

ANNUAL REPORT ON PRIVACY FINES 2022



ABOUT TSAARO

At Tsaaro, we empower businesses to manage their compliance with data privacy and cybersecurity regulations. We provide data privacy and protection services to help organisations meet legislative, regulatory, contractual and business requirements, while maintaining a robust security infrastructure.

Our Mission is to assist businesses in achieving this by fervently committing to safeguarding the individuals who are the sources of the data. Our industry-standard privacy services include Privacy compliance programmes, DPO-as-a-service, EU Representative-as-a-service, Vulnerability Assessment & Penetration Testing, Cyber Strategy, DPIA to name a few, delivered by our expert privacy professionals recognised by IAPP.

Our objective is to increase the number of data privacy specialists in order to close the global talent gap, replacing the need for expensive consultants or recruiting in-house experts. We want to fill this gap in the market for global data privacy by establishing a global network of privacy experts who can assist organizations in the development of trust, risk mitigation, and revenue growth.

A one-stop solution for all Data Privacy and Cybersecurity Services, Tsaaro has partnered with Top Privacy Solution Implementation Companies like OneTurst, BigId, IAPP, and Arculus Labs. Partnerships with them enable us to implement best in class Privacy Solutions, catering to our clients specific requirements.



FOREWORD

The advancement of technology has increased the quality of life, but it has also led to corporations having large datasets about their consumers – who are people like us. This has put such corporations in a unique position where they would know more about us than we would know about ourselves. To prevent the misuse of such data, various Data Protection Authorities in the EU have started awarding fines that goes up to several hundreds of millions of Euros. To look at such fines individually would create a tunnel vision and impede our understanding of the importance of the GDPR and can falsely create an image where privacy compliance remains a worry for larger corporations.

The Privacy Fines Report 2022, the first of its kind, adopts a bird's eye view of privacy fines and analyses them as a whole. The fines on privacy not only seek to rectify wrongs committed, but also set a precedence for corporations as it depicts that privacy breaches are not to be taken lightly and non-compliance would put them in hot water with the authorities. As consumers, it is important to be acquainted from time to time with the facts and realities of the rapidly developing world which is taking place at the expense of personal data – a fact that is often hidden in plain sight.

Tsaaro Solutions is proud to present its first annual Report on Privacy Fines (2022) which aims at being informational not just to consumers, but also to the corporations to whom the compliance measures of GDPR would apply.

Akarsh Singh

CEO & Co-Founder

Tsaaro





TABLE OF CONTENTS

1	Introduction & Scope	8	Most Frequently Violated Articles
2	Fines & Penalties under GDPR	9	Summary of Findings
3	Key Findings	10	Suggestions
4	Top Penalties of 2022	11	Spotlight on India & UAE
5	Enforcement Trends	12	Our Services
6	Industry-wise Analysis	13	Acknowledgements & Contact Us
7	Country-wise Analysis		



1. | INTRODUCTION & SCOPE

Our commitment to privacy is the cornerstone of what we do at Tsaaro. The First Annual Tsaaro Report on GDPR Fines & the Privacy Landscape of 2022 is a product of the same commitment. For the purpose of the report, our team has analyzed approximately 500 fines & penalties that data protection authorities within the EU have imposed under the EU GDPR.



Approximately 500 fines & penalties have been analyzed for this report.

It has been another busy year for enforcement authorities with record-breaking fines making it to the Top 5 on the GDPR fines league table. Backed with extensive research, this report is the perfect place to find information about what the privacy domain looked like in 2022. The report analyses and summarizes important privacy developments and the fines imposed on organizations due to non-compliance with the GDPR provisions.

In addition to this, the report also takes an industry-specific approach to provide an overview of the industries with the maximum number of violations. It provides insight into the countries which topped the chart with the highest aggregate penalties; and throws light on the GDPR articles which were infringed on the most. Along with this, a slew of insights and suggestions have been provided by Tsaaro's data privacy experts based on the available dataset.

1. | INTRODUCTION & SCOPE

Our commitment to privacy is the cornerstone of what we do at Tsaaro. The First Annual Report on Privacy Fines is a product of the same commitment and throws light on the Privacy Landscape of 2022. For the purpose of this report, our team has analyzed approximately 500 fines & penalties that data protection authorities within the EU have imposed under the EU GDPR. The report will limit itself to the reporting and analysis of privacy fines awarded in 2022 under the jurisdiction of EU's GDPR legislation; and data protection regulations of different countries have not been included.

In preparation of this report, the team has looked at the fines awarded by over 30 European countries which amounted to 440. The primary sources for these fines are publicly available open source platforms such as official reporting by the Data Protection Authorities and News Articles. Since all fines are not made public by data protection authorities, the dataset cannot be completed. Therefore, Tsaaro does not take any legal responsibility of such data.



2. | FINES & PENALTIES UNDER GDPR

GDPR fines are designed to make non-compliance around data privacy a costly mistake. Breaches are taken seriously, and the associated fines can reach hundreds of millions of euros.

For each individual case, fines must be proportionate, effective, and dissuasive. A statutory catalogue of criteria, which the authorities must consider in making the decision of whether and what type of penalty can be imposed, is available to the specific authorities. A penalty can be increased for a variety of reasons, including intentional infringements, failure to mitigate damage, and lack of collaboration with authorities.

A punishable action in a company may be discovered through:

- proactive inspections conducted by the data protection authorities;
- complaint by an unsatisfactory employee;
- complaint from a customer or potential customer;
- official self-denunciation of the company;
- investigative journalism etc.



2. | FINES & PENALTIES UNDER GDPR

**€20M
or 4%**

It is possible to be fined up to 20 million euros for particularly serious violations listed in Article 83(5) GDPR, or up to 4% of the preceding fiscal year's total global turnover for undertakings.

**€10M
or 2%**

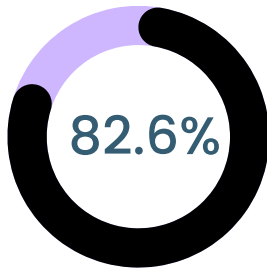
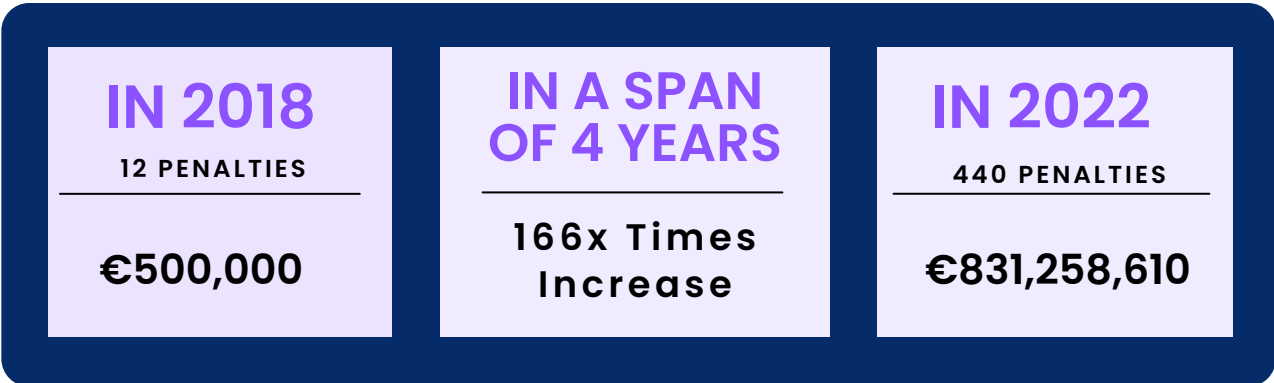
A lesser-severe violation is defined in Art. 83(4) GDPR as one that may result in a fine of no more than 10 million euros or 2% of a company's worldwide sales during the preceding fiscal year, whichever is higher.



