Public Sector Innovation – An Analysis of Privacy Disasters

Aaloka Anant* and Ramjee Prasad

CTIF Global Capsule, Aarhus University, Herning, Denmark
E-mail: aaloka@mayadataprivacy.eu; ramjee@btech.au.dk
**Corresponding Author*

Received 10 March 2023; Accepted 27 October 2023;
Publication 07 February 2024

Abstract

Europe has multiple hubs for innovation. Some of them namely being Munich, Berlin, Paris, Helsinki, Copenhagen, Dublin and many more. Innovations have been the prime driver of economic progress. Most often innovations have brought a country ahead of others in economic prosperity. Innovations like steam engine, electricity, nuclear energy, internet, 5G and many more like these have changed the course of history of mankind by bringing a change in how people live their life from one generation to another. This paper highlights the challenges presented by privacy protection laws in nurturing innovation, if any. These challenges are faced by Educational Institutions as well as public sector organizations across Europe while promoting and nurturing innovation. The old way of collecting information, running surveys, collecting personal or sensitive information about people are no more acceptable due to digitisation, where hacks and security breaches are becoming commonplace. The restriction of knowledge sharing and knowledge gathering due to lack of technology to preserve privacy is also

Journal of Mobile Multimedia, Vol. 20_1, 181–200.
doi: 10.13052/jmm1550-4646.2017

highlighted in the paper with analysis of the current situation on breaches in public sector organizations. This is an exploratory paper which analysis the GDPR fines with focus on public sector organisations and highlights the need of comprehensive action along with impact on innovation in this context.

Keywords: Privacy, anonymisation, innovation, data security, public-sector, GDPR, cyber security.

1 Introduction

Promotion of innovation is often linked with economic prosperity of a country [1]. Knowledge sharing is a primary proponent of innovation. Public sector organisations are considered as primary drivers for innovation in several countries as Governments promote innovation across Europe. Though with the enforcement of privacy law GDPR, there has been several fines on public sector enterprises. While technology innovation is essential for the public sector's efficiency and effectiveness, it can also create significant privacy risks for individuals and communities. Therefore, it is important to understand the dynamics between innovation adoption and privacy in the European union. This research paper aims to explore the privacy related fines on public sector enterprises and evaluate if these are linked to technology innovations in the European public sector or they are linked to other issues like outdated practices etc. By examining the causes and consequences of these incidents, the study seeks to provide insights into how policy-makers, public sector organizations, and individuals can strike a balance between promoting innovation adoption and protecting privacy rights in Europe.

The organisations in European countries are increasingly adopting technological innovations to improve service delivery and meet the growing demands of citizens. These innovations include but are not limited to cloud computing, big data analytics, artificial intelligence, and the internet of things (Industry 4.0). The adoption of these technologies has the potential to improve service delivery, reduce costs, and increase the efficiency of these organisations. For instance, digital platforms can enable better communication and collaboration between citizens and organizations, public sector organisations improve public services' responsiveness, and help streamline administrative processes. In addition, technological innovations can help

public sector organizations make better-informed decisions by providing accurate data analysis and prediction.

However, the adoption of technology in general and the public sector in particular can also lead to privacy disasters. For example, there have been cases of data breaches that have exposed citizens' sensitive information to unauthorized parties. In addition, the use of facial recognition technology by law enforcement agencies has raised concerns about potential violations of privacy and human rights. Several fines for GDPR on German police were noted in 2022. Moreover, the use of big data analytics in public services can result in discriminatory outcomes, which can disproportionately impact marginalized communities. These privacy disasters have raised concerns about the potential misuse of technology in the public sector and have highlighted the need to balance innovation adoption with privacy protection. It is essential to understand the underlying causes of these incidents and explore strategies for addressing them. Therefore, this research paper aims to present a comprehensive analysis of the GDPR fines primarily focussing on public sector enterprises in Europe. In depth analysis is also performed for a few of these fines to identify the root cause of the issue, linking it with the type of GDPR violation to generalize the reasons for such fines across different organisations.

Educational institutions have been in the forefront producing innovators like Newton, Einstein, Cavendish and many more. European institutions in the entire history of mankind have produced most innovators known, though this paper highlights the challenges due to needed privacy protection faced by Educational Institutions as well as Public sector organizations across Europe. Educational institutions have been on the forefront of collaboration across industries including cross industry collaboration to result in innovation cycles, like Industry 4.0. Due to privacy regulations and increasing fines in the public sector, educational institutions are also threatened to continue their pace of innovation. Collaboration between researchers and publication of data collected from individuals is under the highest scrutiny today than ever.

