 August 2022).
[254] Confederation of German Employers' Associations, *op. cit.* (fn. 216), p. 2.
[255] *CJEU - C-807/21 - Deutsche Wohnen SE*, GDPRhub, available at https://gdprhub.eu/index.php?title=CJEU_-_C-807/21_-_Deutsche_Wohnen_SE (last visited 27 August 2022).
[256] *Ibid.*

Some other commentators though, find that "direct corporate liability principle is consistent with antitrust law and follows the general tradition of EU law on sanctions that have been already established by other EU legal acts."[257]

5.9. Other suggestions

There have been a number of suggestions by the commentators that had no clear connection to the previous chapter of this work, but that its writer still found worthwhile to mention.

One commentator suggested the Guidelines should "identify, for consistency with the other Authorities, a common appeal frame and process for appealing final decisions."[258]

Many have pointed out that the possibility of issuing a reprimand (Article 58 (2) (b) and Recital 148 GDPR) should also be addressed[259]. Without it, to some critics it seemed as if "imposing fines was the main purpose of the GDPR and the only enforcement tool provided to the supervisory authorities without primarily considering the impact of the non-compliance into the rights and freedoms of individuals."[260]Their reasoning is that the "goal of data protection, which is the strengthening of the informational self-determination of individuals and the protection from misuse of their personal data, would be contradicted if remedial measures were to become irrelevant if a fine were to be imposed at the end of every contact with a supervisory authority anyways."[261]Further adding that, "from the point of view of the protection of the rights of individual data subjects, the application of other corrective powers can in many cases be a far more effective measure than solely imposing a fine."[262]

A real life example for the aforementioned measures from is "the decision of the Belgian personal data protection authority ordering the Interactive Advertising Bureau Europe -IAB-, an

[257] D. Gattullo, *Insurance Europe Comments on EDPB Guidelines on Calculation of Administrative Fines under GDPR*, p. 1, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Insurance%20Europe%20Comments%20on%20EDPB%20Guidelines%20on%20Calculation%20of%20Administrative%20Fines%20under%20GDPR.pdf (last visited 26 August 2022).
[258] A. Lombardi, *Wind Tre S.p.A. - Antongiulio Lombardi PUBLIC CONSULTATION_0*, p. 3, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Wind%20Tre%20S.p.A.%20-%20Antongiulio%20Lombardi%20PUBLIC%20CONSULTATION_0.pdf (last visited 26 August 2022).
[259] Schön, *op. cit.* (fn. 242), p. 1.
[260] Rámiš, Selby and Nonnemann, *op. cit.* (fn. 162), p. 1.
[261] Pfau, *op. cit.* (fn. 250), p. 2.
[262] Rámiš, Selby and Nonnemann, *op. cit.* (fn. 162), p. 2.

organization representing stakeholders in Internet advertising, to submit an action plan within a specific timeframe in order to remedy the shortcomings observed in the Transparency and Consent Framework -TCF, a tool used to record the consent of Internet users."[263]

Some critics stress the need to harmonize and increase the transparency about the DPAs enforcement activities and the way the EDPB's methodology will be applied. In their view, "enhanced publicity and transparency about imposed fines will strengthen their deterrent effect which will be otherwise limited since there will be no signals of the cost of non-compliance."[264]

Providing additional information on the fines "can also have an educational effect and lead to changes in behaviour." Therefore, they especially criticize that the Guidelines emphasize that "DPAs are not obliged to provide reasoning surrounding aspects of the Guidelines that are not applicable[265]"[266]

For some commentators, "it is not sufficiently emphasized that the Guidelines can help to have a detail theoretical scheme but - in concrete - it will be always upon the discretion of the supervisory authority involved in the specific case to assess the real scenario."[267]

In the comments, there was concern that, "since even a minor mistake could result in a high fine for the employer, it will burden employees and jeopardize the working atmosphere."[268]

Within the insurance sector, there was a possible problem with determining the turnover of insurance companies. Commentators ask that "in accordance with international accounting standards (especially IFRS 17 Insurance Contracts) and to ensure comparability and a level playing field with other sectors, when determining the turnover of insurance companies, amounts the insurer is obligated to repay to a policyholder regardless of whether an insured event occurs (so-called 'investment component') should always be excluded."[269]