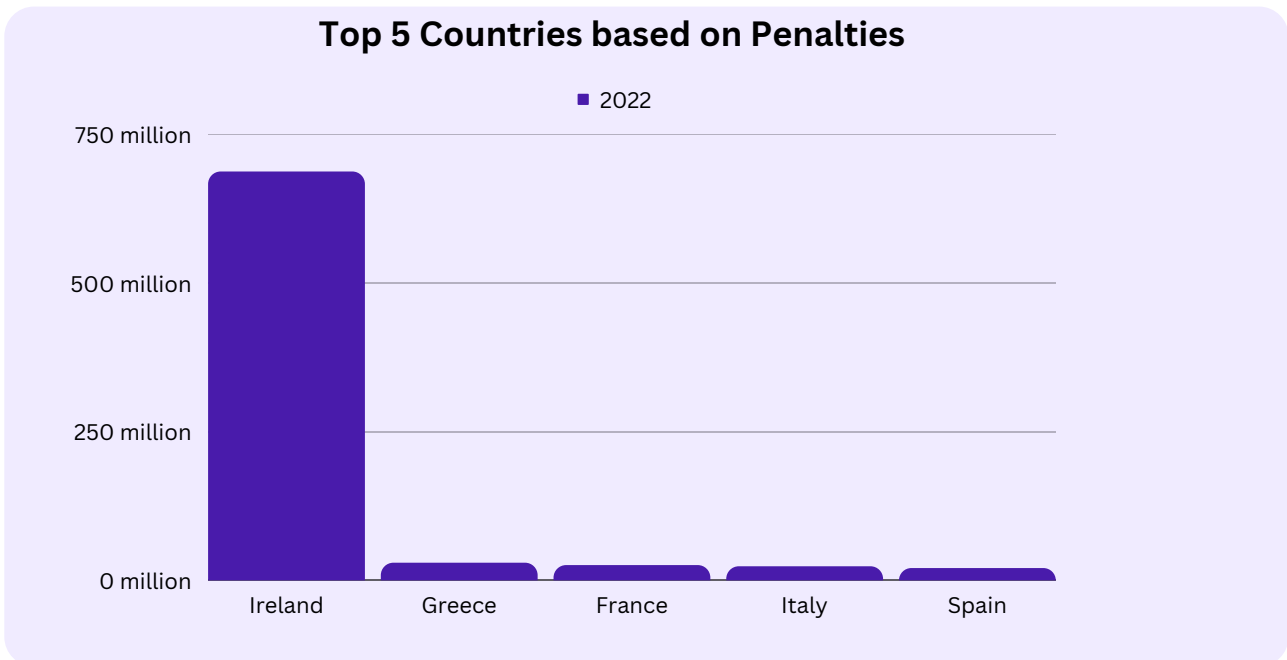
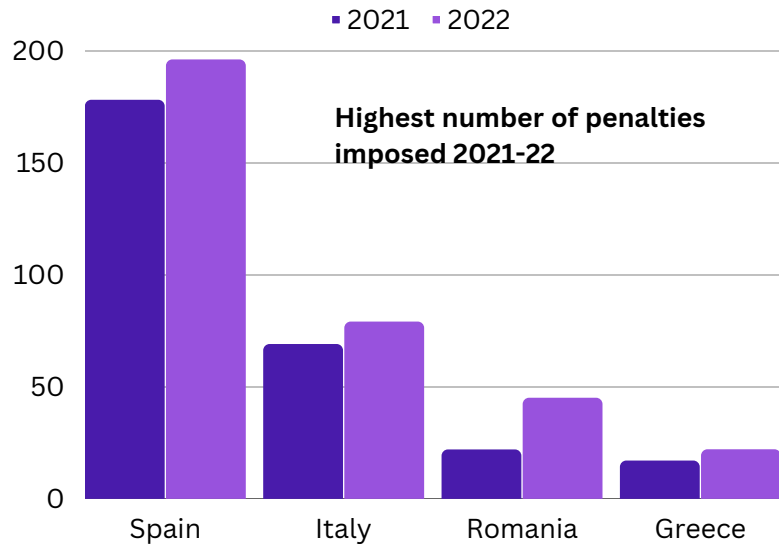
Additional Penalties

Member States may lay down additional penalties under their national regulations, such as criminal penalties for certain GDPR violations or national rules which can be imposed by national authorities based on GDPR's flexibility clauses. These penalties act as an additional deterrent.

3. | KEY FINDINGS



The penalties imposed on the Meta Platforms contribute 82.6% (€687 M) of the total fine.



* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

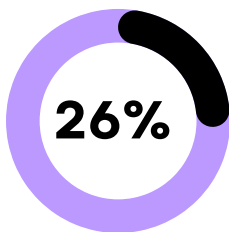


3. | KEY FINDINGS



86%

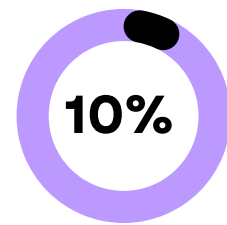
Media, Telecoms and Broadcasting Industry Accounted for about 86% of the total fines.



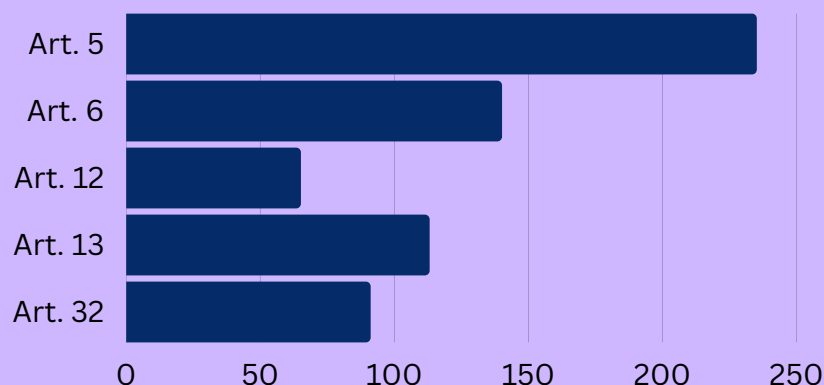
In the Finance, Insurance & Consulting sector, roughly 26% violated Article 5 of the GDPR.



Nearly 29% of the penalized companies in the Transport & Energy sector violated Article 6 of the GDPR.