Information has never been more fluid and distributable today than in the entire recorded history of human civilization. Any information captured at one place in a digital format, can easily be transmitted simultaneously across miles apart locations in fraction of a second. Such power of information exchange has presented one of the biggest challenges to researchers on protecting the individuals who may be negatively impacted by the information, if it falls in the wrong hands. Privacy regulation in the form of GDPR across

European Union is one of the best safeguards available to individuals to protect their interests while recording their information in digital format.

Public sector organizations including educational institutions, face a bigger challenge in dealing with the topic of privacy protection and has seen several fines by the regulator. In Ireland over 40% of the GDPR fines are imposed on public sector organizations. The number only differs slightly for other countries share of fines on public institutions compared to total fines issues in count; with countries like Denmark, Sweden, Portugal being above 50%, Ireland, Iceland, Malta, being above 40%, Norway, Italy, Lithuania, Poland, Estonia, Cyprus being above 30%.

Public sector organizations are the primary avenues where public can obtain services from Govt. and other public organizations. Critical personal information is stored by such organizations. This data of individuals is critical for the public body, at the same time, this data is very important for the public body to analyse, enhance and use for optimizing the benefits they can provide to the individual. Though this comes with the risk of fines and hence appropriate measures are required. The fines, not only expose the current practices in the public sector organization, but also indicate the vulnerability of these organization and the need of technology innovations in the digital economy in public sector.

Objective of the paper is to establish the fact that there have been several fines in the public sector organizations related to Privacy. And the scare of such fines is curtailing innovation in public sector operations or it's curtailing their approach to innovation in general. The research paper's significance lies in its potential to contribute to the understanding of the dynamics between innovation adoption and privacy in the European public sector context. The study will provide insights into the causes and consequences of privacy disasters and strategies for addressing them. It will also help policymakers, public sector organizations, and individuals balance the need for innovation adoption with privacy protection. The study's findings will be relevant to a range of stakeholders, including policymakers, public sector organizations, civil society representatives, and technology companies.

Second section of the paper establishes the relevance of GDPR in the Public sector. Section three establishes the basis of analysis to categorize the public sector institutions and underlines the extended use of ICB Industry standards for the purpose of this analysis. Section four presents an exploratory analysis of the GDPR fines, with focus on Public sector, healthcare and educational institutions. Section five presents a view to the future and section six concludes the paper with future work proposals.

2 GDPR and the Public Sector

The public sector has a unique responsibility to protect the personal data of its citizens. Public sector organizations, including government bodies, healthcare providers, and educational institutions, process vast amounts of sensitive personal data daily. This data is much more critical than personal data posted on Facebook or other social media, as this data is associated with personal data of the people interacting with the public services. This personal data which is also known as "Master data" of data subject contains critical information, which if fallen in wrong hands can lead to manipulation of his/her actions. A few of the actions, which have been noticed to be manipulated by misuse of personal information are changed opinion in elections, paying a scrupulous person, falling of a device in wrong hands leading to large organisational data breach, impersonation and many others [2].

The GDPR requires public sector organizations to appoint a data protection officer (DPO) to oversee compliance and ensure that data protection policies are adhered to. Failure to appoint a DPO can result in fines of up to €10 million or 2% of an organization's annual global turnover [3]. Public sector organizations must also implement technical and organizational measures to protect personal data from unauthorized access, loss, destruction, or alteration. Failure to implement adequate security measures can result in fines of up to €20 million or 4% of an organization's annual global turnover, whichever is higher.

Public sector organizations must also ensure that individuals' data protection rights are respected. GDPR requires organizations to obtain explicit consent from individuals for data processing and to inform them of their data protection rights. Organizations must also provide individuals with the right to access, rectify, and erase their personal data. Failure to comply with these requirements can result in significant fines.

Public health sector during the transition period of 2016 to 2018 across the European Union, made costly adjustments to meet the requirements of personal health data protection. In short term they suffered a shock to their financial performance to achieve preliminary success [4]. There are many other tenets in the criticism, including a lack of transparency and cooperation between DPAs, diverging legal interpretations, cultural conflicts, prioritization inconsistencies, old-fashioned information systems, and general over-tolerance or even reluctance to enforce laws [5].

GDPR is also seen to be presenting a level playing field between private and public sector when it comes to personal data. In many ways helping the

public sector to be at par with private sector. Actors working with personal data in public or private sector face similar challenges now [6].

3 Categorisation of Fines – with Focus on Public Sector

The General Data Protection Regulation (GDPR) was enacted in May 2018 to regulate the processing and storage of personal data, regardless of whether the data is processed within or outside of the EU. Data on fines imposed on companies is available via individual Govt. organisation in every country in Europe. In this section we analyse the fines in different dimensions taking the details from different sources like [7] and many other news articles and information websites.

