International Journal of Information Systems and Project Management

Volume 9 | Number 1 Article 3

2021

An analysis of violations and sanctions following the GDPR

Wanda Presthus
Kristiania University College

Kaja Felix Sønslien
Sopra Steria

International Journal of
Information Systems and Project Management
ISSN (print):2182-7796, ISSN (online):2182-7788, ISSN (cd-rom):2182-780X
Available online at www.sciencesphere.org/ijispm

An analysis of violations and sanctions following the GDPR

Wanda Presthus
Kristiania University College
Kirkegaten 24-26, 0153 Oslo
Norway
wanda.presthus@kristiania.no

Kaja Felix Sønslien
Sopra Steria
Biskop Gunnerus gate 14 A, 0195 Oslo
Norway
kaja.sonslien@soprasteria.com

Abstract:
This paper investigates the violations and sanctions that have occurred following the implementation of the General Data Protection Regulation (GDPR). The GDPR came into effect in May 2018 with the aim of strengthening the information privacy of European Union/European Economic Area citizens. Based on existing taxonomies of (i) potential consequences of violating the GDPR (including surveillance, discrimination), (ii) an analysis of 277 sanctions, and (iii) interviews with experts, we offer a mapping of the violations and sanctions almost two years after the regulation was implemented. The most typical complaints were, in descending order: unlawful processing and disclosure of personal information, failure to act on and secure subject rights and personal information, and insufficient cooperation with supervising authorities. Our analysis also indicates an increasing number of fines over time. Regarding size, the fines range from 50,000,000 euros to (symbolic?) 90 euros. While research on GDPR violations and sanctions is somewhat scarce, our study mainly confirms existing findings: that the GDPR is complex and challenging. However, our study provides insight on some of the challenges. Our contribution is mainly practical and aimed at managers in any organization whose goal is to protect information privacy and to learn from the mistakes made by other companies. We also welcome more research on the topic.

Keywords:
privacy; General Data Protection Regulation; GDPR; data management; violations; sanctions.

DOI: 10.12821/ijispm090102

Manuscript received: 14 May 2020
Manuscript accepted: 22 February 2021

1. Introduction

Our society has undergone many revolutions, from steam engines and electricity to the introduction of information systems and social media. New and rapid technological advances merge the physical, digital, and biological worlds. It is easy for companies to collect, store and use data about individuals, and the amount of data available is growing at an astounding rate [1, 2]. At the same time, the importance of regulations concerning individual privacy is increasing [3]. '*The right to be let alone*' was declared in 1890 by Warren and Brandeis as they saw the need for laws to protect individuals [4]. While many researchers refer to Warren and Brandeis, few mention that is was the portable camera that activated this concern [5]. Approximately one century later, Weiser argued that technology could enable firms to make unpleasant use of the information they collect [6]. Technology is advancing faster than the law [5] and human perception [7], and the vast amount of consumer data allows for its unprecedented use for business purposes [8].

One example of the most comprehensive information privacy violations was revealed in March 2018—the Facebook-Cambridge Analytica case. Personal information of up to 87 million Facebook users globally was collected without their consent. It is alleged that this information was used to target individuals in various campaigns, with positive outcomes for those using the data. The information has been linked to, for example, the US presidential campaign in 2016 [9], the Kenyan elections in 2013 and 2017 [10] and Brexit in 2016 [11].

Over the years, privacy has become deeply intertwined with technology [12]. Consequently, the European Commission proposed the General Data Protection Regulation (GDPR) in 2012, and it was approved by the European Parliament and the European Council in 2016. It was to be enforced on May 25, 2018 but was delayed until July 1, 2018 in European Free Trade Association (EFTA) states. However, it was *'the most lobbied against legislation in European history, with almost 4,000 amendments'* [13 p. 24, 14]. This might be a result of the demands placed on companies, as the GDPR regulates what and how they can use and process information. Ultimately, this can affect how they conduct their business and can lead to major changes in business models to ensure survival. The GDPR seems a good idea on paper, but it is difficult to comply with [3]. Concerns have been expressed in the US, where regulations resembling the GDPR are being enforced in states such as California and New York. Companies fear that it will be impossible to comply with a patchwork of multiple regulations [7]. Despite these obstacles, the GDPR is referred to as setting a global standard for privacy [13].

The sanctions for violating the GDPR can be substantial, and some have already been enforced. These include the epoch-making examples of large fines levied against Google in France [15] and against a German real estate company [16]. However, any company that collects customer data belonging to the European Union (EU) or the European (EEA) must comply with the GDPR regardless of size (small or large), type (profitable or non-profit) or nationality (European or non-European). Moreover, if they do not collect customer data, the company probably has a website, and websites must comply with the GDPRs rules regarding cookies and the right to forgotten for visitors from the EU and the EEA [17]. However, complying with the GDPR is not without challenges [18] and our research question pertaining to this is *What types of violations and sanctions have occurred following the implementation of the GPDR?*

The remainder of this paper is structured as follows. Section 2 covers related research on information privacy and the GDPR. Section 3 describes how we collected and analyzed our data. Sections 4 and 5 detail the study findings and limitations and discusses future research opportunities. The conclusion in presented in Section 6.

2. Related Research

This section presents related research on information privacy and frameworks, followed by a brief presentation of the GDPR in an information systems context. However, there are also some references to juridical publications.

2.1 Information privacy

The need for privacy protection was established even before advanced technology [4], and currently the common definition is the ability for one to control information about oneself. However, according to Solove *'Privacy seems to be about everything, and therefore it appears to be nothing'* [19]. When talking about privacy, it is often related to our fears and anxieties. What seems to be missing is the translation of why privacy problems are harmful, which makes it difficult for companies to develop policies and attempt to solve the issues [19]. Solove developed a taxonomy to address these problems that consist of four main harmful activites: information collection, information processing, information dissemintation and information invasion. For this paper, we found that Solove's taxonomy covered most of our scope; however, Solove does not specifically include actors such as *Authority* outside a company or *Controller* within a company. This might be because Solove's point of departure is the data subject and because the GDPR was yet to be implemented. Therefore, we examined the work of Colesky et al. [20], whose point of departure is the organization. As shown in Fig. 1, the two frameworks overlap nicely with the data subject, which we illustrate by means of the dotted circle. We also observe that Colesky et al. [20] offer some solutions to reduce harmful actions, which are to separate, hide, abstract, and minimize data.