---

[263] Flament-Mascaret and Fontaine, *op. cit.* (fn. 166), p. 1.
[264] Federation of European Data and Marketing, *op. cit.* (fn. 206), p. 6.
[265] EPDB, *op. cit.* (fn. 8), p. 6.
[266] Federation of European Data and Marketing, *op. cit.* (fn. 206), p. 2.
[267] M. Constantini, *Public Consultation 04 2022 - Marco Costantini DPO Comments*, p. 2, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Public%20Consultation%2004%202022%20-%20Marco%20Costantini%20DPO%20comments.pdf (last visited 26 August 2022).
[268] Confederation of German Employers' Associations, *op. cit.* (fn. 216), p. 2.
[269] German Insurance Association, *220627_GDV_comment_on_EDPB_guidelines_04-2022_final*, p. 2, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/220627_GDV_comment_on_EDPB_guidelines_04-2022_final.pdf (last visited 26 August 2022).

6. Croatian DPA – AZOP

This work will further elaborate on the activity of the Croatian DPA (Agencija za zaštitu osobnih podataka). In 2019, AZOP issued no fines.[270] In 2020[271], there was only one, issued to a bank because it refused to provide its customers with copies of credit documentation[272] (insufficient fulfilment of data subjects rights).

In its annual report for 2021[273], AZOP states that four fines were issued in that year, even though GDPR Enforcement Tracker acknowledges only three, all with unknown amounts. This is mentioned simply as a reminder to the incompleteness of online databases. According to the report, two of them were issued for violating Article 27(1) of Croatian General Data Protection Regulation Application Act which regulates insufficient fulfillment of information obligations in relation to CCTV. First one amounted to around 3 318 € and the other to 4 645 €. The other two fines of 2021 were issued for insufficient technical and organizational measures to ensure information security and resulted in higher, 5 digits fines (30 526 €[274], 64 702 €). The biggest fine of the year was issued when an employee of the security company recorded the video surveillance footage with a phone and shared it with a third party. The recording was ultimately made available on social media and in the media.[275]

The biggest fine by AZOP so far was issued in 2022 and amounted to 285 000 €, for the same type of violation. A telecommunications company was hacked and attackers had managed to access data from about 100,000 data subjects. AZOP found that such a breach was facilitated by the company's failure to implement adequate technical and organizational security measures for the processing of personal data.[276] According to GDPR Enforcement Tracker, there were 3 more

[270] AZOP, *Annual Report for 2019*, available at https://azop.hr/wp-content/uploads/2021/06/GODISNJE_IZVJESCE_AZOP_2019.pdf.
[271] AZOP, *Annual Report for 2020*, p. 50, available at https://azop.hr/wp-content/uploads/2022/07/GODISNJE_IZVJESCE_AZOP_2020.pdf.
[272] https://www.enforcementtracker.com/ETid-239 (last visited 24 January 2023).
[273] AZOP, *Annual Report for 2021*, p. 47, available at https://azop.hr/wp-content/uploads/2022/07/GODISNJE_IZVJESCE_AZOP_2021.pdf.
[274] https://www.enforcementtracker.com/ETid-745 (last visited 24 January 2023).
[275] https://www.enforcementtracker.com/ETid-566 (last visited 24 January 2023).
[276] https://www.enforcementtracker.com/ETid-1293 (last visited 24 January 2023).

fines issued in 2022, in amounts of 124 245[277], 89 250[278] and 4 000 €[279]. This shows a significant increase in amounts of fines from recent years. Annual report for 2022 hasn't been published yet, but according to AZOP's website, it has issued at least 10 more fines in 2022.[280] They were all issued for violating Article 27 of the aforementioned Croatian General Data Protection Regulation Application Act. All combined, they amounted to 24 686 €, thus averaging 2 468 € a fine. This amount is compliant with Article 51 which, for violations of Article 27, establishes fines up to 6 636 €. Comparing these amounts to similar fines issued by other DPAs, they are about average. For example, fines by the Spanish DPA for violations in relation to CCTV ranged between 500 and 6 000 €[281].