Furthermore, to analyse the fines imposed under GDPR, different dimensions of the data were taken to present different perspectives. One of the major dimensions is the country. Different countries see a different pattern of distribution of GDPR fines for example. This is discussed in detail in subsequent section.

Another important dimension is the industry sector of the company receiving the fine. To identify the industry sector of the company, ICB index was used. ICB index also known as "Industry Classification Benchmark" was launched by Dow Jones and FTSE in 2005 and is used by FTSE international and STOXX. The ICB index provides a standardized and widely recognized way to categorize companies based on their primary business activities. By using the ICB index, more than 1600 entities including companies, public sector enterprises and individuals, which have received GDPR fines has been sorted and grouped into 10 sectors, 19 super sectors, 41 sectors, and 114 subsectors. All these are not analysed though in this paper and focus is kept on the public sector entities. Public sector entities not meaning all public limited companies, but for this research purpose, this means companies, which have major stakeholder or major financier as one of the Government departments or a Government agency. This can provide a clearer picture of the composition of the list and allow for more meaningful comparisons and analysis between companies within and across sectors. For example, such an analysis can identify if Govt. funded institutions in a given country are receiving majority of the fines or not. This can facilitate more targeted research with conclusive evidence.

A combination of the country and the industry sector present a major trend in the GDPR fines also reflecting that the demographics of the place and history of the country do influence the trend of GDPR fines, even though

this is no factor in determining the fine imposed under GDPR. This factor is not analysed in this research paper.

The "Type of Violation of GDPR" is also an important dimension, while analysing the fine. This dimension does not present any specific indication for a country or a major industry sector, though when combined from a historic basis, it may present a trend in the fines imposed on Enterprise, if any.

3.1 Classification of Companies Funded by State

There are several institutions which are run by Govt. in different countries in EU. Apart from directly the ones, which are from Govt. there are many societies which are funded by Govt. money. Another set of organisations, which are not fully funded by Govt. in different countries are Universities. Apart from Govt. bodies and private organisations, non-profit organisations are also a big sector with institutions, which are not categorised in the ICB index. A major challenge in using ICB index, was that it did not have any categorization for such institutions. For this reason, a different notation was used for public sector government funded institutions. Special sub-categories were created as below:

- Ministry: Where a Ministry is directly named
- Company from Govt.: District body, society run by public funds
- Political Party: A registered political party
- Public: Any institution which is directly not falling in any of the above categories
- Academic: Universities, Schools, education related other bodies.

Airport, Universities, Schools, Academic Institutions, water services, Child Welfare Institutions, Provincial authorities, Associations, Ministry departments, Police, are considered in our research as Public bodies as they have funding from Govt. agencies to run their operations.

Category Public used in this research covers institutions like Municipalities, Region or a City, Police, Post, Military facilities, Revenue, Staff of public authorities like Mayor, Judge etc. Public hospitals in some cases are categorised in the Public, while in many cases are categorized as Healthcare institutions. Care has been taken to categorize institutions in the very right way, though there may be some cases, where such categorization is found to be wrong and needing a correction.

Overall care has been taken that the institutions funded by the Govt. of a country are categorized in one of these 5 categories as mentioned above. Healthcare being an exception, where the institutions are partly funded by

Govt. in many cases. A separate section is created in this research paper to highlight the fines in Healthcare sector, even though it's not a public sector in general across Europe and has several companies which are completely private.

3.2 Fines by Type of Violation

Below is a list of 10 major categories in which majority of the GDPR fines can be placed. Some of the fines could not be elaborately studied for details and hence their data is not included in analysis in this paper.

- Insufficient fulfilment of data subject rights
- Insufficient cooperation with supervisory authority
- Insufficient data processing agreement
- Insufficient fulfilment of data breach notification obligations
- Insufficient fulfilment of data subjects' rights
- Insufficient fulfilment of information obligations
- Insufficient involvement of data protection officer
- Insufficient legal basis for data processing
- Insufficient technical and organisational measures to ensure information security
- Non-compliance with general data processing principles

These categories are created based on simple terms to explain what the reason for a fine imposed based on the articles in GDPR regulation. Most companies are fined for violation of more than one article in GDPR after investigation, though complain can be on any one of the regulations. These categories help understand the biggest problem relevant to categorise that fine.

4 Analysis of Fines

Institution receiving the fine gets a detailed analysis report for the fine imposed by the authority. In this section, we rely on the overall fine related statements made by the authority while imposing the fine and do not delve into details of each fine.