Our purpose for connecting the two frameworks is to illustrate the complexity of information privacy, but also to provide an overview when presenting the GDPR in the next section. For example, *Authority* in Fig.1 can be a country's data protection authority or a law firm. It is the country's data protection authority that will issue the sanction. The *Controller* typically represents the management of a company, however, it can also be an individual person, as we will demonstrate in the discussion. Finally, the *Data Subject* is the individual, who is to be protected by the GDPR, for example in the role as a consumer, web-browser, or a citizen of the EU/EEA.

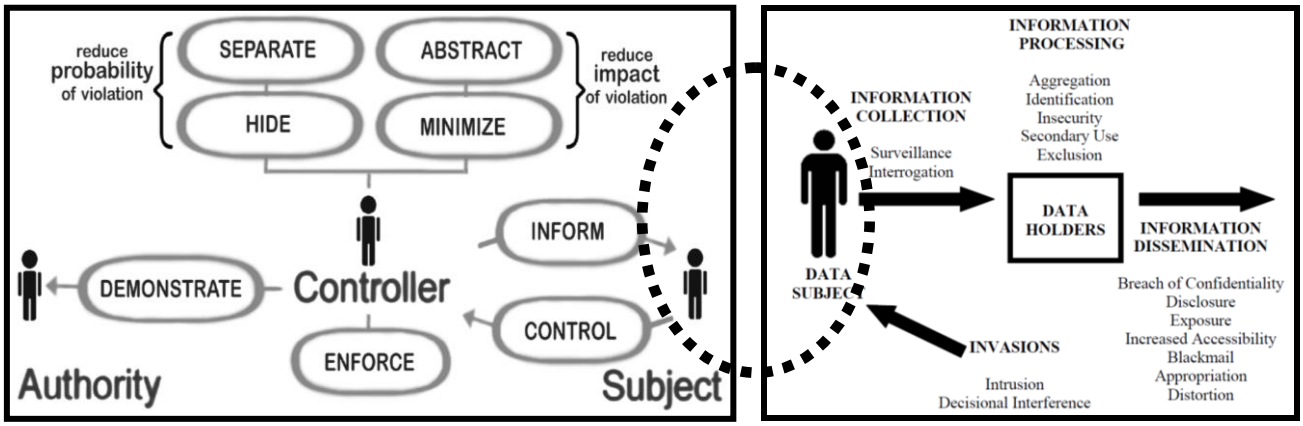


Fig. 1. Our illustration (dotted circle) of the overlap of frameworks by [20 p. 39] and [19 p. 490].

2.2 The General Data Protection Regulation (GDPR)

The GDPR was enforced after six years of preparation and debate. It supersedes various privacy regulations in EU and EEA countries, with the main changes being extended territorial scope, new definitions (for example data portability), new provisions and principles (for example data minimization) and added conditions concerning children's consent [21]. The role of national data protection authorities is strengthened, as they can impose substantial penalties on those who infringe data subject rights of up to 4% of global turnover or 20 million euros, whichever is higher [7, 21, 22]. A

survey of 62 companies in 2018, right before the GDPR was implemented, revealed some confusion about the penalty. One participant pondered:

> *"I do not understand how to calculate this fine. It reads:* 'up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher'. *How this could ever be more than €20 million is beyond my comprehension"* [22 p. 10].

The fine can indeed be above 20 million euro. The aforementioned survey asked the companies to calculate the amount of a hypothetic fine. The paper reported that the highest amount could be as much as €1 666 892 392 (almost 1,7 billion euro) and another company found it to be as low as 400 euro. These results demonstrated large differences, both in terms of revenue and economic consequences for the companies who partook in the survey.

The implementation of the GDPR entails benefits in addition to challenges for companies. A literature review identifies several benefits including risk identification, better data management, security measures, and training awareness [18]. However, the digital revolution has led to a lag between existing regulations and how they are practiced [23]. Regulations are often so overwhelming that they tend to scare organizations away from creating new business. For regulations to be successfully implemented and enforced, Dunlap, Cummings and Janicki [24] state that authorities should provide sufficient expertise. Koops argues that this has not been done. What the GDPR does in practice is to make data protection more complicated with ambiguous phrasing and complex dependencies between some of the articles [3]. Koops further argues there is a disconnection between law and reality. Concurring with this, Tikkinen-Piri, Rohunen and Markkula [25] and Mansfield-Devine [26] argue the GDPR does not 'spell out' what companies need to do to become compliant.

Existing research has started to pay attention to violations, but also inventive ways to avoid complying to the regulation. For example, one study reveals that web sites do not offer a proper way to opt out of cookies, and some websites simply refuse access users in the EU [27]. A related study claims that Internet usage has indeed improved privacy rights but mostly for EU citizens and less for US citizens [17]. For example, the empirical study by Dabrowski et al. found that EU citizens are less likely to receive persistent cookies. Sanchez-Rola et al. [27] state that:

> '*From an economic point of view, stakes are big: on the one hand, fines imposed because of non-compliance to the GDPR can be very large; on the other hand, though, the main source of income of many websites is advertising, and we speculate that […] letting users easily opt out from tracking could negate them a part of their income that could potentially be even larger than the fines they could face. Uncertainty with respect to the scope of the legislation and the likelihood of it being enforced may also be involved*' [27 p. 10].

Tambou [15] states that the fine imposed by the French Data Protection Authority on January 21, 2019 was not the first. However, the significant amount of 50 million euros demonstrated the effect of the GDPR and can be representing a paradigm shift. Tambou describes how Google tried to argue against the fine but in vain [15]. A preliminary study by [28] aims at developing a conceptual framework of privacy violations.

Researchers outside the European border are also taking a greater interest in the GDPR. For example, [29] explores the beneficial and questionable consequences of advanced technology, and [7] have suggested several solutions, such as algorithmic transparency and the creepiness scale. The creepiness scale puts the data subject in focus when it comes to companies' use of personal data and algorithms. Watson and Nations [7] categorized the data subjects' reaction from "this is helpful"; "this is creepy"; "this is so wrong". For example, when LinkedIn uses algorithms to match job recruiters and applicants it is perceived as helpful, but if companies use algorithms to screen job applicants based on analyzing their smile it is perceived to be wrong. It should be mentioned that use of algorithms and automated decision making is not illegal per se, however a company must inform the data subject that algorithms (may) have affected the outcome.