7. Conclusion

Since 2018, the number of GDPR fines keeps steadily growing. Their severity has mostly increased, fines from 2021 against "Big Tech" being overshadowed by 2022 fines. Top violations are insufficient legal basis for data processing, non-compliance with general data processing principles and insufficient technical and organizational measures to ensure information security. The most active in the activity of issuing fines is Spain, but its DPA is not too harsh with the amount. Italian DPA, on the other hand is both active, being bested only by Spain, but with a significant lead on the sum gathered. Special case is Luxembourg DPA with a single fine, that since it has been issued, stands as the highest fine ever at 746 00 000 € but with a very low number of other fines. Ireland DPA has issued over 850 000 000 € worth of fines to "Big Tech", which is especially interesting considering that a lot of tech companies choose Ireland to be their European headquarters because of, among other reasons, its low corporate tax[282]. France's DPA has also joined that fight, their main culprits being Facebook and Google. "Media, Telecoms and Broadcasting" is the sector that suffered the most by fines, which isn't shocking seeing as the

[277] https://www.enforcementtracker.com/ETid-1092 (last visited 24 January 2023).
[278] https://www.enforcementtracker.com/ETid-1093 (last visited 24 January 2023).
[279] https://www.enforcementtracker.com/ETid-1292 (last visited 24 January 2023).
[280] A. Mladinić, *Izrečeno novih 10 upravnih novčanih kazni*, 22 December 2022, Agencija za zaštitu osobnih podataka, available at https://azop.hr/izreceno-novih-10-upravnih-novcanih-kazni/ (last visited 24 January 2023).
[281] See 4.2. „Accommodation & Hospitality", p. 18.
[282] A. Levy, *Why Silicon Valley Likes Ireland so Much*, CNBC, available at https://www.cnbc.com/2016/08/31/why-silicon-valley-followed-apple-to-ireland-eventually.html (last visited 15 December 2022).

aforementioned fines against tech companies belong to this sector. The nature of this sector potentially allows for the most profitable breaking of GDPR, since it involves easy acquiring and selling data to marketers. “Industry and Commerce” follows, with most fines but whose amount is mostly so high because of the aforementioned 746 000 000 € fine by the Luxembourg DPA.

EDPB has published the “Guidelines on the calculation of administrative fines under the GDPR” which has proven to be quite controversial. Notably, the introduction of starting points of fines has been extensively criticized, as it hasn’t been mentioned by the GDPR. Using the undertaking’s global turnover in the calculation has also caused many to ask for more clarity and wonder about the real goals of GDPR in relation to imposing fines. Mitigating circumstances were often mentioned by the critics, mostly because of the opinion that there are too little. Codes of conduct seem to be a lot less important to the EPDB than to the commentators, failure to comply with them being only a possible aggravating circumstance. The Guidelines are not as of yet final, and it will be very interesting to see what will change, and what will not.

With more fines, more explanation from DPAs and guidelines, fines imposed under GDPR can be expected to get more harmonized in future years. An important part of this effort is led by online databases, such as GDPR enforcement tracker, which has been extensively used in the writing of this work.

8. References

a) Books and articles

AZOP, *Annual Report for 2019*, available at https://azop.hr/wp-content/uploads/2021/06/GODISNJE_IZVJESCE_AZOP_2019.pdf.

AZOP, *Annual Report for 2020*, available at https://azop.hr/wp-content/uploads/2022/07/GODISNJE_IZVJESCE_AZOP_2020.pdf.

AZOP, *Annual Report for 2021*, available at https://azop.hr/wp-content/uploads/2022/07/GODISNJE_IZVJESCE_AZOP_2021.pdf.

Bradford, Aboy, and Liddell, '*COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes*', 7 Journal of Law and the Biosciences (2020), available at https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsaa034/5848138 (last visited 14 September 2022).

Burgess, J.P., Floridi, L., Pols, A. and van Den Hoven, J., 2018. Towards a Digital Ethics: EDPS Ethics Advisory Group., available at https://philpapers.org/archive/BURTAD-3.pdf (last visited 14 September 2022).