4.1 Country Wise Analysis

Fines has been imposed in 31 States which follow GDPR including United Kingdom while it leaves the European Union.

Figure 1 Amount of GDPR fines for top 10 countries.

In terms of the total amount of fines imposed in a country, Ireland ranks on the top with over Euro 1.3 billion worth of fines imposed on companies with approximately 46% of all fines under GDPR. Luxembourg ranks second with about quarter billion Euros in fines. France, Italy and United Kingdom rank as third, fourth and fifth, while Spain, Germany, Greece, Austria and Sweden form the top 10 list in terms of volume of fines imposed per country. This is reflected in Figure 1. By volume these top 10 countries account for over 90% of the amount in total fines in GDPR. Approximate number can only be presented here as there are some fines, for which the amount is not disclosed in public. For example, for fines on individual positions like Police etc.

In terms of count of fines, Spain tops the list with 589 fines imposed by February 2023 as reflected in Figure 2. This constitutes one-third of all the fines imposed under GDPR. Italy comes second with 241 fines, Romania, Germany, and Hungary take the third, fourth and fifth place, while Greece, Norway, Poland, Belgium and Cyprus form the top ten. Top 10 countries by count account for 81% of the fines.

Fines are not distributed evenly across sectors and countries. If we do the same analysis for fines on public sector institutions, the numbers change, and Italy emerges as the top country for count of fines on public sector institutions followed by Spain and Germany. A total of 349 GDPR fines has been imposed on public sector entities by end of February as reflected in Figure 3.

In terms of amount of fines, Netherlands tops the list with over 10 Million imposed in fines on 10 institutions. This is reflected in Figure 4. Highest fine imposed on Dutch Tax and Customs Administration of 3.7 Million Euros

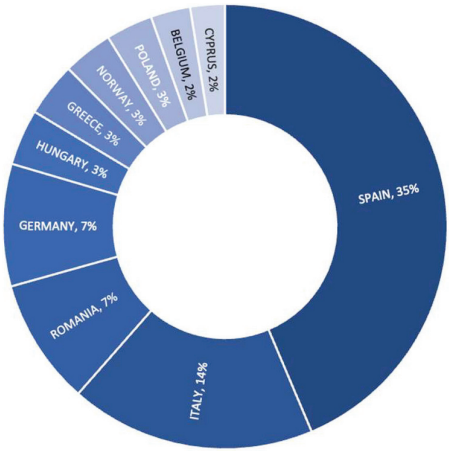

Figure 2 Count of GDPR fines for top 10 countries.

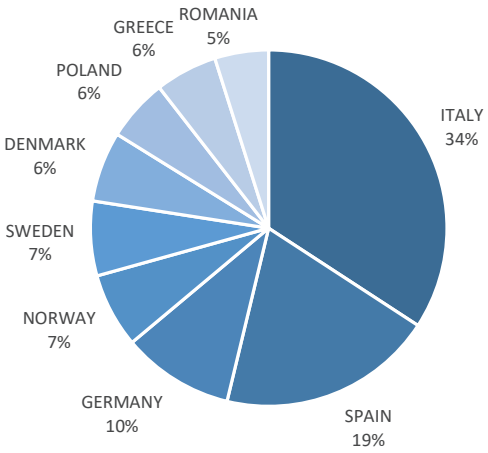

Figure 3 Count of fines for Public Sector for top 10 countries.

followed by Dutch Minister of Finance for 2.75 Million Euros. Overall average amount of fine per institution across 349 fines comes to over Eur 90,000 per fine.

4.2 Analysis by Fine Types

Analysis of fine based on the categorization as noted in the section above based on Articles in GDPR, gives a fair idea on what are the major challenges

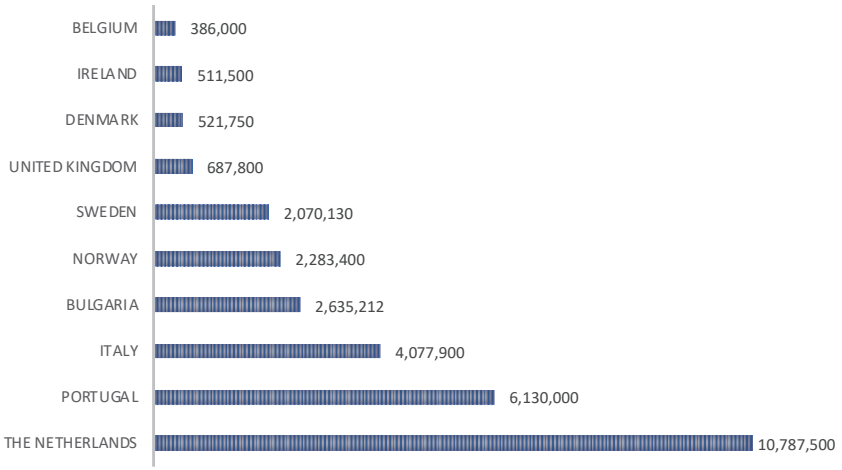

Figure 4 Amount of fines for public sector for top 10 countries.