Another study from the data subjects' (in this case as the role of consumers) perspective was conducted by [30]. Based on a survey, three insights were gained in the wake of the implementation of the GDPR: (1) consumers had increased knowledge about their information privacy; however, they remained rather unconcerned about executing their enhanced rights. (2) About 50% of respondents felt that they had control of their personal data, while almost 40% stated that they had no control over their personal data. (3) The consumers had trust in companies' management of their personal data.

Summing up the existing research, we observe an increased interest in information privacy and the GDPR. So far, most researchers agree that the aim of the GDPR is positive but that the regulation is challenging for organizations. There are several studies on the potential harmful consequences of the lack of privacy, and many conceptual frameworks exist. Because the GDPR is relatively new, less research has addressed violations and sanctions. We aim to fill this gap.

3. Method

This is mainly a qualitative study, and we collected data from three main sources. First, a review of related research was conducted between 2018 and 2020, resulting in our theoretical framework (Fig. 1, presented above). Second, interviews with four experts were conducted in 2018 and repeated in 2020 (three of them answered). We also e-mailed two other juridical professionals in 2020 because some questions arose from our findings. Third, an analysis of violations and sanctions based on two official websites was conducted from January 1 to April 1, 2020.

Table 1. Summing up our sources of qualitative data collection

Data source	Date conducted	Outcome
Related research	2018 and 2020	Theoretical framework based on Colesky et al. [20 p. 39] and Solove [19]. The framework is found in Fig. 1 in section 2.
Interviews with 4 experts	2018 and 2020	Seven interview transcripts.
Juridical advice from 2 professionals	2020	Two e-mail transcripts, in order to shed additional light from our findings.
2 different websites	2020	Analysis of 277 GDPR violations and sanctions.

3.1 Collection and analysis of the four expert interviews in 2018 and 2020

In spring 2018, right before the implementation of the GPDR, we conducted four interviews with experts in their fields. They were chosen based on their diverse roles and relevance vis-à-vis the GDPR, allowing us to illuminate the regulation from a broad perspective. All four participants granted us permission to refer to them by professional title:

1) General Secretary, The Norwegian Computer Society
2) Lecturer and privacy researcher, University of Oslo
3) Advocate, specialist in technology and privacy
4) Commissioner, The Norwegian Data Protection Authorities

The interviews in 2018 were conducted face to face between March 8 and April 13 and lasted between 30 and 40 minutes. All the participants agreed to having the interviews recorded, and they received the transcripts the following day. The recordings were deleted immediately after approval. The semi-structured interview questions, which are based on the existing research in Section 2, covered the following:

1) What are the expected advantages and disadvantages of the GDPR?
2) Is the GDPR about security or privacy?
3) What kind of impact will the GDPR have on data subjects and organizations?
4) What do you think about the sanctions and authority control?

Based on our observation of the many violations and sanctions in the wake of the implementation, we wanted to obtain more insight. We contacted the same four experts, who were happy to share their knowledge with us. The follow-up interviews with the same participants in February 2020 were conducted by e-mail, and the answers were returned the same way. Three participants provided thorough answers, while the fourth apologized for not being able to participate. The essence of the follow-up questions was as follows:

1) Are you surprised by the violations, and do you see any patterns?
2) Are the sanctions fair?
3) What are the benefits/challenges for the data subjects after the implementation of the GDPR?
4) Does the hysteria around the GDPR prevail?
5) Has the GDPR had the intended effect on organizations and data subjects?

The analysis of the transcripts was guided by the themes of the questions, but we also made clusters by creating a matrix and reducing the text, as suggested by Miles and Huberman [31].

3.2 Collection and analysis of the two websites on GDPR violations

As of April 2020, there are several websites that offer an overview of the violations and sanctions following the implementation of the GDPR. To compare the results, we chose two websites: *GDPR Fines Tracker & Statistics* (https://www.privacyaffairs.com/gdpr-fines/) (left side in Fig. 2) and *GDPR Enforcement Tracker* (https://www.enforcementtracker.com/) (right side in Fig. 2). *The GDPR Enforcement Tracker* was also recommended by the advocate. This website allows filtering by country or choosing from among the 99 GDPR articles.

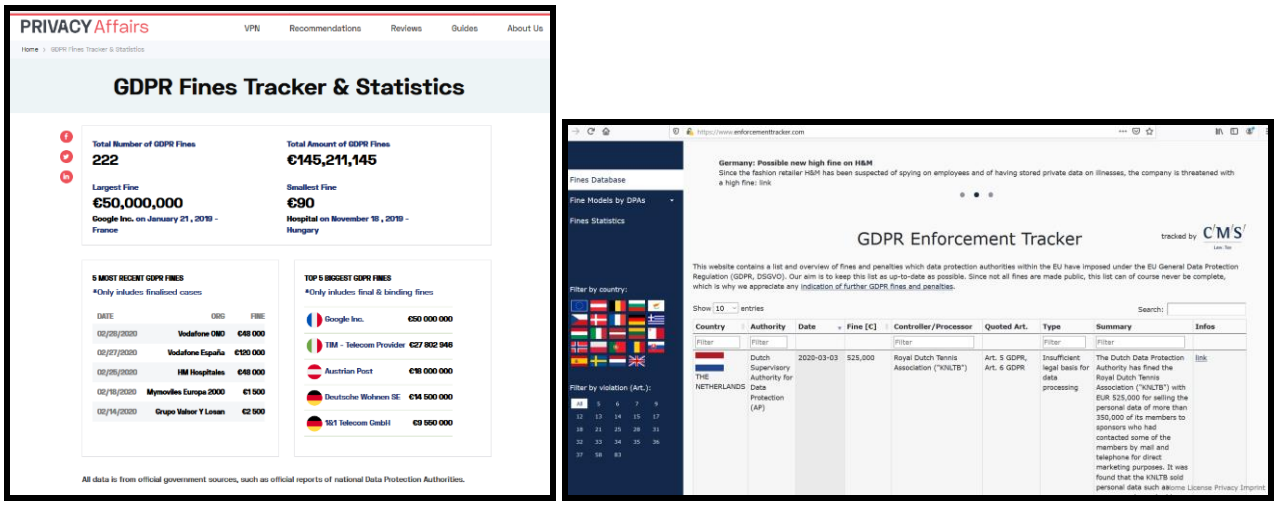


Fig. 2. *GDPR Fines Tracker & Statistics* and the *GDPR Enforcement Tracker*. Screen shots taken on March 9, 2020 and March 4, 2020, respectively.