Cavus and Sekyere-Asiedu, '*A Comparison of Online Video Conference Platforms: Their Contributions to Education during COVID-19 Pandemic*', 13 World Journal on Educational Technology: Current Issues (2021) 1180, available at https://un-pub.eu/ojs/index.php/wjet/article/view/6329 (last visited 13 September 2022).

Floridi, '*Soft Ethics, the Governance of the Digital and the General Data Protection Regulation*', 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences (2018) 20180081, available at https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0081 (last visited 14 September 2022).

Forcier et al., '*Integrating Artificial Intelligence into Health Care through Data Access: Can the GDPR Act as a Beacon for Policymakers?*', 6 Journal of Law and the Biosciences (2019) 317, available at https://academic.oup.com/jlb/article/6/1/317/5570026 (last visited 20 January 2023)

Golla, '*Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR*', 8 2017, p. 71.

'*Google Is First Company Hit with Major GDPR Fine*', 2019 Computer Fraud & Security (2019) 1, available at http://www.magonlinelibrary.com/doi/10.1016/S1361-3723%2819%2930013-2

Houser, Kimberly and Voss, W. Gregory, GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? (July 11, 2018). Working Paper, 25 Rich. J. L. & Tech. 1, 2018 Forthcoming, Available at SSRN: https://ssrn.com/abstract=3212210

Joint Webinar - Beyond the Exit Strategy: Ethical Uses of Data-Driven Technology in the Fight against COVID-19, The Nuffield Council on Bioethics, available at https://www.nuffieldbioethics.org/news/joint-webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19 (last visited 14 September 2022).

Larrucea et al., '*Towards a GDPR Compliant Way to Secure European Cross Border Healthcare Industry 4.0*', 69 Computer Standards & Interfaces (2020) 103408, available at https://linkinghub.elsevier.com/retrieve/pii/S0920548919304544 (last visited 13 September 2022).

Liapakis, '*A GDPR Implementation Guide for the Insurance Industry:*', 7 International Journal of Reliable and Quality E-Healthcare (2018) 34, available at http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJRQEH.2018100103 (last visited 13 September 2022).

Lombarte, '*The Spanish Experience of Enforcing Privacy Norms: Two Decades of Evolution from Sticks to Carrots*', in D. Wright and P. De Hert (eds.), Enforcing Privacy vol. 25 (2016) 123

Luciano, '*Mind the App—Considerations on the Ethical Risks of COVID-19 Apps*', 33 Philosophy & Technology (2020) 167, available at https://link.springer.com/10.1007/s13347-020-00408-5 (last visited 14 September 2022).

N. Parlov, Ž. Sičaja, T. Katulić i R. Luša, "Information security and the lawful interception of communications through telecom service providers infrastructure: advanced model system architecture", *Policija i sigurnost*, vol.30, br. 1/2021, str. 112-130, 2021

Ouwerkerk, '*Beware of GDPR - Take Your Cyber Risk Responsibility More Seriously*', in The InsurTech Book (2018) 175.

Shu, Jahankhani, '*The Impact of the New European General Data Protection Regulation (GDPR) on the Information Governance Toolkit in Health and Social Care with Special Reference to Primary Care in England*', in 2017 Cybersecurity and Cyberforensics Conference (CCC) (2017) 31.

Stan, Miclea, '*New Era for Technology in Healthcare Powered by GDPR and Blockchain*', in S. Vlad and N. M. Roman (eds.), 6th International Conference on Advancements of Medicine and Health Care through Technology; 17–20 October 2018, Cluj-Napoca, Romania vol. 71 (2019) 311.

T. Katulić and N. Protrka, "Information Security in Principles and Provisions of the EU Data Protection Law," *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2019, pp. 1219-1225

T. Katulić, "Towards the Trustworthy AI: Insights from the Regulations on Data Protection and Information Security", *Medijska istraživanja*, vol.26, br. 2, str. 9-28, 2020

Vojković, Milenković and Katulić, '*IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law*', 11 Business Systems Research Journal (2020) 167, available at https://www.sciendo.com/article/10.2478/bsrj-2020-0033

Ziegler, Evequoz and Huamani, '*The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities*', in A. Aagaard (ed.), Digital Business Models (2019) 201

b) Web Sources

A. Mladinić, Izrečeno novih 10 upravnih novčanih kazni, 22 December 2022, Agencija za zaštitu osobnih podataka, available at https://azop.hr/izreceno-novih-10-upravnih-novcanih-kazni/ (last visited 24 January 2023).