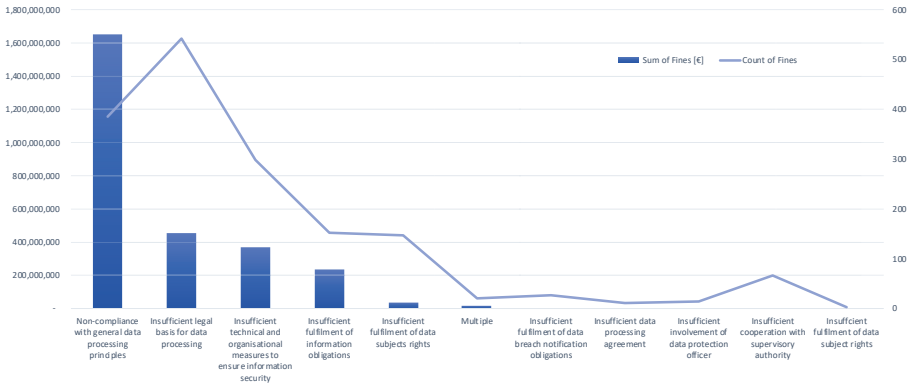

Figure 5 Sum of fines and count of fines as per Type of fine.

being faced by institutions. Non-compliance with general data processing guidelines appears to be the major reason for fines. The amount of fines as well as the count of fines for all the fines has been plotted in Figure 5, though Figure 6 showcases the same information only for public sector fines.

Second most common fine type overall and for public sector varies. Insufficient Technical and Organisational measures to ensure information security emerge as a major type for public sector fines. This does reflect the low technology adoption by public sector companies in general. Further cascaded analysis by country and type of fine is presented in next section.

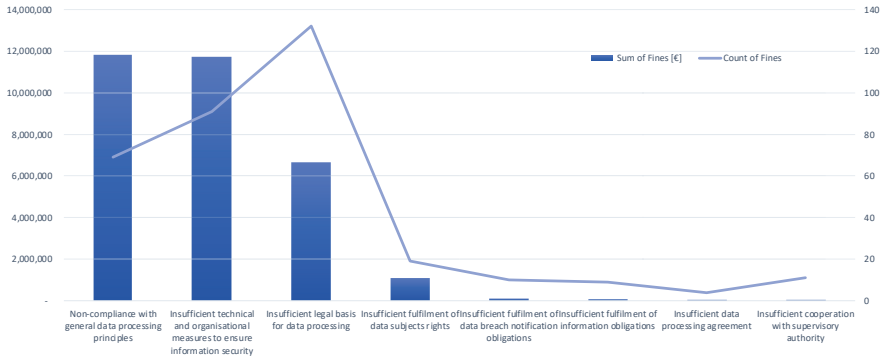

Figure 6 Public Sector: Sum of fines and count of fines as per Type of fine.

Table 1 Public sector fines: Type of fine for top 5 countries

Country	Fine Type	% of Fines
Italy	Insufficient legal basis for data processing	48%
Spain	Non-compliance with general data processing principles	50%
	& Insufficient legal basis for data processing	40%
Germany	Insufficient legal basis for data processing	88%
Norway	Insufficient technical and organisational measures to ensure information security	83%
Sweden	Insufficient technical and organisational measures to ensure information security	50%

Insufficient legal basis for data processing emerges as third major type for fines in public sector while this is the second number overall when it comes to amount of fines. Though this reason is the major reason in both cases, when it comes to the count of fines. This reflects that the public sector organisations are not conservative in their approach to process information.

4.3 Public Sector: Analysis by Fine Type Per Country for Top 5 Countries by Count

Top 5 countries for public sector fines by count are Italy, Spain, Germany, Norway and Sweden. The type of fine differs significantly when we consider only public sector companies. Insufficient legal basis for data processing forms the major reason in Germany and Italy for fines, though not others. Table 1 indicates the top reason in terms of fine count for these top 5 countries.

For public sector fines across the board, Insufficient legal basis for data processing turns out to be the major type with over 37% of fines by count being for this type. Another major point to note in Germany was that the amount of fines imposed was not disclosed in many cases, rather an indicative "three figure" or "four figure" fine was published. Many of these fines are on Police personnel.