Both websites offer structure and search function, but we wanted an in-depth analysis and a comparison. First, we only included the fines that were reported on both websites (Fig. 2). This excluded 23 cases; 15 were listed on *The Enforcement Tracker* but not *The Fines Tracker & Statistics*, and 8 vice versa. We also excluded fines that were not settled by March 31, 2020, such as those levied against Marriott International and British Airways. Another issue was that some of the fines had been based on multiple privacy breaches. In those cases, we clustered according to the largest breach.

Second, we manually loaded the content from the two websites into a Microsoft ® Excel sheet. This allowed us to use Excel's filtering, searching and visual graphics in order to analyze and cluster the data. Thus, all figures in Section 4 are

our creation. The clusters were identified by means of selected GDPR articles, in addition to simple cluster techniques facilitated by reducing text [31] and creating small tables. Our goal was to pinpoint the concreate violation. For example, where the website read: "Failure to comply with processes principles", our analysis would divide this into "failure to act on subject request" and "unlawful processing of personal information".

3.3 Summing up the methods section

Our method for this whole study was guided by the *ladder of abstraction* from Carney (1990), cited in [32]. The researcher climbs the three main steps of the ladder by summarizing the data and identifying themes and trends before trying to explain the findings. This ladder proved useful for our study; however, it is worth mentioning that several iterations were made between steps 2 and 3, as illustrated in Fig. 3.

Step 3 (constructing an explanatory framework) New insights and confirmation of Colesky et al. (2016)'s and Solove's taxonomies (2006)	**Sections 4-6 in this paper:** Findings, Discussion and Conclusion
Step 2 (identifying themes and trends) Themes: clusters of violations, insights from experts Trends: increasing academic interest in privacy, increasing number of sanctions in the industry	**Sections 4 and 5 in this paper:** Findings and Discussion
Step 1 (summarizing and packaging data) Common traits of existing frameworks, interview transcripts in tables, matrix based on the website findings	**Section 3 in this paper:** Method

Fig. 3. Our complete method using *the ladder of abstraction* [32]

4. Findings

In this section, we present our findings from the interviews and from the analysis of the websites.

4.1 The interviews with experts pre-GDPR in 2018

In general, all four experts were positive about the coming GDPR and saw it as a necessity to increase awareness of privacy. The General Secretary of the Norwegian Computer Society argued that the handling of personal information had been inadequate, as '*companies do not have a conscious relationship to the information they actually have*'. In addition, supervision by the authorities had been lacking, and the '*GDPR makes people aware of this*'.

We observed that the various roles of our participants may have influenced some of their answers. For example, the General Secretary of the Norwegian Computer Society and the Commissioner of the Norwegian Data Protection Authorities had different perspectives on the regulation itself. While the Commissioner argued that it is a '*well written regulative*', the General Secretary claimed that the GDPR had been rushed through. Despite this, the General Secretary *loved* the citizen aspect of the regulation; however:

> '*The problem is that individual citizens really don't have a clue about it…[…]…Some of the articles you can read 2000 times, and still not get any wiser*' and '*I hope this [GDPR] leads to increased attention towards person value, but I believe the changes will be less significant than they should be*'.

The lecturer and privacy researcher at the University of Oslo agreed that even though the GDPR is better than the prior Privacy Act (in Norway), the phrasing is still obscure, making it difficult to '*give precise advice on the regulation*'. The lecturer also emphasized how the GDPR should have been more explicit: '*they have tried to ensure that there is some room for courts of law to create precedence in some areas. By making it a bit vague, they make this possible*'. The advocate stated that '*It is not possible to make a distinct regulation, because it will not be able to cover everything*'.

Regarding the fairness of the sanctions, the participants agreed on the necessity. The Commissioner of the Norwegian Data Protection Authorities stated that '*Sadly, there has to be a possibility of sanctions. If not, there is no leverage to ensure the fulfilment of regulations*'.

4.2 The interviews with experts following the GDPR in 2020

As mentioned above, we were able to conduct a follow-up interview with three of the four experts. None of them were surprised by the number of breaches and had expected more, but they suspected that not all violations are reported. According to the Commissioner of the Norwegian Data Protection Authority, '*a clear pattern of the cases is due to human error, poor training and lack of competence*'. The advocate was surprised that only two fines have been given in Norway as of February 2020. Regarding the fines, the experts perceive them as justified. The lecturer and privacy researcher points to the difficulty of *Article 17: The right to erasure* and points to the case in France with Google who defended itself based on this right (as also described by [15]). The commissioner says that it remains to be seen how the various data protection authorities will form a unified front.

In addition to the remaining difficulties with interpreting the regulation, all three experts agree that the GDPR has strengthened the rights of the data subject. The commissioner is pleased that more breaches are being reported, such as lack of access or lack of deletion. However, the advocate points to the cookie confusion on websites. This issue is addressed by existing research; however, the advocate sheds some new light, stating that:

> '*Gathering information about website users and customizing content and features on web pages is something most users probably want, but now there seem to be websites that completely refrain from collecting personal information. It is both unnecessarily from a legal point of view, and it impedes services offered and users' experience of websites and services. But this is a lack of understanding of the regulations, and not the GDPR itself*'.

4.3 The two websites for fines

Having scrutinized and compared the two websites, we present the following insights: (i) number of fines for each country, (ii) the size of the fines, (iii) clustering the five most frequent type of fines, and (iv) a timeline. Each insight is presented followed by an explanation.

Starting by the number of fines, we found that the total as of March 31, 2020 was 227. Fig. 4 shows that Spain has the most fines in Europe at 64. Lithuania, Malta, Croatia, and the UK account for one fine each.