Agencia Española de Protección de Datos | AEPD, available at https://www.aepd.es/es (last visited 5 December 2022).

Bellamy B., Heyder M. and Gerlach N., *CIPL Response to the EDPB Guidelines 04 2022*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/CIPL%20Response%20to%20the%20EDPB%20Guidelines%2004%202022%20.pdf (last visited 26 August 2022).

Casella J., *Guidelines 04/2022 on the Calculation of Administrative Fines*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Comments%20on%20Guidelines%2004%202022%20on%20the%20calculation%20of%20administrative%20fines.pdf.

Comments Guidelines in Consultation 270622, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/comments%20guidelines%20in%20consultation%20270622.pdf (last visited 26 August 2022).

Comments on the Guidelines 04-2022, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Comments%20on%20the%20Guidelines%2004-2022..pdf (last visited 26 August 2022).

Confederation of German Employers' Associations, *Opinion to the Guidelines for the Calculation of Fines*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Opinion%20to%20the%20Guidelines%20for%20the%20calculation%20of%20fines.pdf (last visited 26 August 2022).

Constantini M., *Public Consultation 04 2022 - Marco Costantini DPO Comments*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Public%20Consultation%2004%202022%20-%20Marco%20Costantini%20DPO%20comments.pdf (last visited 26 August 2022).

COVID-19 Apps, Wikipedia24 August 2022, available at https://en.wikipedia.org/w/index.php?title=COVID-19_apps&oldid=1106470205 (last visited 14 September 2022).

Dacuro GmbH, *Dacuro GmbH's Comments to Draft EDPB 042022 Guidelines*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/dacuro%20GmbH%27s%20comments%20to%20draft%20EDPB%20042022%20Guidelines.pdf (last visited 26 August 2022).

Di Felice A. and Ericson B., *DIGITALEUROPE Response to the EDPB Consultation on the Draft Guidelines on the Calculation of Administrative Fines*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/DIGITALEUROPE%20response%20to%20the%20EDPB%20consultation%20on%20the%20draft%20Guidelines%20on%20the%20calculation%20of%20administrative%20fines.pdf (last visited 26 August 2022).

Federation of European Data and Marketing, *FEDMA_Answer to EDPB Consultation_Guidelines on GDPR Fines*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/FEDMA_Answer%20to%20EDPB%20Consultation_Guidelines%20on%20GDPR%20fines.pdf (last visited 26 August 2022).

Flament-Mascaret E. and Fontaine A., *EDPB Guidelines on the Calculation of Administrative Fines under the GDPR - AFEP - June 2022*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/EDPB%20guidelines%20on%20the%20calculation%20of%20administrative%20fines%20under%20the%20GDPR%20-%20AFEP%20-%20June%202022.pdf (last visited 26 August 2022).

Floridi, '*Soft Ethics, the Governance of the Digital and the General Data Protection Regulation*', 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences (2018) 20180081, available at https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0081 (last visited 14 September 2022).

Foreign Investors Council, *FIC Position on EDPB Guidelines 4.2022*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/FIC%20Position%20on%20EDPB%20Guidelines%204.2022.pdf (last visited 26 August 2022).

Gattullo D., *Insurance Europe Comments on EDPB Guidelines on Calculation of Administrative Fines under GDPR*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Insurance%20Europe%20Comments%20on%20EDPB%20Guidelines%20on%20Calculation%20of%20Administrative%20Fines%20under%20GDPR.pdf (last visited 26 August 2022).

German Insurance Association, *220627_GDV_comment_on_EDPB_guidelines_04-2022_final*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/220627_GDV_comment_on_EDPB_guidelines_04-2022_final.pdf (last visited 26 August 2022).