Second highest reason for public sector fines emerges as the "Insufficient technical and organisational measures to ensure information security". This does not come as a surprise, though this indicates that there has not been enough measures taken in the public sector organisations to improve their technical readiness to comply with GDPR. Though the count is high in Norway, Denmark, Italy, Sweden and Cyprus, volume/ amount of fines are higher in Netherlands, Bulgaria, Norway, Sweden and Denmark.

Non-compliance with general data processing principles emerges as the third largest reason, with Spain and Italy topping the list. Netherlands with only 1 fine in this category, makes the country with highest published fine in public sector for 3.7 Million Euros, followed by Italy, Portugal and Norway in terms of the amount of fines.

4.4 Public Sector: Analysis Summary

Findings from the analysis cannot be concluded by mere numbers. Cultural and regional factors appear to be in play, though there is no regulation based on culture and region in GDPR. Nordic countries appear to have more fines which are imposed due to insufficient technical and organisational measures though Germany, Italy, Spain, appear to impose more fines for insufficient legal basis for data processing. Overall trend in terms of type of fines is the same across public sector or private companies with "Insufficient legal basis for data processing" being the top reason followed by "Non-compliance with general data processing principles" and "Insufficient technical and organisational measures to ensure information security". There 3 reasons account for over 70% of fines imposed under GDPR and over 80% of fines imposed on institutions in public sector.

4.5 Fines Across Healthcare Institutions

Healthcare institutions are one of the major institutions in a country which affect the life of people. Healthcare in European countries is comprising of institutions run by Govt as well as institutions run for profit. In this analysis, companies which work in healthcare area have been categorized in most

cases, irrespective of the ownership of the institution. In some cases, where the ownership of the institution was very clear as mentioned in the GDPR fine as Govt. hospital or Govt. staff, then they have been put in the public sector and has been analysed with other companies in previous sections.

Healthcare institutions in this analysis comprise of Health Care Facilities, Health Care Management Services, Health Care Services, Medical Equipment, Medical Services, Medical Supplies, Pharmaceuticals and Health Care: Misc. Apart from these there is another group with software companies which specialise in healthcare, though these have been kept out of this category.

Overall, there has been 88 fines as identified in our analysis for healthcare sector. Maximum has been in the area of health care services which account for 47% of the fines though in terms of value these account for more than 50% of the fines, over 4 million Euros. The next major area in our analysis has been found as healthcare miscellaneous these has not been of any clearly defined for example Easy Life. It's a retailer which sells healthcare equipment and was fined specifically for selling and marketing health care equipment to its customers based on certain criteria which it had no consent to do. Apart from these, medical services has also seen several fines for violation of GDPR, amounting to over 2 million euros.

Analysis of fines in this sector based on type of fine clearly reveals that the major reason for fine has been the insufficient technical and organizational measures, which amount to more than 6 million euros in fines and constitute almost 2/3 of all the fines in the healthcare sector. The next major reason for fines is the insufficient legal basis for data processing this amounts to almost quarter of all the fines amounting in value over 2 million euros. The third major category is the non-compliance with general data processing principles. These three together constitute more than 95% of all the fines in the health care sector as identified in our analysis.

A few of the fines worth mentioning in this section which are not classified in public sector in the analysis in previous sections, are listed in Table 2.

Apart from these many healthcare institutions have already been identified and analyzed in the above section as public sector. Some of these institutions are hospitals run by the state. 20 such hospitals have been fined out of which seven has been fined in six digits. Haga hospital in Netherlands Karolinska Hospital in Sweden and Østfold Hospital in Norway, to name a few for big fines. One of the major reasons for large fines in hospital are the hospitals which has received large fines is "Insufficient technical and organisational measures to ensure information security".

Table 2 Healthcare fines: top 5 – not included in public sector analysis

Company	Industry Sector	Fine Type	Fine Amount
Capio St. Göran AB	Healthcare Services (Hospital)	Insufficient technical and organisational measures to ensure information security	2,900,000
Easylife Ltd.	Health Care: Misc (Retailer)	Insufficient legal basis for data processing	1,547,000
Aleris [8] Sjukvård AB	Medical Services	Insufficient technical and organisational measures to ensure information security	1,463,000
Aleris [9] Närsjukvård AB	Medical Services	Insufficient technical and organisational measures to ensure information security	1,168,000
DEDALUS BIOLOGIE	Technology (Healthcare Software)	Insufficient technical and organisational measures to ensure information security	1,500,000

4.6 Fines Across Educational Institutions

In this paper we have included this fine on educational sector as a separate section in itself. Though the number of fines in this sector is 45 which is not a significant number as compared to overall fines, this number is the most relevant number when it comes to innovations. Our educational institutions have been in the forefront of innovation and the restrictions which has been seen on these educational institutions may change the way how innovation is nurtured in our future generations. Hence this special section highlights an analysis of the 45 fines which has been identified to be on educational institutions for violation of GDPR regulations.

