Practitioners' Corner

An Economic Analysis of Appropriateness under Article 32 GDPR

*Annika Selzer, Daniel Woods and Rainer Böhme**

I. Introduction

While privacy laws establish obligations on organisations to protect the fundamental rights of individuals, they rarely provide explicit prescriptions about *how* to do so.[1] This forces organisations to balance the risk to privacy of data subjects against the costs of implementation options, such as technical and organisational measures (hereinafter 'privacy measures' or simply 'measures') or stopping processing personal data. Therefore, privacy laws often occupy a middle ground between prescribing appropriate privacy measures and allowing organisations to self-define what is appropriate. This approach creates uncertainty over which privacy measures to implement while also threatening penalties if the appropriate measures are not in place.[2] Uncertainty looms over aspects like which privacy measures to choose (see II. 1.), how much measures will cost directly and indirectly (see II. 2.), and what the likelihood and impact of a violation on the individual and the organisation is (see II. 3.). In addition, organizations may have to defend such decisions to regulators, which necessitates a structured approach with documented evidence.

Risk management is frequently prescribed as an appropriate decision-making framework. For example, the European Union's General Data Protection Regulation ('GDPR') specifically invokes the notion of a privacy risk assessment - the so-called *risk-based approach* of the GDPR[3] - when implementing privacy measures in accordance with Article 32 GDPR. Quantitative risk management promises a rigorous evidential approach, but the practical challenges involved in an economical quantification of privacy risk are less frequently considered. Within Article 32 of the GDPR, appropriate measures must mainly balance the following considerations: the state of the art; the costs of implementation (detailed analysis in III.), and the risks to the rights and freedoms of natural persons (detailed analysis in IV.).

With regards to the risks to the rights and freedoms of natural persons, the GDPR identifies severe risks as those that could lead to physical, material or non-material damage, eg where the processing may give rise to discrimination, identity theft or fraud, damage to the reputation, or any other significant economic or social disadvantage (Recital 75 of the GDPR). The consideration of state of the art serves to reduce the scope for decision-making to only those controls which are based on proven knowledge (see Section II 1).

Finally, implementation costs cover not only the costs of the initial implementation of a privacy measure, but also follow-up costs, such as regularly occurring operating and maintenance costs[4]. The GDPR

DOI: 10.21552/edpl/2021/3/15

* Annika Selzer is leading a research group for information law and interdisciplinary research at the Fraunhofer-Institute for Secure Information Technology SIT in Darmstadt (Germany); Daniel Woods is Post-Doc at the Security and Privacy Lab of the University of Innsbruck (Austria); Rainer Böhme is a Principal Investigator at the University of Münster (Germany) and a professor in the faculty of computer science and leads the Security and Privacy Lab of the University of Innsbruck (Austria). This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the German Federal Ministry of Education and Research within the project Edumida (16KIS1361K & 16KIS1363). Daniel Woods is funded by the European Commission's call H2020-MSCA-IF-2019 under grant number 894700. This paper was written during a two-month research stay at the Security and Privacy Lab of the University of Innsbruck in 2020. The author Annika Selzer thanks Rainer Böhme and the entire team of the Security and Privacy Lab for making this research stay possible.

1 Robert Kazemi, *The General Data Protection Regulation in Legal Consultation Practice* (Deutscher Anwalt Verlagm 2019) 95.

2 Cedric Burton in Christopher Kuner, Lee Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR) – A Commentary* (Oxford University Press, 2020) Article 32, 636; (n 1) 95.

3 Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer, 2017) 40.

4 Annika Selzer, 'The Appropriateness of Technical and Organizational Measures under Article 32 GDPR' (2021) 7 EDPL 7,124.

provides no practical guidance about how to balance abstract legal assets, epistemic and technical aspects, and economic costs.

This contribution answers these three issues with a case study rather than providing general answers that are antithetical to risk management.[5] It conducts a mixed-methods, quantitative risk assessment tailored to the question of *appropriate* privacy measures with reference to Article 32 of the GDPR. The quantitative risk assessment involves in-depth interviews with representatives of 27 organisations of varying sizes and from different industries conducted in order to estimate and validate the costs of implementing privacy measures considered state of the art under Article 32. Separately, the risk to data subjects is quantified via a secondary analysis of two databases of GDPR fines and compensation awards. Combining these two exercises represents - as far as apparent - the first documented risk assessment with reference to GDPR in the scientific literature.

Section II introduces the research design to explore appropriateness of state of the art measures with reference to Article 32 GDPR as well as the decision-making process in organisations. Section III quantifies the costs of implementing state of the art measures. These measures are intended to reduce the risk to data subject's fundamental rights, which will be estimated in Section IV. Section V discusses the decision factors in adopting privacy measures. Section VI explains the limitations of the findings, and Section VII offers conclusions.

II. Research methods

The approach taken identifies state of the art privacy measures (1.), estimates the associated implementation costs (2.), and then quantifies a proxy for the risk to data subjects (3.). This necessitates a multi-method research design which breaks down into a legal analysis, 27 structured interviews, and secondary analysis of two databases of GDPR legal actions.

1. Method to Assess State of the Art Privacy Measures

To assess the costs of the privacy measures, we first needed an assessment of the state of the art. For this, three exemplary legal requirements were chosen aligned with the requirements set out in Article 32 as a basis for the implementation of privacy measures, each of which can be implemented with one or more purely technical, purely organisational, and combined technical-organisational measures:

- personal data in emails needs to be transferred confidentially (1),
- employees need to know and follow relevant data protection statutes (2), and
- physical access to personal data needs to be restricted (3).