Helena, *Dash Cams around the World*, 26 August 2020, VIA Technologies, Inc., available at https://www.viatech.com/en/2020/08/dash-cams-around-the-world/ (last visited 13 September 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/methodology-and-contacts (last visited 19 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/executive-summary (last visited 19 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/finance-insurance-and-consulting (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/accommodation-and-hospitality (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/health-care (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/industry-and-commerce (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/real-estate (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/media-telecoms-and-broadcasting (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/public-sector-and-education (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/transportation-and-energy (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/individuals-and-private-associations (last visited 7 December 2022).

https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/employment (last visited 9 December 2022).

https://cms.law/en/int/about-cms/about-us (last visited 19 December 2022).

https://cnpd.public.lu/en.html (last visited 5 December 2022).

https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub (last visited 19 December 2022).

https://ico.org.uk/ (last visited 8 December 2022).

https://vdai.lrv.lt/en/ (last visited 8 December 2022).

https://www.autoriteitpersoonsgegevens.nl/en (last visited 5 December 2022).

https://www.enforcementtracker.com/ (last visited 19 December 2022).

https://www.enforcementtracker.com/?insights (last visited 8 December 2022).

https://www.enforcementtracker.com/ETid-1005 (last visited 5 December 2022).

https://www.enforcementtracker.com/ETid-1092 (last visited 24 January 2023).
https://www.enforcementtracker.com/ETid-1093 (last visited 24 January 2023).
https://www.enforcementtracker.com/ETid-1292 (last visited 24 January 2023).
https://www.enforcementtracker.com/ETid-1293 (last visited 24 January 2023).
https://www.enforcementtracker.com/ETid-1373 (last visited 8 December 2022).
https://www.enforcementtracker.com/ETid-1502 (last visited 8 December 2022).
https://www.enforcementtracker.com/ETid-189 (last visited 9 December 2022).
https://www.enforcementtracker.com/ETid-218 (last visited 5 December 2022).
https://www.enforcementtracker.com/ETid-23 (last visited 9 December 2022).
https://www.enforcementtracker.com/ETid-239 (last visited 24 January 2023).
https://www.enforcementtracker.com/ETid-24 (last visited 7 December 2022).
https://www.enforcementtracker.com/ETid-384 (last visited 5 December 2022).
https://www.enforcementtracker.com/ETid-405 (last visited 10 December 2022).
https://www.enforcementtracker.com/ETid-522 (last visited 5 December 2022).
https://www.enforcementtracker.com/ETid-566 (last visited 24 January 2023).
https://www.enforcementtracker.com/ETid-571 (last visited 5 December 2022).
https://www.enforcementtracker.com/ETid-58 (last visited 5 December 2022).
https://www.enforcementtracker.com/ETid-60 (last visited 5 December 2022).
https://www.enforcementtracker.com/ETid-718 (last visited 10 December 2022).
https://www.enforcementtracker.com/ETid-719 (last visited 10 December 2022).
https://www.enforcementtracker.com/ETid-745 (last visited 24 January 2023).
https://www.enforcementtracker.com/ETid-747 (last visited 10 December 2022).
https://www.enforcementtracker.com/ETid-778 (last visited 8 December 2022).
https://www.enforcementtracker.com/ETid-820 (last visited 9 December 2022).
https://www.enforcementtracker.com/ETid-876 (last visited 5 December 2022).
https://www.enforcementtracker.com/ETid-946 (last visited 5 December 2022).
https://www.enforcementtracker.com/ETid-978 (last visited 9 December 2022).
https://www.enforcementtracker.com/ETid-979 (last visited 9 December 2022).
https://www.enforcementtracker.com/ETid-980 (last visited 9 December 2022).
https://www.top10vpn.com/research/covid-19-digital-rights-tracker/ (last visited 14 September 2022).

Kolawole K. and Gennaro C., *EFAMRO ESOMAR Response to Consultation 422_EDPB*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/EFAMRO%20ESOMAR%20response%20to%20consultation%20422_EDPB.pdf (last visited 26 August 2022).

Larrucea et al., '*Towards a GDPR Compliant Way to Secure European Cross Border Healthcare Industry 4.0*', 69 Computer Standards & Interfaces (2020) 103408, available at https://linkinghub.elsevier.com/retrieve/pii/S0920548919304544 (last visited 13 September 2022).