First we analyze the type of fines which has been imposed on this sector and the top reason for fines is insufficient technical and organizational measures to ensure information security this reason alone accounts for 66% which is two third of all the fines in terms of value. This also accounts for 1/3 of all the fines. The second reason is insufficient legal basis for data processing this accounts for another one third of all the fine symbolized in terms of numbers.

Further going into this analysis to find which countries have imposed more fines per fine type we found that Sweden has imposed three major fines amounting to more than 700,000 euros in the reason type insufficient technical and organizational methods to to ensure information security. Italy comes second in the value of fines though first in the count of fines for this

reason. Italy on the other hand has more fines for reason, insufficient legal basis for data processing. Another major country which emerges to have imposed fines in this topic is Ireland where two institutions, which has been fined a total of above 100,000 euros.

Another major point to consider while analyzing the fines for educational institutions is to understand that these educational institutions may already fall into one of the sectors which has been already analyzed above. For example major fines in Sweden has been to two universities which are in the healthcare sector primarily dealing with patients data. It is almost impossible to segregate educational institutions from other streams for example healthcare, technology, business, etc. as educational institutions do cater to different lines of business and impact our lives in many ways.

Some of the notable institutions where such fines have been imposed are mainly Karolinska university in Sweden, Sahlgrenska university in Sweden, Bocconi university in Italy, University College Dublin in Ireland, Azienda sanitaria university in Italy, Cork university in Ireland and many more. Though the fines on universities have been smaller still it's very significant in terms of expenditure as seen for universities in Europe. The money which is spent by the universities to pay these fines reflects that significant attention needs to be given on this topic.

Universities and educational institutions are on the forefront of technology and innovation. Several researchers perform independent research based on surveys and primary information collection. In case adequate safeguards or technological measures as identified in the analysis, are not provided to the students and researchers in these universities there is a high risk that the research quality can degrade. Such a move would definitely curtail the innovation which may have been seen with a liberal privacy regulation or with easy-to-follow guidelines, privacy protection and privacy preservation technology adoption by such institutions.

In the absence of appropriate measures and appropriate technology for compliance, the Ethics Committee in these universities may be regarded as the dreaded body by researchers. The Ethics Committee which forms a very critical and important part for any research may work as an inhibitor for innovation rather than being a protector of individual rights.

5 Road to Future

Information commissioners in United Kingdom, has set out a revised approach to working more effectively with public authorities [10] in June

2022. Institutions like Technology University Munich [11] have come out to support data anonymization technologies. Though there are several technologies and approaches which are being currently used and trialed by several organizations a clear path to future is not there. The analysis in this paper has observed that there are many ways in which different institutions are trying to deal with data privacy. One of the major areas where technologies have been adopted for, is the identification of personal information [12]. It appears to be the first step to identify where is personal information which falls under the purview of GDPR and privacy regulations. The next step is definitely then to take action and ascertain that personal information is adequately protected and preserved. These different steps may or may not be done in sequence rather these can run in parallel as most innovations do. Innovations do not wait for milestones. A general practice to start privacy as a consideration right from the beginning when information is collected can change the way privacy is looked at today.

6 Conclusion and Further Work

The researcher in no way suggests reducing the compliance requirements for GDPR and other privacy regulations as these are very necessary in the growing digital world. Rather the findings indicate to enhance the technical and organizational measures in addition to a general awareness and compliance for data by all the institutions whether private or in public sector.

Another major finding in the analysis is the fact that different countries show the impact of regulation in very different ways. Though some countries have come with fines which are more in value and less in quantity other countries have come with fines which are small in value and very high in numbers. A more detailed analysis per fine needs to be conducted to be conclusive. The work presented in this paper merely scratches the surface of the problem which is evident in the public sector.

Further to this paper more research needs to be conducted in identifying how the situation can be improved. Public sector organizations and most public bodies which are liable to collect decimate, and process personal information do have requirements for having a data privacy officer as per GDPR. Further research should be conducted with interviews and interaction with such authorities to understand and analyze in a deeper way on how the regulations are affecting innovations in different countries at the same time how the situation can be improved and what measures should be adopted to have a more compliant society with more compliant institutions public or private.