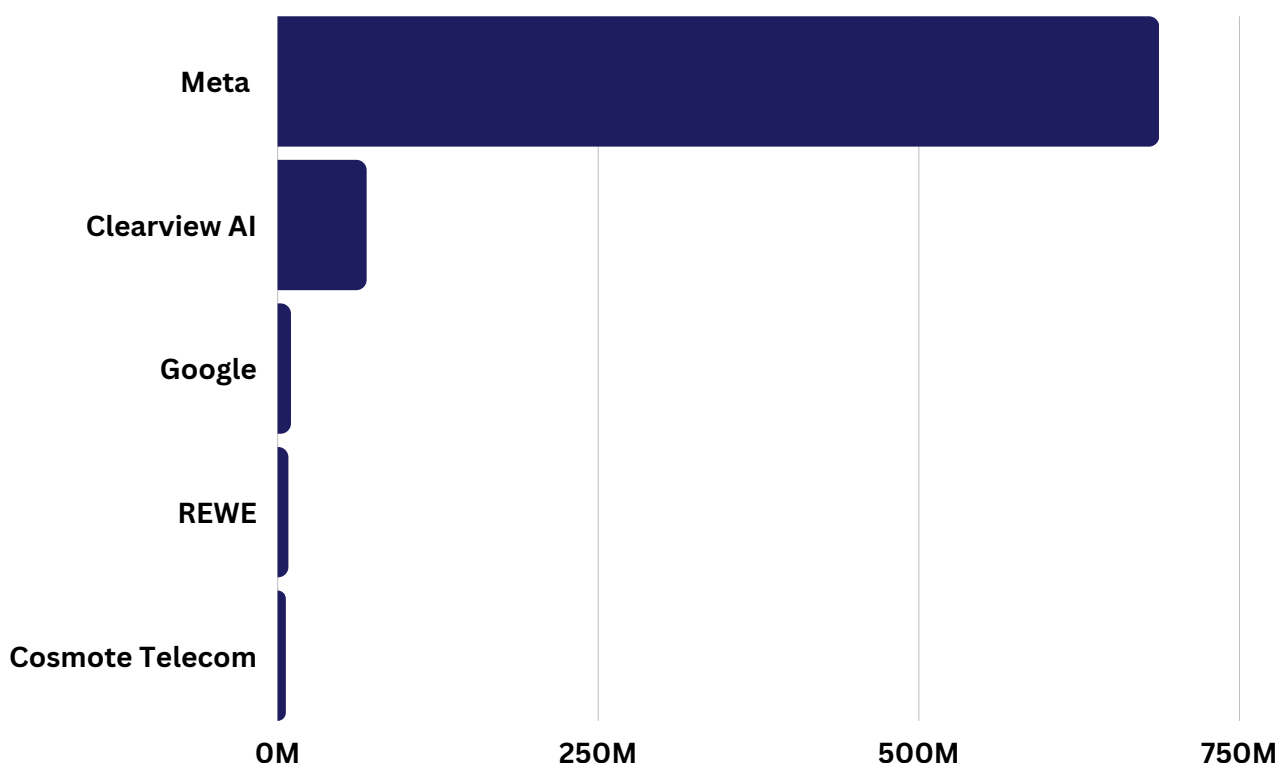
Public Sector Entities & Educational Institutions were heavily penalized, contributing to about 10% of the total fines imposed.



The above graph depicts the Top 5 provisions for which organizations were penalized the most.

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

4. | TOP PENALTIES OF 2022



1. Meta Platforms Inc. – € 687 Million

Meta was fined at 3 separate instances in 2022 by the DPA of Ireland, with the highest penalty being 405 million Euros levied on 9th May 2022. This fine was levied after the investigation revealed that the personal data of minors had been publicly displayed. It was further found that the default settings of underage accounts were set to “public” making their accounts viewable by anyone unless the account holders went & changed the settings.

On the other 2 instances, Meta was fined 265 million Euros & 17 million Euros being levied on 25th November 2022 & 15th March 2022, respectively. These fines were levied after Meta was unable to demonstrate they had sufficient technical & organizational security measures in place.

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

2. Clearview AI Inc. – € 69 Million

Clearview was fined a total of 4 times in 2022 with 3 of those fines amounting to 20M Euros each levied by Greece, Italy, & France's DPA. UK's DPA levied a fine of 9M Euros. Clearview company holds a facial image database of more than 20 billion images from around the world, & provides users with a search service that allows individuals to be identified based on the biometric data extracted from the images. The fines were levied after the DPAs found that the company's database had processed the data unlawfully & without a valid legal basis.

3. Google LLC – € 10 Million

Spain's DPA imposed a fine of 10 million Euros on the basis of an investigation which took place after two data subjects complained that Google had disclosed their personal data to third parties without authentication. The investigation revealed that Google had passed on the personal data of the data subjects to the 'Lumen project' which was run by the Berkman Klein Center for Internet & Society at Harvard University. The project was initially started in 2002 for collecting requests relating to the removal of content from websites not limited to the United States. It was found that the data was transferred to a third country without giving the data subjects the option to object to it. In some cases, sensitive personal data was also processed.

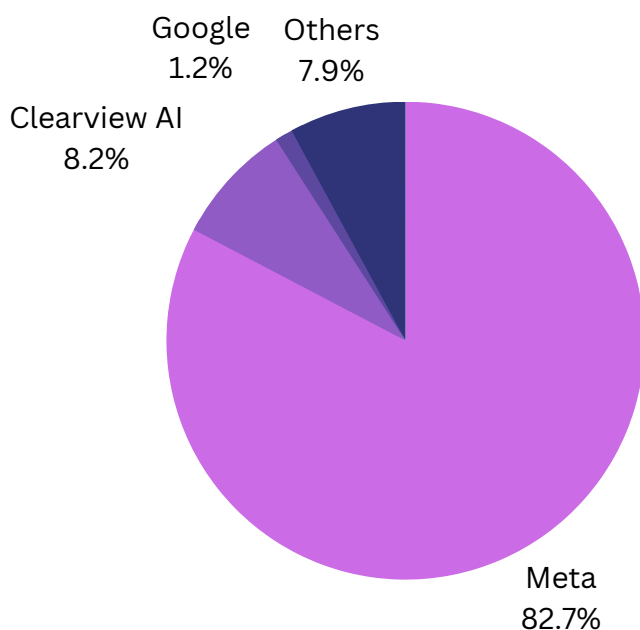
4. REWE International – € 8 Million

The Austrian food retailer, REWE International, was fined 8 million Euros by Austria's DPA for the careless handling of customer data. The company's loyalty club allegedly collected data on the users without their consent and used it for marketing purposes, thus violating various provisions of GDPR.

5. Cosmote Telecomm. SA – € 6 Million

Greece's DPA imposed a fine of 6 million Euros on Cosmote Telecommunications pursuant to Article 33 of the GDPR. The investigation revealed that a hacker had gotten through the controller's system & had leaked the data of customers. The HDPa found that Cosmote had failed to put in place technical & organizational measures which would have ensured the proper execution of the data anonymization process. Furthermore, Cosmote had failed to conduct a Data Protection Impact Assessment (DPIA) and failed to inform its customers on the data processing criteria.