Levy A., *Why Silicon Valley Likes Ireland so Much*, CNBC, available at https://www.cnbc.com/2016/08/31/why-silicon-valley-followed-apple-to-ireland-eventually.html (last visited 15 December 2022).

Lombardi A., *Wind Tre S.p.A. - Antongiulio Lombardi PUBLIC CONSULTATION_0*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Wind%20Tre%20S.p.A.%20-%20Antongiulio%20Lombardi%20PUBLIC%20CONSULTATION_0.pdf (last visited 26 August 2022).

Lorenz, '*'Zoombombing': When Video Conferences Go Wrong*', The New York Times (2020) , available at https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html (last visited 8 December 2022).

Ostwald E., *Statement Re. Draft to Guidelines_RWE SE*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Statement%20re.%20Draft%20to%20Guidelines_RWE%20SE.pdf (last visited 26 August 2022).

Pfau D., *Statement BVDW Guidelines 042022 on the Calculation of Administrative Fines under the GDPR*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/statement%20BVDW%20Guidelines%2004%3A2022%20on%20the%20calculation%20of%20administrative%20fines%20under%20the%20GDPR.pdf (last visited 26 August 2022).

Rámiš V., Selby A. and Nonnemann F., *2022_06_27_SpOOU_EDPB_Guidelines_calculations_fines (EN)_final*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2022_06_27_SpOOU_EDPB_Guidelines_calculations_fines%20%28EN%29_final.pdf (last visited 26 August 2022).

Raphael M., *CEN-CLC JTC 13 WG5 Consultation Task Force Feedback on EDPB Guidelines 042022 on the Calculation of Administrative Fines under the GDPR*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/CEN-CLC%20JTC%2013%20WG5%20Consultation%20Task%20force%20feedback%20on%20EDPB%20Guidelines%20042022%20on%20the%20calculation%20of%20administrative%20fines%20under%20the%20GDPR.pdf (last visited 26 August 2022).

Schön R., *Stellungnahme Der WKÖ Amtssigniert*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Stellungnahme%20der%20WK%C3%96%20amtssigniert.pdf (last visited 26 August 2022).

Skogen Lund K. and Caulier A., *European Tech Alliance - Response to the Public Consultation of the European Data Protection Board*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/European%20Tech%20Alliance%20-

%20Response%20to%20the%20public%20consultation%20of%20the%20European%20Data%20Protection%20Board.pdf (last visited 26 August 2022).

Velázquez E., *We Are at Your Disposal for Any Questions.*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Final%20ACCIS%20Letter%20on%20Guidelines%2004%3A2022%20on%20the%20calculation%20of%20administrative%20fines%20under%20the%20GDPR.pdf.

Weiß R., *20220627_Bitkom Position Paper Administrative Fines GDPR*, available at https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/20220627_Bitkom%20Position%20Paper%20administrative%20fines%20GDPR.pdf (last visited 26 August 2022).

c) Regulations and judgments

CJEU - C-807/21 - Deutsche Wohnen SE, GDPRhub, available at https://gdprhub.eu/index.php?title=CJEU_-_C-807/21_-_Deutsche_Wohnen_SE (last visited 27 August 2022).

Council of Europe, European Convention of Human Rights, CETS NO. 005, 1950.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal dana and on the free movement of such data, OJ 1995 L 281.

ECJ, *Akzo Nobel NV and Others v Commission of the European Communities*, Case C-97/08 P , 10 September 2009, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62008CJ0097 (last visited 20 September 2022).

EU, Charter of Fundamental Rights of the European Union, OJ 2012 C 326.

EU, Consolidated version of the Treaty of the Functioning of the European Union, OJ 2012 C 326

Guidelines 04/2022 on the Calculation of Administrative Fines under the GDPR, version 1.0, available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en (hereinafter referred to as "Guidelines")

Guidelines on the Application and Setting of Administrative Fines for the Purpose of the Regulation 2016/679, WP253 (Hereinafter Referred to as "Guidelines WP253").

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); (hereinafter referred to as GDPR).

United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948

Zakon o Provedbi Opće Uredbe o Zaštiti Podataka, NN 42/2018, available at https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html (last visited 10 December 2022).