References

[1] R. P. Maradana, R. P. Pradhan, S. Dash, K. Gaurav, M. Jayakumar, and D. Chatterjee, "Does innovation promote economic growth? Evidence from European countries," *J. Innov. Entrep.*, vol. 6, no. 1, p. 1, Jan. 2017, doi: 10.1186/s13731-016-0061-9.

[2] W. Christl, "HOW COMPANIES USE PERSONAL DATA AGAINST PEOPLE," 2017.

[3] "Data protection," Jun. 04, 2021. https://commission.europa.eu/law/law-topic/data-protection_en (accessed Feb. 23, 2023).

[4] B. Yuan and J. Li, "The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation," *Int. J. Environ. Res. Public. Health*, vol. 16, no. 6, Art. no. 6, Jan. 2019, doi: 10.3390/ijerph16061070.

[5] J. Ruohonen and K. Hjerppe, "The GDPR enforcement fines at glance," *Inf. Syst.*, vol. 106, p. 101876, May 2022, doi: 10.1016/j.is.2021.101876.

[6] P. Quinn, "Research under the GDPR – a level playing field for public and private sector research?," *Life Sci. Soc. Policy*, vol. 17, no. 1, p. 4, Mar. 2021, doi: 10.1186/s40504-021-00111-z.

[7] "GDPR Enforcement Tracker – list of GDPR fines." http://www.enforcementtracker.com (accessed Feb. 12, 2020).

[8] "beslut-tillsyn-aleris-sjukvard-di-2019-3844.pdf." Accessed: Mar. 10, 2023. [Online]. Available: https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-aleris-sjukvard-di-2019-3844.pdf

[9] "beslut-tillsyn-aleris-narsjukvard-di-2019-3842.pdf." Accessed: Mar. 10, 2023. [Online]. Available: https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-aleris-narsjukvard-di-2019-3842.pdf

[10] "ICO sets out revised approach to public sector enforcement," Jul. 08, 2022. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/ico-sets-out-revised-approach-to-public-sector-enforcement/ (accessed Feb. 23, 2023).

[11] F. Prasser, J. Eicher, H. Spengler, R. Bild, and K. A. Kuhn, "Flexible data anonymization using ARX – Current status and challenges ahead," *Softw. Pract. Exp.*, vol. 50, no. 7, pp. 1277–1304, 2020, doi: 10.1002/spe.2812.

[12] C. Pearson, N. Seliya, and R. Dave, "Named Entity Recognition in Unstructured Medical Text Documents." arXiv, Oct. 14, 2021. Accessed: Mar. 10, 2023. [Online]. Available: http://arxiv.org/abs/2110.15732.

Biographies

Aaloka Anant is the founder of MAYA Data Privacy Limited, based out of Ireland. Company enables organizations to use data in a better way, complying with GDPR and other privacy regulations. He has held leadership and senior positions in SAP and Honeywell since 2004 and also worked with start-ups like Idea Device Technologies, MovidDLX, NGeneR and co-founded a non-profit organization Anant Prayas.

He is a researcher at CTIF Global Capsule, Aarhus University, Denmark since October 2019. He attained his Post Graduate degree in Enterprise Management from Indian Institute of Management Bangalore and B.Sc in Electronics and Communication Engineering from BIT Sindri in India. He teaches students for Masters program in Data Science as Associate Lecturer in National College of Ireland, Dublin and has taught previously at Furtwangen University, Germany. He is actively pursuing research on the topic of Privacy Preservation. His work focusses on new approaches for privacy preservation of Enterprise data and missing technology and structural framework for achieving end-to-end data privacy.

Ramjee Prasad, Life Fellow IEEE, Fellow IET, IETE, and WWRF, is a Professor of Future Technologies for Business Ecosystem Innovation

(FT4BI) in the Department of Business Development and Technology, Aarhus University, Herning, Denmark. He is the Founder President of the CTIF Global Capsule (CGC) and Founder Chairman of the Global ICT Standardisation Forum for India.

He has been honoured by the University of Rome "Tor Vergata", Italy as a Distinguished Professor of the Department of Clinical Sciences and Translational Medicine. He is Honorary Professor of University of Cape Town, South Africa, and University of KwaZulu-Natal, South Africa. He has received Ridderkorset af Dannebrogordenen (Knight of the Dannebrog).

He has received several international awards such as: IEEE Communications Society Wireless Communications Technical Committee Recognition Award.

He has published more than 50 books, 1000 plus journal and conference publications, more than 15 patents, over 145 PhD Graduates. Several of his students are today worldwide telecommunication leaders themselves.