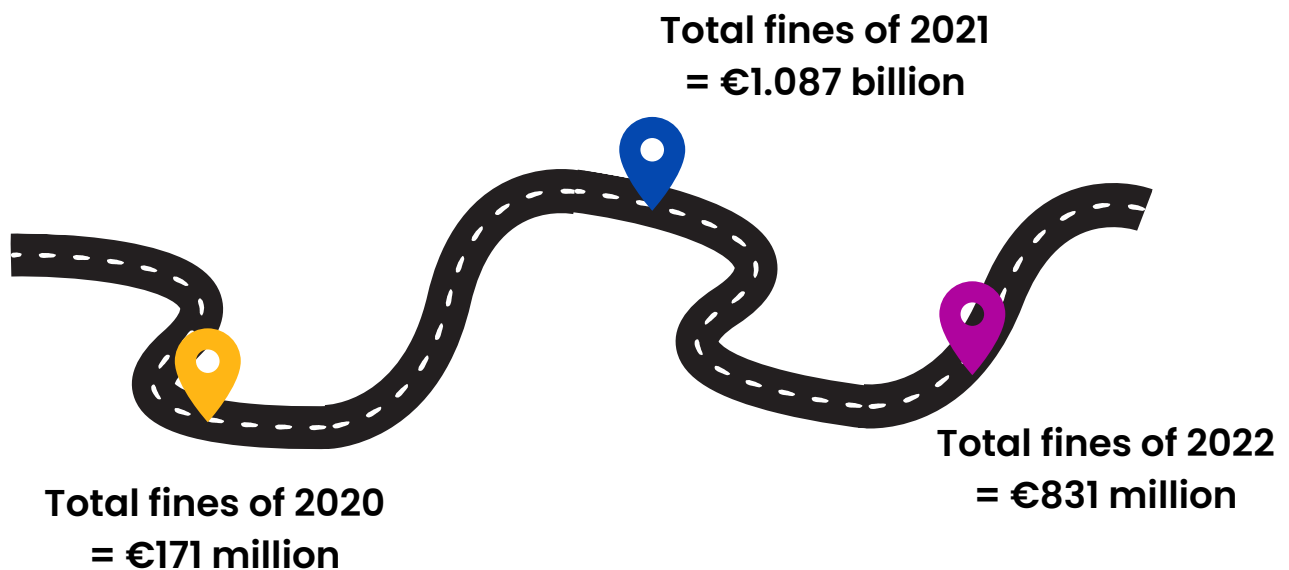
PERCENTAGE SHARE OF THE HIGHEST GDPR PENALTIES OF THE YEAR 2022.



The penalties imposed on the Meta Platforms contribute 82.6% of the total fines & dominated the charts in 2022. The penalty imposed on Clearview AI covers a percentage share of 8.3% & Google shares a percentage value of 1.2%. Lastly, all the penalties imposed on other entities in the EU constitute 7.9% of the penalties imposed in the year 2022.

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

5. | ENFORCEMENT TRENDS



INCREASING TREND

2021 saw an increase in GDPR penalties with the upward trend continuing through 2022 as well, though the overall fines awarded were smaller compared to 2021. The upward trend can be attributed to the fact that supervisory authorities are cracking up their enforcement regime & did not leave a stone unturned in ensuring compliance. For example, in the Accommodation and Hospitality sector, the supervisory authorities fined even small companies with some penalties ranging up to seven figures.

PROACTIVE IMPLEMENTATION

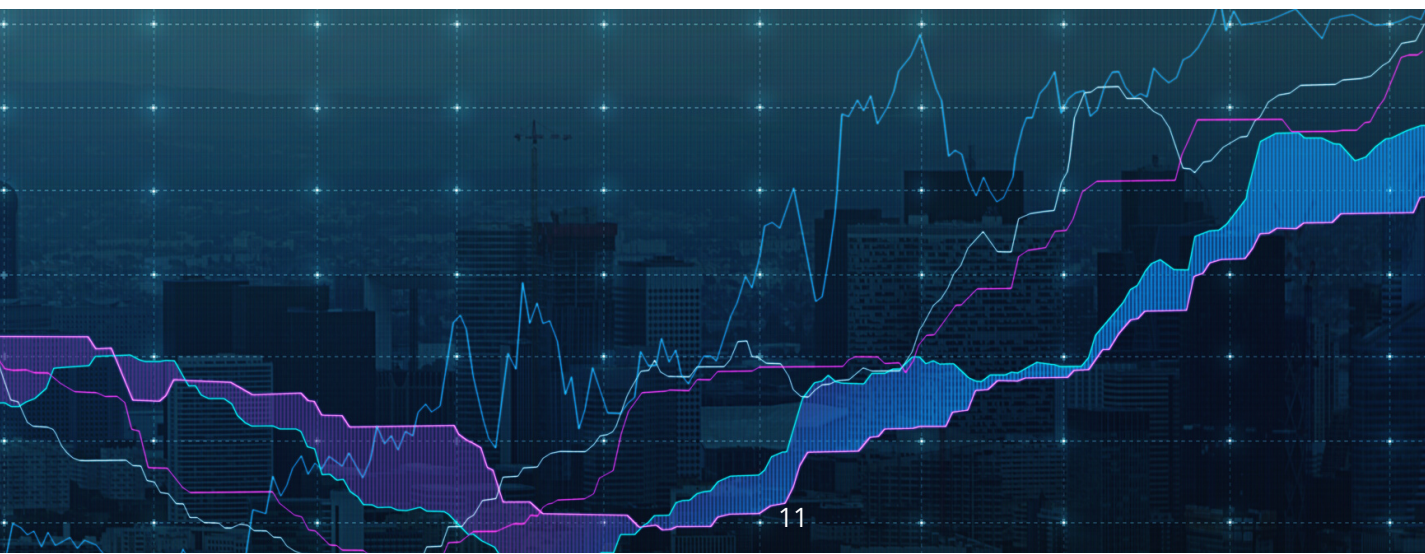
The supervisory authorities in the EU are becoming more stringent with GDPR compliance. Multinational organizations are facing hefty fines as can be observed in the case of Meta Platforms in 2022. At the same time, smaller corporations and entities have also been fined with the smallest publicly available recorded fine of 2022 being of 120 Euros which was fined by the Spanish Data Protection Authority.

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

6. | INDUSTRY-WISE ANALYSIS

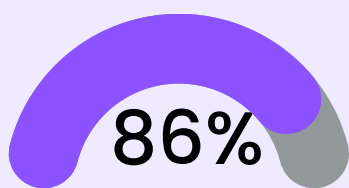
Rank	Industry	Penalty (Approx. Figures)
1	Media, Telecoms and Broadcasting	€ 718 M
2	Industry and Commerce	€ 86 M
3	Public Sector and Education	€ 8.9 M
4	Finance, Insurance and Consulting	€ 5.65 M
5	Transportation and Energy	€ 5.63 M
6	Healthcare	€ 2.5M
7	Real Estate	€ 2 M
8	Accommodation And Hospitality	€ 255K
9	Employment	€ 206K
10	Individuals And Private Associations	€ 193K

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.



6.1 | MEDIA, TELECOM & BROADCASTING – € 718 MILLION

The Media, Telecom & Broadcasting Industry was significantly penalized, and breaches were appropriately punished. This industry contributed roughly 86% of the total fines collected. This demonstrates the need for evolving privacy policies, without which organizations would continue to face scrutiny. Even huge firms like Meta that were imposed with the largest fine of €405M were not given immunity. This shows that the authorities are now stringent to take action against companies whenever it deems security measures are not adequate or are causing trouble to the data subjects. In this way, the transparency concept may be used to build confidence amongst the users.

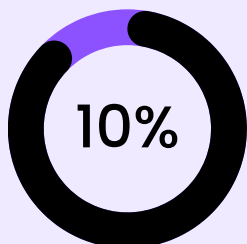


Media, Telecom & Broadcasting Industry accounted for about 86% of the total fine.

6.2 | INDUSTRY & COMMERCE – € 86 MILLION

For businesses in the Industry & Commerce sector, in particular, failure to comply with General Data Protection Regulation and inadequate data security measures led to significant fines. Fines in this sector contributed to about 10% of the total fines collected. Data protection authorities have demonstrated that they are prepared to inflict six-figure or even seven-figure fines for inadequate security measures, particularly when significant volumes of personal data are made accessible to the public. Authorities are carefully considering the need for data processing & the length of storage periods in terms of general data protection rules. 7 figure fines are also feasible for certain kinds of offences, depending on the severity of the infringement. The heavy fine on Amazon might not be the only instance of such a heavy penalty in the future. Even Clearview AI was imposed with a fine at 4 separate instances which combined to a total of of € 69 Million.