Second, regarding the size of fines, the largest was given to Google in France (50,000,000 euros), while the smallest was given to a hospital in Hungary (90 euros). Google did not follow the principles of transparency, sufficiency of information and the presence of a legal basis. The hospital was fined for charging a copy fee and violating a patient's right to access data. A company cannot charge for a request for information, at least not for the first request [21]. In total, the sum of fines amounts to over 150,000,000 euros as of March 31, 2020.

Third, we carefully studied all 227 fines and clustered them into five main types (Fig. 5). Most of the fines were given for unlawful processing and disclosure of personal information; failure to act on and secure subject rights and personal information; and insufficient cooperation with supervising authorities. In two cases, the websites did not reveal the reasons for the fines (indicated as 'unknown' in Fig. 5). Following are the five clusters and some of the typical reasons for the fines:

1) unlawful processing of personal information: lack of legal basis of processing and lack of consent, especially regarding surveillance

2) disclosure of personal information: third parties acquired access to personal information without a legal basis or consent and publication of personal information on a company's website

3) failure to act on subject rights: failed to delete personal information upon subjects' request (subjects had not been informed about data processing)

4) failure to secure personal information: lack of organizational and technological measures, such as access management, securing containers and hacking prevention

5) insufficient cooperation with supervising authorities: company did not comply with measures imposed by the Data Protection Authority and refused to comply with the obligation to appoint a data protection officer

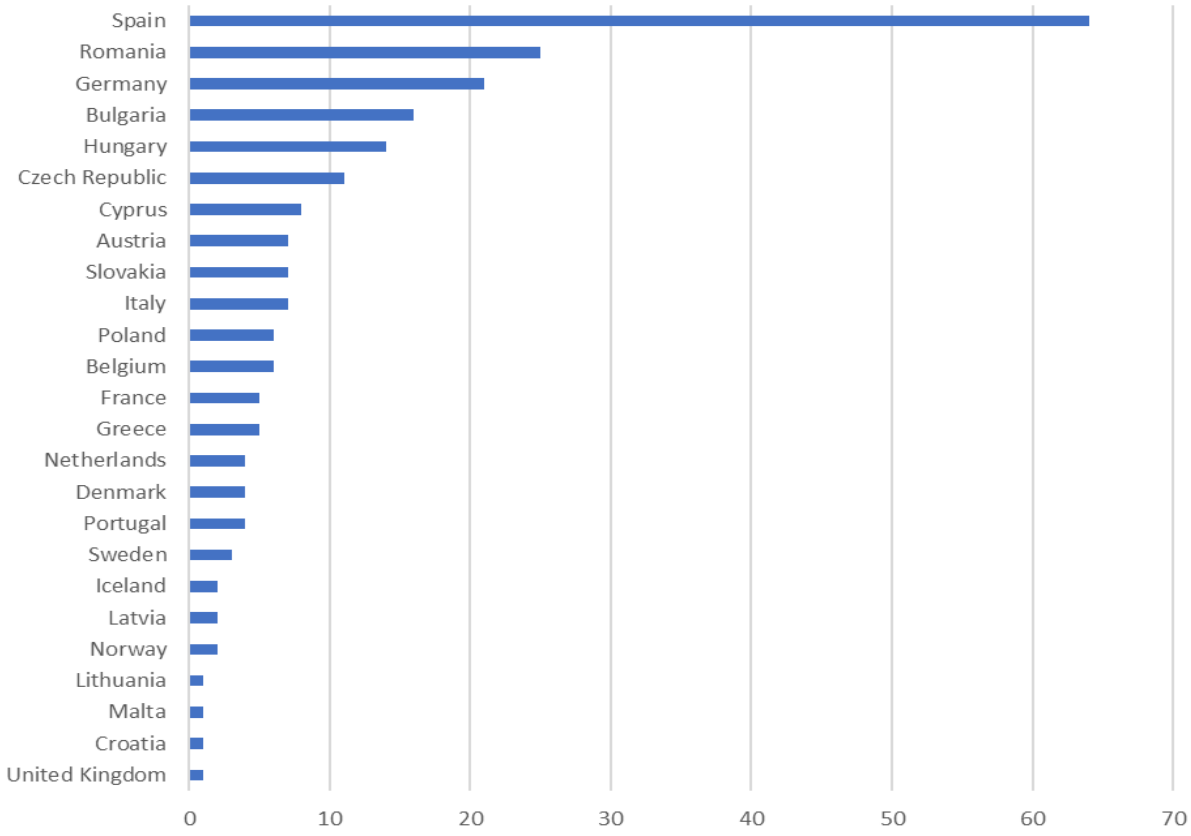


Fig. 4. Number of fines based on country

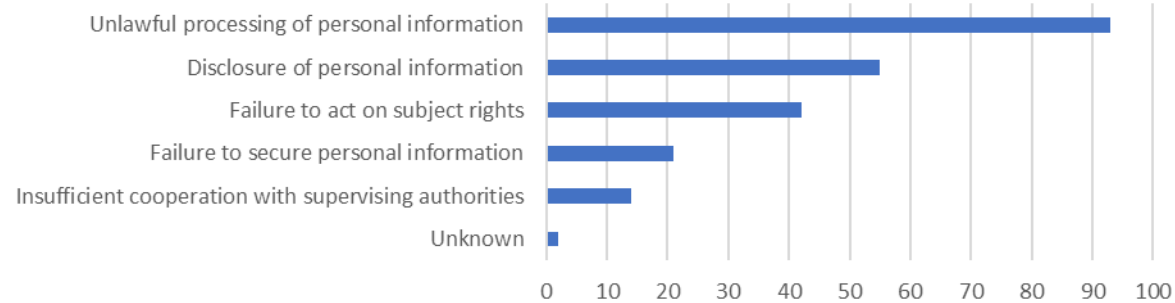


Fig. 5. Our clustering of the reasons for the 277 sanctions given as of March 31, 2020

From this clustering, we can also derive the most violated Articles of the GDPR (of which consists of 99 Articles and can be found here: https://gdpr-info.eu/). At the time of this study, the most frequently violated Articles were 5 and 6. Specifically, we found that Article 5, point (b): *Principles relating to processing of personal data* was most frequently violated. An excerpt of Article reads:

> '*…collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');…'* (https://gdpr-info.eu/).