6.3 | PUBLIC SECTOR & EDUCATION – € 8.9 MILLION



Even Public Sector Entities & Educational Institutions were heavily penalized, contributing to about 10% of the total fines imposed.

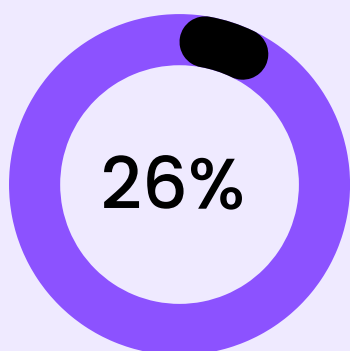
Due to their unique position of trust, public agencies must adhere to data protection rules with exceptional strictness & maintain high levels of data security. The same is true for educational institutions like schools, particularly those that handle minors' personal data. As this sector became increasingly dependent on technology due to Covid-19, infractions were caused & duly punished. In this industry, the entity with the largest fine was Portuguese National Statistical Institute, with a fine worth € 1.3 Million. Recently, there have been more penalties handed out in the public sector for transgressions of data protection laws including the processing of sensitive personal data (eg. medical information), profiling, & the tracking or surveillance of persons. Future continuation of this pattern is likely. This time, this sector was responsible for almost 1% of the total fines imposed.

6.4 | FINANCE, INSURANCE & CONSULTING – € 5.65 MILLION

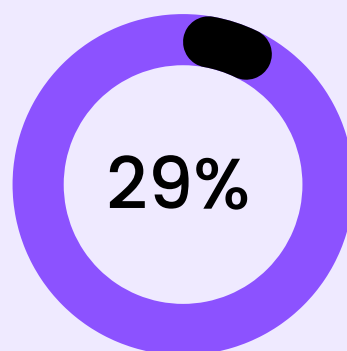
The growth in fines in the Finance, Insurance, & Consulting sectors has persisted with new penalties totaling millions which cumulatively contributed to about 0.68% of the total fines collected. Additionally, it appears that authorities are paying closer attention to how precisely consent was gained & if data subjects were adequately informed by the controller. Additionally, inadequate data security procedures led to hefty penalties & brought significant harm to the company's reputation as well. It is important to note that 26% of the fines were imposed for violating Article 5 of the GDPR, which relates to the principles relating to processing of personal data. Even Danske Bank, which had the highest fine of € 1.3 Million was penalized for violating this Article.

6.5 | TRANSPORT & ENERGY– €5.63 MILLION

The fines in this sector range from low 4-figure to high 7-figure fines. Despite the sector being hit by the Covid-19 Pandemic, the Data Protection Authorities have not spared the Transport & Energy Sector. This sector made up 0.67% of the total fines imposed. The fines have gone up & the Authorities have duly taken note of non-compliance and breaches. The number of data subjects concerned, the severity of the individual violations, as well as the willingness to comply with the individual Data Protection Authorities have all played crucial roles in determining the amount of the fines. In this segment, Amazon Road Transport Spain S.L., was the organization which had the largest fine of € 2 Million. Nearly 29% of the penalized companies violated Article 6 of the GDPR which refers to the lawfulness of processing of data.



In Finance, Insurance & Consulting sector, roughly 26% of the penalized companies violated Article 5 (Principles of Processing Data) of the GDPR.



Nearly 29% of the penalized companies in the Transport & Energy sector violated Article 6 of the GDPR that refers to the lawfulness of processing of the data.

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

7. | COUNTRY-WISE ANALYSIS

7.1 | RISE OF GDPR PENALTIES

In the year 2018, when the GDPR came into force, it was observed that there were just 12 penalties imposed by a total of 6 EU Data Protection Authorities. These were the Portugal DPA, Hungary DPA, Germany DPA, Czech Republic DPA, Bulgaria DPA and Austria DPA. The total penalties in 2018 amounted to less than €500,000.

The total amount of GDPR Penalties imposed by all EU Data Protection Authorities accounted for €831 M for the year 2022.

2018

12 PENALTIES:

€500,000

IN SPAN OF 4 YEARS

166x Times
Increase

2022

440 PENALTIES:

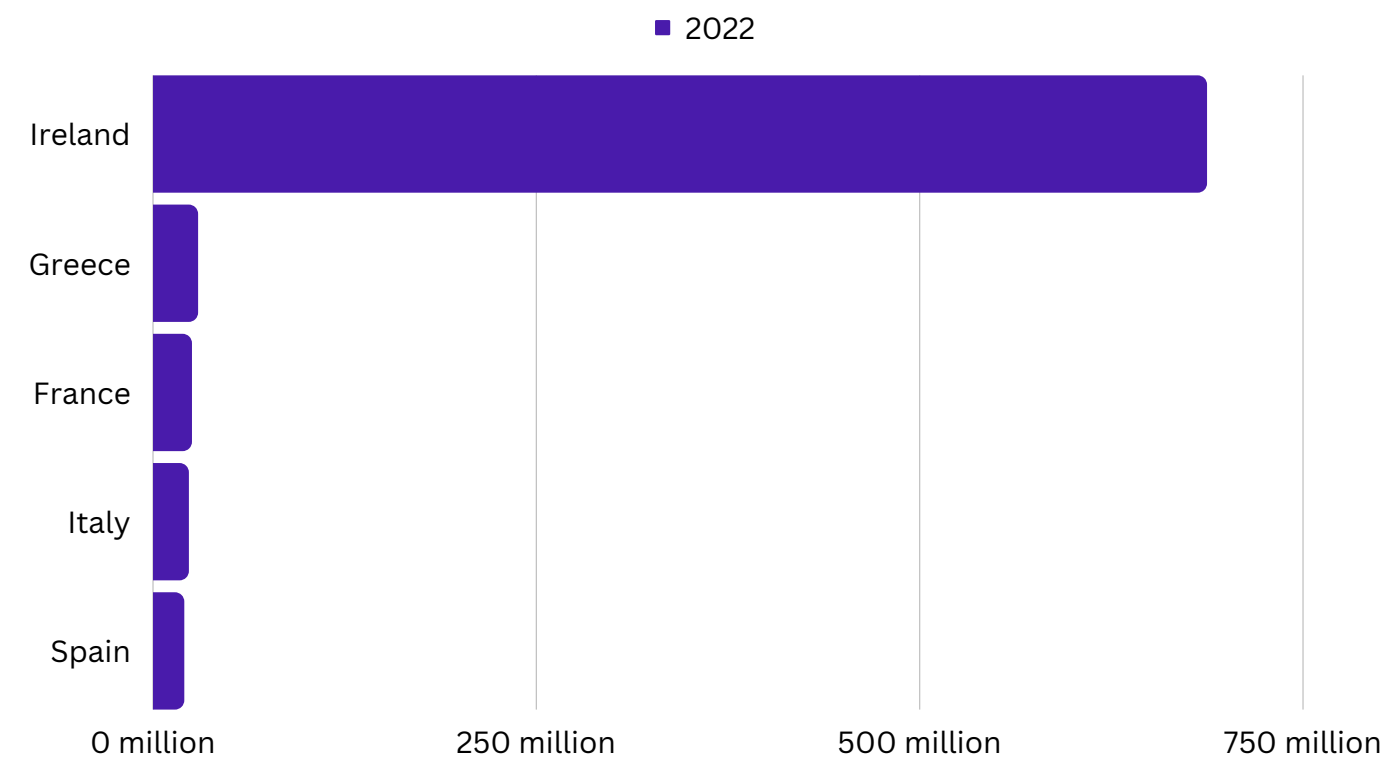
€831,258,610

The findings show that since the enforcement of the GDPR in the year 2018, the penalties have increased massively by 166,152%. The GDPR Penalties are only expected to rise in the coming years.



* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

7.2 | TOP 5 COUNTRIES BASED ON PENALTIES



The above-displayed bar graph showcases the Top 5 Countries in the EU based on the GDPR Penalties imposed on them in the year 2022.

Ireland tops this list by an extreme majority of the total amount of penalties imposed in the entire EU in 2022. Furthermore, the Irish DPA in 2022 imposed a total of 5 penalties which amounted to a total of €687 M.

The Hellenic DPA (Greece) ranks second in this list & they imposed a total of 22 penalties in the year 2022, which amounted to a total of €29 M.

On the other hand, the French DPA ranks third in this list, and imposed a total of 9 penalties in the year 2022, which amounted to a total of €25 M.

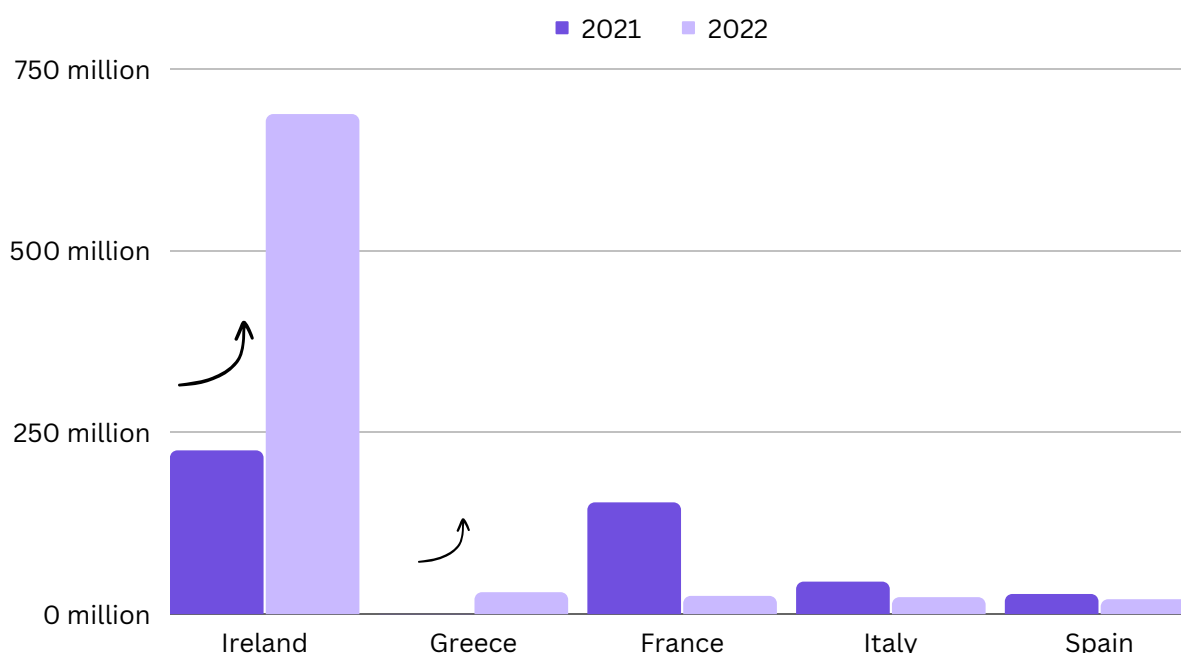
The Italian DPA ranks fourth in this list and imposed a total of 79 penalties which amounted to a total of €23 M in 2022.

The Spanish DPA ranks fifth in this list and imposed a total of 196 penalties which amounted to a total of €20 M in 2022.

7.2 | TOP 5 COUNTRIES BASED ON PENALTIES

From the present findings & the data available, we found out that the Irish DPA tops in imposing the biggest individual penalty in the year 2022 against Meta Platforms Inc., amounting to €405 Million.

If we compare this with the 2021 penalties imposed by the Irish DPA i.e. 225 Million Euros, shown in the bar graph given below; it is observed that there has been an exponential rise of 205.18% in the value of penalties imposed by the Irish DPA in just a span of 1 year.



With the present statistics, we can further conclude that the Irish DPA is the strictest and most stringent DPA in the EU. Furthermore, it has also been observed that though the Irish DPA issues a significantly smaller number of penalties each year, the value of each penalty issued by the Irish DPA is significantly rising, showcasing their stricter approach towards the enforcement of the GDPR.

Moreover, there has been a massive rise of 104,580% in the value of penalties imposed by the Hellenic DPA (Greece). As of the year 2021, it issued total penalties amounting to €281,000, whereas in the succeeding year, it issued penalties amounting to €29 Million, leading to exponentially high growth in the value of penalties imposed by them.

7.2 | TOP 5 COUNTRIES BASED ON PENALTIES

It is essential to note here that the value of penalty differs majorly because of two vital ingredients i.e. seriousness of the violation and size of the organization. Under the GDPR, for less serious violations, a fine of €10 million or 2% of a firm's annual revenue from the preceding financial year is imposed, depending on which amount is higher. Moreover, serious violations could lead to a fine of up to €20 million or 4% of a firm's annual revenue from the preceding year, depending on what is higher.

Negative growth in the amount of GDPR penalties

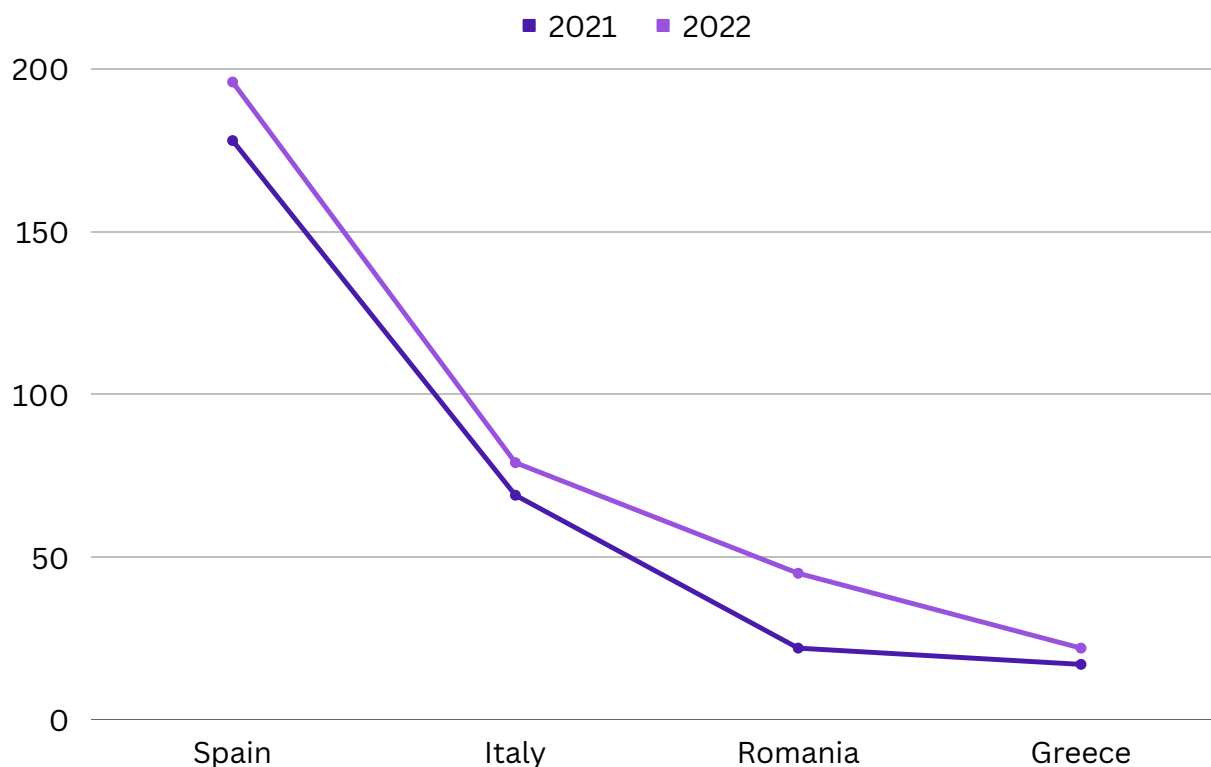
The year 2022 witnessed a negative growth in the amount/value of the penalties imposed by some of the top DPAs in the EU, namely- the French DPA, the Italian DPA & the Spain DPA. They still rank on the top 5 Country/DPAs list; but compared to their previous year's (2021) statistic, the penalties imposed were significantly lower.