Fourth, we created a trend line with dates of when the fines were given (Fig. 6). The graph starts in May 2018 when the GDPR came into effect and indicates an increase in fines over time (there were also 15 more fines, but the websites did not specify the dates and consequently they are omitted in this illustration).

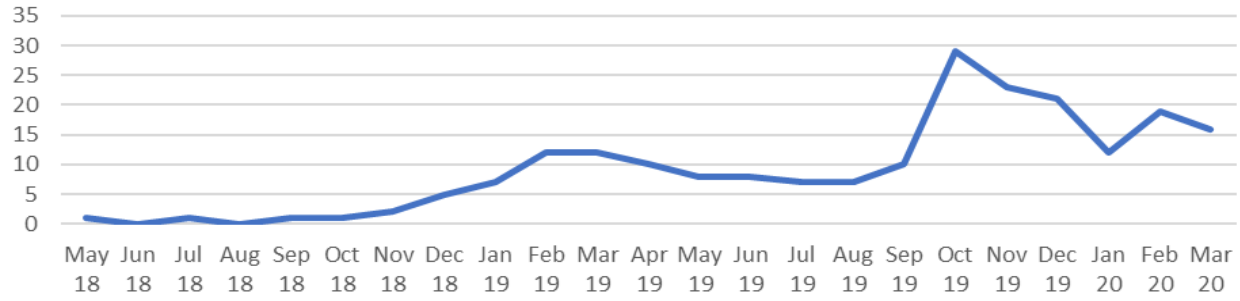


Fig. 6. Number of sanctions over time

5. Discussion

This section briefly discusses the findings from Section 4 and maps them against related research from Section 3. The four insights from the website analysis structures the section. The contribution is presented before pointing to limitations and suggested future research.

5.1 Number of sanctions for each country

According to the interviewed experts, the fines that have been given are not surprising, and they are justified. The experts mentioned that some fines may be the result of *'bad luck'* (at getting caught). For example, we do not believe that Spain is the 'bad seed' in Europe, despite the country's many sanctions. While we acknowledge that *'bad luck'* is probably not a favored term in research, it was nonetheless mentioned by the experts. The large diversity in the number of sanctions per country could also be explained by the fact that GDPR has replaced more than 40 privacy acts in European countries, thus a unified understanding is yet to be achieved. Koops [3] argues how this contributes to develop an incoherence between law and reality, and the advocate agreed and even claimed that parts of the regulation are '*not adjusted to the real-world (…) Some of the regulations is basically impossible*'. Both Koops and the advocate particularly referred to the articles on erasure.

5.2 The size of the fines

As presented in the Related Research, the potential size of fines can be substantial. Our findings range from Google in France (50,000,000 euros), to a hospital in Hungary (90 euros). The latter case makes us ponder, as most companies should be able to come up with 90 euros. Perhaps it was symbolic? The reason for the hospital fine was unlawful charging of a copy fee and for violating a patient's right to access data. These reasons are at least possible to rectify, which could be one reason for the low amount. Or, could it be due to the greater need of a hospital for Hungary: While

all of our experts agreed on the necessity of fines, they were equally unsure about the enforcement. According to the advocate, '*The Norwegian Data Protection Authority cannot give fines to everyone who is not totally compliant, that is impossible*'. With over 577,067 Norwegian companies (per 2018), the General Secretary argued that the Norwegian Data Protection Authority would lack the capacity to inspect all companies and had to prioritize the ones with sensitive personal data. Some of the participants argued that giving fines is the last solution; for example, the General Secretary said that '*because if they do so, it doesn't solve the problem itself*'. If a company gets a large fine, there is a risk of them becoming insolvent and sending employees to the Norwegian Labor and Welfare Administration, which is not beneficial for either the company or society. Therefore, the authorities will have to evaluate the consequences of imposing sanctions. However, the commissioner was certain that they would conduct signal audits, that is, using one company to set an example regarding the importance of the regulation.

On the one hand, existing research state that companies want to comply [22], but on the other hand, research also finds that the lack of resources as one of the biggest challenges for companies [18]. The General Secretary in the Norwegian Computer Society emphasized that '*unfortunately, I meet more and more people who say fuck it. They argue that they do not have the resources to prioritize it*'. The company attitude seemed to be that this issue was to be dealt with when or if it happened. The websites do not reveal whether warnings were given in all 277 cases we studied, so we cannot claim that warnings are always given before sanctions. However, we do observe several cases where the companies were given the possibility to rectify the situation but failed to seize the opportunity.

5.3 Clustering the five most frequent type of violations

We were somewhat surprised by the nature of the most frequent violations. From Solove's [33] taxonomy (right side of Fig. 1) the violations typically fall under *information collection* and *information processing*. Some of the reasons, according to the experts interviewed, might be complexity, lack of resources and lack of understanding, which has also been cited many times in the existing research. Despite this, we are puzzled. Should not some of these violations have been easily avoided? Why has so many failed to cooperate with the authorities? While some researchers have suggested that the emergence of big data would entail greater privacy risk (for example [29, 34]), our findings rather reveal that the violations are not necessarily rooted in big data.

In addition, from our own analysis of the websites we observe that private individuals have also been sanctioned. All seven of these cases related to 'non-compliance with lawful basis for data processing'. One case concerned disclosure of personal information, and the remaining six cases concerned surveillance (for example a trainer who filmed the team players in the wardrobe). Such surveillance can easily get out of hand. The Norwegian Data Protection Authority filed a complaint against a grocery store on February 28, 2020. The store manager filmed four under-aged people who stole, but this was not the problem. Rather, the violation was that the manager sent the film to an acquaintance, asking "Is this your son?" The mother replied "No, not my son" and forwarded the film to her son who then sent it to his classmates. Soon, the identity of the young shoplifters was exposed. The complaint, which can be read in full (Norwegian only) at https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-overtredelsesgebyr-til-butikk-tilknyttet-coop-finnmark/, does not include further discussion about the mother or the children who forwarded the film. We asked the juridical advisor at the Norwegian Data Protection Authority about the responsibility of the mother. The juridical advisor admitted that the Authority must prioritize their resources, but the most important issue was to target the data controller, which was also explained by the second juridical expert. This case, which was not settled at the time of publishing this study, is an example of the complexity of the GDPR's many articles, roles [20] and stakeholders, including the grocery store, the Data Protection Authority, the mother and the children. Whether the mother should have forwarded the video or whether she is to be considered as a data controller is beyond the scope of this paper.

We had expected more cases related to cookies and automated decision making [7]. One reason can be that it is easier to discover and prove that "you are filming me in the wardrobe" versus calling up your bank and claim "your algorithms are discriminating me".

5.4 Dates and timeline of sanctions

Our graph reveals a spike in October 2019, but we do not know the reason for this. One possibility is that the authorities accumulate the cases and settle them at the same time. Another possibility lies in the reply from one of the experts interviewed, who said that perhaps the countries are awaiting each other's actions. This spike aside, the graph indicates an increase in sanctions. Our graph may also demonstrate that the sanctions given in the wake of the GDPR have strengthened the rights of the data subject and increased the responsibilities of companies. However, both our expert interviews and related research agree that there are challenges associated with human interpretation of the regulations. It will be interesting to follow the trend of the graph in the future. We are only humble researchers, but we hope that this study provides insights to companies. Our implications for controllers are provided in Table 2 in the next section.

5.5 Contributions, limitations, and suggested future research

Our contribution is mainly for practitioners, as we offer a mapping of the violations and sanctions following the GDPR up to March 31, 2020. Table 2 presents the top five most common violations and our comments on what companies can do to learn from other's mistakes. We acknowledge that the comments are abstract, but they are based on real-life sanctions.

Table 2. Our main findings and implications for the controllers

Violations identified in our study	**Comments on implications for the controllers**
Unlawful processing of personal information	It is worth the effort to obtain control over the data being processed. Based on our study, this is a good place to start.
Disclosure of personal information	Our study does not indicate that disclosure was deliberate; rather, it appeared accidental in most cases.
Failure to act on subject rights	Establish routines for data management.
Failure to secure personal information	Gain knowledge or focus on how to protect personal data.
Insufficient cooperation with authorities	Follow the advice of data authorities, especially by ensuring routines and appointing a data protection officer (if needed). It should be easy to avoid a fine related to this type of violation.

Our study has several limitations, some of which are opportunities for future research. The first category is scope. The ethical aspects are beyond the scope of this study; we have focused only on juridical violations of the GDPR. In this regard, we have not paid attention to the potential non-monetary consequences of violating the GDPR. Existing research has mentioned loss of reputation [18], but more research should be conducted to determine what other impact receiving a fine might have on a company beyond monetary loss. For example, the Cambridge Analytica case resulted in a #deleteFacebook campaign, but the number of Facebook members still increases steadily [35]. Future studies can therefore investigate the effect of GDPR on the GAFA companies (Google, Amazon, Facebook, and Apple) and other large tech companies. Likewise, a study could be done on whether the GDPR has impacted companies' business models in general.

The second category regards our method. Starting with the most obvious, more in-depth case studies should be made on some of the cases from the websites we have analyzed. For example, we do not know the reason for the many violations of insufficient cooperation with authorities (as found in Table 2). Our first reaction was that this should be easy to avoid, but there may be reasons that are not listed in the websites. We also observe that some of the fines were reduced or completely withdrawn, but we did not investigate this further. It would be interesting to investigate if there are any typical actions that a company can take to make amends and reduce the impact once they have received an official complaint. Another limitation pertaining to our method is that our interviews were all conducted with Norwegian experts. We hope that future research can build on this article by interviewing similar respondents in Europe, but also in the USA where comparable laws and regulations are emerging. Finally, we welcome future researchers to duplicate and/or build on our analysis so that either confirmation and/or contraction can be made.

6. Conclusion

This explorative study has investigated the research question *What types of violations and sanctions have occurred following the implementation of the GPDR?* Based on an analysis of 277 violations and sanctions, we identified five main violations:

1) unlawful processing of personal information
2) disclosure of personal information
3) failure to act on subject rights
4) failure to secure personal information
5) insufficient cooperation with supervising authorities

Regarding the scope of the sanctions, the fines range from 50,000,000 euros to (perhaps symbolic?) 90 euros. Based on interviews with experts, the reasons range from companies saying: *'let's risk it'*, via wanting to protect information privacy but failing to understand the 99 articles of the GDPR, to simply poor data governance. We have addressed the implications for the companies in Table 2. Our contribution is mainly practical and aimed at managers in any organization whose goal is to protect information privacy and to learn from the mistakes made by other companies.

However, we argue that every actor - whether it be the authority (data protection authority), the controller (the company or processor) or the data subject (the individual) - has a responsibility. By analyzing and mapping the violations and sanctions, we hope that our study can contribute to a better understanding of the GDPR, both for the industry and academia. Albeit our study confirming existing research of the challenges of complying with the GDPR, the issues addressed in this paper should remain interesting to researchers in the future, as our findings indicate an increase in violations and sanctions.

Acknowledgements

We thank the experts who have provided us with valuable insights. Gratitude also goes to the editor and to the anonymous reviewers of International Journal of Information Systems and Project Management (IJISPM) who helped improve the quality of this study. We deeply appreciate their time, honesty, and effort.

References

[1] P.A. Pavlou, "State of the information privacy literature: where are we now and where should we go?," MIS Quarterly, vol. 35, no. 4, pp. 977-988, December, 2011.

[2] R.K. Rainer and C.G. Cegielski, Introduction to Information Systems. Singapore: John Wielt & Sons, 2013.

[3] B.-J. Koops, "The trouble with European data protection law," International Data Privacy Law, vol. 4, no. 4, pp. 250-61. November 2014.

[4] F. Bélanger and R.E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," MIS Quarterly, vol. 35, no. 4, pp. 1017-1041. December, 2011.

[5] D.J. Solove. (2020, January 26). Privacy + Security Blog. News, Developments, and Insights [Online]. Available: https://teachprivacy.com/cartoon-the-history-of-privacy/

[6] M. Weiser, "The Computer for the 21st Century," Scienfitic American, vol. 265, no. 3, pp. 94-105. July,1991.