Country	2021	2022	% Decrease
France	€153M	€25M	-83.59%
Italy	€44M	€23M	-46.28%
Spain	€27M	€20M	-23.35%

The reasons behind this negative growth could be a less stricter approach by the DPA, violations caused by small-sized businesses, and/or cases of less serious violations.

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

7.3 | HIGHEST NO. OF PENALTIES IMPOSED (2021-22)



From the above data, it can be observed that the Spanish DPA imposed the highest number of penalties both in 2021 & 2022. From 178 penalties in 2021 to 196 penalties in 2022, the annual percentage growth in the number of penalties in Spain is by 10%.

Some DPAs are significantly more active than others, and this can be determined by analyzing the number of penalties imposed yearly, along with the percentage growth in the number of penalties imposed.

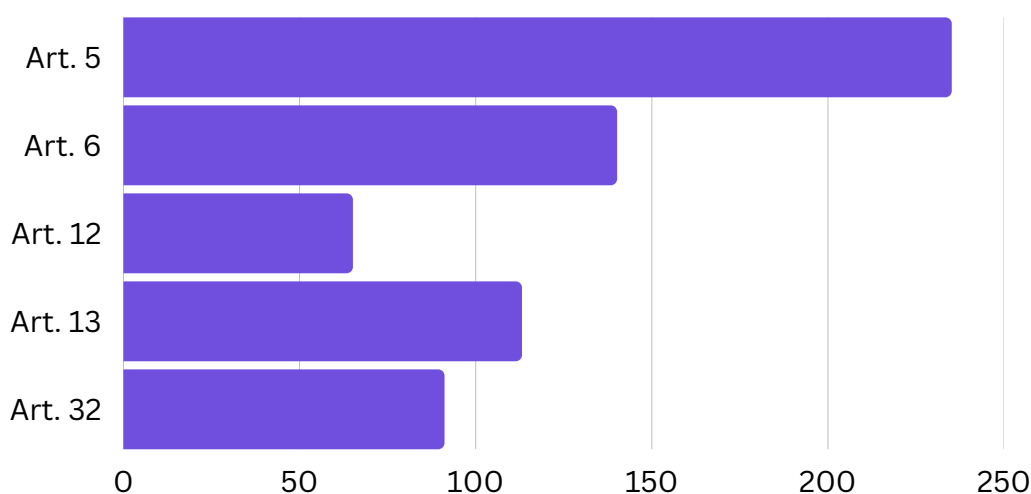
Thus, we can conclude that the Spanish DPA and the Romanian DPA have been the most actively working DPAs in the EU. There was an annual growth of 104.54% in the number of penalties imposed by the Romanian DPA i.e., from 22 Penalties in 2021 to 45 Penalties in 2022.

There has been an annual growth of 29.41% in terms of the number of penalties imposed by the Hellenic DPA (Greece) i.e., from 17 penalties in 2021 to 22 Penalties in 2022. Lastly, an annual growth of about 14.49% w.r.t the number of penalties issued by the Italian DPA, i.e., from 69 penalties in 2021 to 79 penalties in 2022.

8. | FREQUENTLY VIOLATED GDPR ARTICLES

In the year 2022, a global surge has been observed in privacy-related fine impositions across the European Union and the United Kingdom.

Out of the 33 GDPR provisions violated, the top 5 provisions for which violators were penalized the most are Article 5 followed by Article 6, Article 13, Article 32 & Article 12.



Penalty for violations of 4 out of the top 5 provisions was imposed on the industry & commerce sector.

The public sector also witnessed a large number of violations relating to Articles 5,6,32 and 12 whereas the real estate sector recorded the least number of violations across the Top 5 violated GDPR provision.

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

8. | FREQUENTLY VIOLATED GDPR ARTICLES



Article 5

It outlines the principles of processing personal data. Any processing undertaken under the GDPR must adhere to the principles of Lawfulness; Fairness and Transparency; Purpose Limitation; Data Minimization; Accuracy; Storage Limitation; Accountability; Integrity & Confidentiality.

22%

**Violations caused
by Individuals and
Private
Associations**

The findings suggest that out of the 235 violations recorded for Article 5, Individuals and Private Associations accounted for nearly 22% of the total violations. Following its footsteps is the Industry & Commerce sector at 16%, the Public sector at 11% and the Finance, Insurance & Consulting sector at 10%.

The major causes of fine impositions include undertaking processing in the absence of a legally valid basis, non-adherence to the principle of data minimization & lack of transparency with the data subjects.

* The data mentioned is based on publicly available sources. For further information on sources, refer to the Scope of the Report which has been mentioned on Page 2.

Article 6

22%

**Violations
occurred in the
Industry &
Commerce Sector**

It outlines the lawful bases for processing of personally identifiable data, which are – Consent, Performance of a Contract: Complying with the Legal Obligation of the Data Controller; Protecting the Vital Interests of the Data Subject; Performance of a task carried out in Public Interest/exercise of Official Authority; & Fulfilment of Legitimate Interests pursued by the Controller/Third-party.

The findings suggest that the Industry & Commerce sector continues to hold its top position with the maximum number of violations out of the total 130 violations recorded for Article 6. This accounts for nearly 22% of the total violations. The majority of companies have been penalized on the grounds of insufficient legal basis with the lack of consent being the top most violated provision.

Article 12

It highlights the obligation of the data controller to provide information to the data subjects regarding the processing of their data, facilitate the exercise of data subject rights, provide information on actions taken or not taken in pursuance to a request, and so on.

21%

**Violations occurred
in the Industry &
Commerce Sector**

The findings suggest that similar to the other provisions, the Industry & Commerce sector accounted for the maximum number of Article 12 violations i.e., 21% of the 65 recorded infringements and was followed by the Public sector at 18%.

It was also observed that unlike the other sectors the Real Estate sector had been fined for zero Article 12-related violations. The biggest non-compliance by organizations that resulted in the imposition of fines was the deficiency in providing information to data subjects regarding the processing being undertaken and the non-fulfilment of their rights.