[7] H.J. Watson and C. Nations, "Addressing the Growing Need for Algorithmic Transparency," Communications of the Association for Information Systems, vol. 45, no. 1, pp. 488-510. January, 2019.

[8] W. Presthus, "Catch Me If You Can! How Technology is Running Away from Ethics in Business Intelligence," NOKOBIT - Norsk konferanse for organisasjoners bruk av informasjonsteknologi, Bodø, Norway, 2012, pp. 91-104.

[9] P. Lewis and P. Hilder, (2018, March 23). Leaked: Cambridge Analytica's blueprint for Trump victory [Online]. Available: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory/

[10] J. Moore. (2018, March 20). Cambridge Analytica Had a Role in Kenya Election, Too [Online]. Available: https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html/

[11] E. Power. (2019, July 24). The Great Hack: The story of Cambridge Analytica, Trump and Brexit [Online]. Available: https://www.irishtimes.com/culture/tv-radio-web/the-great-hack-the-story-of-cambridge-analytica-trump-and-brexit-1.3965788/

[12] U. Gasser, "Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy," Harvard Law Review Forum, vol. 130, no. 2, pp. 61-70. December, 2016.

[13] Evry, "Trust in the Personal Data Economy From GDPR compliance to opportunity: How giving individuals control over their personal data unlocks new business opportunities," Whitepaper, pp. 1-54, 2017.

[14] L. Schildberger. (2016, May 30). Lobbying and its influence on the draft of a General Data Protection Regulation of the European Union unveiled in 2012 [Online]. Available: https://www.law.tuwien.ac.at/Schildberger_Einreichversion.pdf/

[15] O. Tambou, *Lessons from the First Post-GDPR Fines of the CNIL against Google LLC.* Eur. Data Prot. L. Rev., vol. 5, p. 80. January, 2019.

[16] C. Ritzer and N. Filkina. (2019 November 12). First multi-million GDPR fine in Germany: €14.5 million for not having a proper data retention schedule in place [Online]. Available: https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/

[17] A. Dabrowski, G. Merzdovnik, J. Ullrich, G. Sendera and E. Weippl, "Measuring cookies and web privacy in a post-gdpr world," International Conference on Passive and Active Network Measurement. Springer-Verlag, pp. 258-270. March, 2019.

[18] G.A. Teixeira, M.M. da Silva, and R. Pereira, "The critical success factors of GDPR implementation: a systematic literature review," Digital Policy, Regulation and Governance, vol. 21, no. 4, pp. 402-418. March 2019.

[19] D.J. Solove, "A taxonomy of privacy," University of Pennsylvania Law Review, vol. 154, no. 3, pp. 477-560. January, 2006.

[20] M. Colesky, J.-H. Hoepman, and C. Hillen, "A critical analysis of privacy design strategies," IEEE Security and Privacy Workshops (SPW), pp. 33-40. May, 2016.

[21] E. Jarbekk and S. Sommerfeldt, Personvern og GDPR i praksis. Cappelen Damm, 2019.

[22] W. Presthus, H. Sørum, and L.R. Andersen, "GDPR compliance in Norwegian Companies," NOKOBIT - Norsk konferanse for organisasjoners bruk av IT. Svalbard, Norway. 2018, pp. 1-15.

[23] J. Krystlik, "With GDPR, preparation is everything," Computer Fraud & Security, vol. 2017, no. 6, pp. 5-8. June, 2017.

[24] L. Dunlap, J. Cummings, and T. Janicki, "Information Security and Privacy Legislation: Current State and Future Direction," Conference of Information Systems Applied Research. Austin, Texas, USA. 2017, pp. 1-9.

[25] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," Computer Law & Security Review, vol. 34, no. 1, pp. 134-153. February, 2018.

[26] S. Mansfield-Devine, "Data protection: prepare now or risk disaster," Computer Fraud & Security, vol. 2016, no. 12, pp. 5-12. December, 2016.

[27] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P-A. Vervier, I. Santos, "Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control," Asia Conference on Computer and Communications Security, Auckland, New Zealand. 2019, pp.1-12.

[28] L.S. Flak, Ø. Sæbø, and P. Spagnoletti, "Privacy violations in light of digital transformation: insights from data breaches in Norway," Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy. Munich, Germany. 2019, pp. 1-7.

[29] K.E. Martin, "Ethical issues in the big data industry," MIS Quarterly Executive, vol. 14, no. 2, pp. 67-85, June, 2015.

[30] W. Presthus and H. Sørum, "Consumer perspectives on information privacy following the implementation of the GDPR," International Journal of Information Systems and Project Management, vol. 7, no. 3, pp. 19-34, May, 2019.

[31] M.B. Miles, "Qualitative Data as an Attractive Nuisance: The Problem of Analysis," Adminstrative Science Quarterly, vol. 24, no. 4, pp. 590-601. December, 1979.

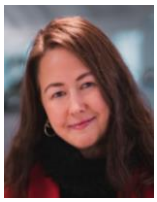
[32] M.B. Miles and A.M. Huberman, Qualitative Data Analysis, 2nd ed. Thousand Oaks: Sage Publications, 1994.

[33] D.J. Solove, "A taxonomy of privacy," University of Pennsylvania Law Review, vol. 154, pp. 477-560. January, 2006.

[34] P.B. Lowry, T. Dinev, and R. Willison, "Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda," European Journal of Information Systems, vol. 26, no. 6, pp. 546-563. November, 2017.

[35] Statista. (2019). Number of monthly active Facebook users worldwide as of 1st quarter 2018 [Online]. Available: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Biographical notes



Wanda Presthus
Wanda Presthus received her Ph.D. from Gothenburg University in Sweden and is an Associate Professor at Kristiania University College in Oslo, Norway. Her research interests include information privacy (how companies manage personal data and how individuals react), research methods (helping junior researchers conduct their research) and business analytics (to improve decision making).

Kaja Felix Sønslien
Kaja Felix Sønslien holds a Master of Science in Information Systems from Kristiania University College (formerly Westerdals Oslo ACT) and works as a senior consultant at Sopra Steria, in the fields of information security, risk, and privacy. Her interests include how organisations should continuously work to secure their values in the best way possible, and at the same time integrate security as a part of corporate governance.