Article 13

It talks about the data controller's obligation to provide necessary information to data subjects when they directly collect personal data from them.

28%

**Violations occurred
in the Industry &
Commerce Sector**

The findings suggest that out of the 113 Article 13 violations, the majority of them have occurred in the Industry and Commerce sector. This amounts to nearly 28% of the total violations, followed by Individuals and Private Associations at 10%.

The majority of the companies were penalized for insufficient fulfilment of their information obligations, the top ranking being their duty to provide details of the processing being undertaken.

Article 32

15%

**Violations
occurred in the
Industry &
Commerce Sector**

It outlines the obligations relating to data security. It requires the controller as well as the processor to establish appropriate technical and organizational measures. Examples of measures that can be implemented to ensure a level of security appropriate to the risk.

- Encryption
- Pseudonymization
- Regular assessment of the effectiveness of existing measures.

The findings suggest that apart from the Industry and Commerce sector which accounts for nearly 15% of the 92 recorded violations, the Insurance, Health Care and Public sectors accounted for 51% of the total violations related to Article 32.

The top 2 security measures that were found to be absent in the majority of the organizations leading to violation of Article 32 were measures to prevent unauthorized access and lack of encryption of personal data.

9. | SUMMARY

The Report on Privacy Fines 2022 analyzed approximately 500 fines & penalties which have been awarded under GDPR and found that the total fines awarded were 831 Million Euros in 2022. The report has given a detailed analysis of the top 5 penalties of 2022, with the highest fine being awarded to Meta Platforms Inc. at 405 Million Euros. With 3 separate penalties, Meta alone accounted for 82.7% of the total fine amounts imposed. Comparing the fines of 2022 with previous years, it was found that the overall amount of fines awarded was lower than in 2021. However, since the enforcement of the GDPR in 2018, the penalties have increased massively by 166,152%. This shows a trend where the supervisory authorities are becoming more active in the implementation of GDPR and are not taking even the smaller violations lightly.



Article 5 which deals with the principles of processing was violated over 200 times making it the article which saw the most violations in 2022. Other articles which witnessed frequent violations were Article 6, Article 12, Article 13 and Article 32. The Media, Telecom & Broadcasting industry was responsible for about 86% of the total fines worth €831 million imposed in the year 2022. The Irish Data Protection Authority displayed a stringent stand this year, and it was responsible for the majority of the fines imposed this year. It was followed by the Hellenic, French, Italian and Spanish DPAs respectively. Our report has also come up with important suggestions to ensure compliance and avoid fines. These suggestions include the adoption of important security measures, awareness of pertinent regulations, and ensuring the basis of data collection and minimizing data collection.

10. | SUGGESTIONS

From a business organization's perspective, it is essential to avoid the above-mentioned hefty penalties.



Know the regulations applicable to your business and processing

Ensure that you have an adequate understanding of all the global laws & regulations including directives that are applicable to the processing being undertaken by your organization. This will help you avoid any transgressions & ensure better compliance.

Establish and Ensure Security Measures

Establish appropriate security measures such as encryption, pseudonymization conducting regular DPIAs, risk assessments etc. in your organization. Regularly monitor and update the effectiveness of such measures.

Get a GDPR-compliant Privacy Policy

Carefully assess and draft an inclusive privacy policy that fulfils the requirements outlined under Articles 5,6,12, 13 and 32. Ensure that your policy is comprehensible and in plain language. Additionally, update your policy regularly and send notify your users of the same.

Be clear on your basis of collection and minimise data collection

Have clarity of the valid grounds based on which you are collecting data and ensure that you are not collecting data more than what is required for the specific purpose. In general, the less data you process, the less likely you are to risk violations and fines.

11. | SPOTLIGHT ON INDIA AND UAE



INDIA'S DIGITAL PERSONAL DATA PROTECTION BILL

The Indian privacy landscape will witness a transformation this year when the Draft Digital Personal Data Protection Bill becomes a law. Under this new law, penalties have been clearly laid down in Schedule 1. Data Fiduciaries can be penalized for up to Rupees 500 crores if they fail to comply with the provisions of the law.

The law provides for various responsibilities for data fiduciaries like implementing reasonable security practices and protecting against data breaches. Non-compliance to this can lead to penalties upto Rupees 250 crores. The law also lays down the need to notify the Data Protection Board incase of any data breach, failure to comply can invite penalties upto Rupees 200 crores. The Schedule provides a detailed laundry list of various penalties which data fiduciaries have to prepare against.



UAE'S PERSONAL DATA PROTECTION LAW

In 2022, the United Arab Emirates achieved a big milestone as it introduced the country's first comprehensive federal legislation aimed at protecting the privacy of data subjects and their related rights in the form of the UAE Personal Data Protection Law, 2022.

The Law is a welcome change which will significantly impact the way companies do business in the region, increase confidence for global companies looking to do business here, and support several large-scale digital transformation projects in both the public and private sectors.

Under the new law administrative penalties may be imposed as part of a decision by the Council of Ministers in response to a breach of the PDPL or the Executive Regulations. While there is no explicit mention of the penalty amount that will be imposed on organizations that fail to demonstrate compliance, strict and rigorous provisions vis-a-vis the Executive Regulations are expected to follow.

OUR SERVICES

200+

Projects
Completed

100+

Clients across
the World

150+

Privacy & Security
Consultants

15+

Regulations
covered

Tsaaro is an initiative by Privacy Leaders & Professionals and provides solutions for all your Privacy & Cybersecurity hurdles and concerns.

- **Privacy Compliance Services**

DPO as a
Service

Staff
Augmentation

Privacy Program
Development

- **Privacy Assessments**

Product
Assessment

Regulatory
Assessment

Privacy Risk
Assessment

- **Cyber Security Service**

CISO as a
Service

Information Risk
Management

Cyber Security &
Governance

- **Cyber Security Assessments**

Third-Party Risk
Assessment

Cyber Security
Maturity Assessment

- **Security and Privacy Standards**

ISO 27001 /
27701 / 22301

NIST

CIS

- **Privacy Regulations**

GDPR

India DPDP

UK's DPA,
PDPA (SGP)

ePrivacy
Directive

CPRA, HIPAA

- **Privacy Tools**

OneTrust

Securiti.ai

BigID

Privado

Exterro



Akarsh Singh
(CEO & Co-Founder, Tsaaro)

Akarsh is a leading expert in Privacy implementation. and a Fellow in Privacy by IAPP, the highest certification in the field of Privacy.

Gauri Singh
Data Protection Consultant, Tsaaro

Gauri is a law graduate and also holds an LLM in IPR & Technology Law. She is well versed with GDPR, CCPA, CPRA & PDPL and assists clients with privacy compliance programs.

Poojan Bulani
Data Protection Consultant, Tsaaro

She is a law graduate from RGNUL Punjab. She works with organizations to help implement privacy compliance programs. She has experience with GDPR, CCPA, ISO 27701.

CONTACT US

You can assess risk with respect to personal data and strengthen your data security by contacting Tsaaro.

Tsaaro Bangalore Office

Manyata Embassy Business Park,
Ground Floor, E1 Block,
Beech Building, Outer Ring Road,
Bangalore- 560045
India
P: +91-0522-3581

Tsaaro Gurugram Office

Level 1, Building 10A,
Cyber Hub, DLF Cyber City,
Gurugram, Haryana 122002
India
+91522-3581306

Tsaaro Amsterdam Office

Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW,
Netherlands
P: +31-686053719

EMAIL US

info@tsaaro.com