Then, the recommended state of the art measures to fulfill each of these three legal requirements were assessed through a legal analysis. Since the GDPR lacks a legal definition of the term 'state of the art', an analysis of the meaning of 'state of the art' in the context of the GDPR was needed. Based on the legal analysis of GDPR commentaries, 'state of the art' in the context of GDPR is understood as measures that are based on proven knowledge, of an advanced state of technical development, practical suitable, already mature and available for technical implementation, but did not yet necessarily have become established in practice.[6] Even when relying on this definition, it is not easy for organisations to be sure whether a measure is considered state of the art. Therefore, several recommendations on the state of the art of privacy measures, such as the recommendations of the European Union Agency for Cybersecurity, have been analysed to elaborate further on this.[7] As a result, a list of different individual state of the art measures was left that - either by themselves or in combination with other individual measures - can fulfill one of the above mentioned requirements. The list of measures (see Table 3-5 in Appendix) was used to carry out the cost evaluation. All measures quanti-

5 Gary Stoneburner, Alice Goguen, and Alexis Feringa, 'Risk management guide for information technology systems' (2002), NIST Special Publication 30, 41.

6 The legal analysis is summarised in Annika Selzer, 'The Appropriateness of Technical and Organisational Measures under Article 32 GDPR' (2021) 7 EDPL 1, 120-128.

7 ENISA and TeleTrusT, 'Guideline state of the art', <https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-02_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf> accessed 22 March 2021.

fied are considered state of the art as required by Article 32 of the GDPR. However, these measures should not be regarded as exhaustive.

2. Method to Evaluate the Costs of Implementing Privacy Measures

In order to understand the impact of risk-based laws, it is necessary to re-construct the risk-based decision at the level of the norm addressee. In this case, this involves collecting empirical data about the costs incurred in pursuing an appropriate level of privacy measures.

a. Assessing the Costs of Implementation

Initially the costs of implementation of the state of the art measures were assessed by carrying out interviews with a single organisation (Table 1). This was necessary because providers of privacy measures are only able to give details about their pricing models, without taking personnel and other costs into consideration that an organisation has when implementing the measures.

In addition to the interviews, the leading providers of individual privacy measures including their pricing models were determined through an online search. Based on this and the results of the interviews a table of individual measures and their estimated costs of implementation was established.

b. Validating the Costs of Implementation

In order to validate these costs, structured interviews with organisations of three different branches that are all based in the EU and operate in one or more countries of the EU, namely 'health', 'retail/service', and 'education/research', as well as with three different organization sizes, namely 'up to 10 employees' (group 1), '11-250 employees' (group 2), and 'more than 500 employees' (group 3) were carried out based on an interview guideline validated beforehand (Table 2). This was aimed at gaining a broad perspective of costs of implementation in terms of varying levels of protection organisations need to reach related to the sector they operate in and validating the costs of implementation in various organisations sizes in order to see, if and to which extent the implementation costs scale, eg because the costs of a license for a privacy tool per employee decrease with a larger amount of employees.

3. Method to Evaluate the Costs of Jeopardising the Rights and Freedoms of Data Subjects

Possible legal actions related to the GDPR were considered by extracting fines issued by national data protection authorities from a database[8]. It contained 85 GDPR fines quoting Article 32 in the statement of reasons for the respective decisions. Most entries name the organization fined, which allowed finding the number of employees. For some anonymised entries, the number of employees could be estimated, such as 'entrepreneur' being a one-person company or a hospital likely having more than 250 employees. The remaining were classified as unknown.

In addition, 13 European case law decisions from 2018-2020 (in which the GDPR has been applicable), specifically concerning compensation under GDPR, but not specific to Article 32 of the GDPR, were extracted from a fee based legal database.

Based on these two datasets, the average amounts for administrative fines and compensations under GDPR were calculated.

4. Method for Risk Assessment

During the structured interviews, cost items of privacy measures per relevant unit, eg per employee, per certificate, and per lockable cabinet were validated. To show the overall costs of the privacy measures for an organisation, the validated costs to calculate the total costs for three hypothetical organisations were used. The cost model is based on an organisation with 10 employees and 1 site, an organisation with 250 employees and 2 sites, and an organisation with 5,000 employees and 5 sites. All costs are split into one-time costs and recurring costs.

The risk model categorises the privacy risk with parameters for impact and likelihood. Implementation costs can be directly compared to risk when cal-

8 CMS Legal Services EEIG <https://www.enforcementtracker.com/> accessed 12 April 2021.

culating the expected loss, which is simply a product of the impact and expected frequency. The expected loss and costs of implementation are only compared informally.

III. Quantification of the Costs of Implementation of State of the Art Measures

The assessment of costs of implementation for state of the art privacy measures resulted in a detailed cost table.[9] This table includes the average costs for exemplary measures of an organisation, categorised by cost items per individual measure. For example, the access control measure 'lockable cabinets' can be decomposed into 'material cost', 'personnel cost -IT-', and 'personnel cost -legal-'.

1. Costs of Privacy Measures

Tables 3-5 summarise the full cost table by showing the costs per individual measure, as well as the minimum and maximum amount shown in the second line of each table element. These tables are derived using the aforementioned hypothetical organisation for each group (10 employees and 1 site, 250 employees and 2 sites, and 5,000 employees and 5 sites). All costs shown in these three Tables are split into one-time costs (OTC) and recurring costs (RC).

- Table 3 shows a summary of the costs for technical measures which ensure that personal data in emails is being transferred confidentially.
- Table 4 shows a summary of the costs for organisational measures which ensure that employees of an organisation know and follow relevant data protection statutes.
- Table 5 shows a summary of the costs for technical and organisational measures which ensure that the physical access to personal data is being restricted.

To calculate the overall costs of the three hypothetical organisations, assumptions were made about the quantity of usage for some of the individual measures::

- each employee logs in/out once per day for the measure 'transport encryption' using a Virtual Private Network (VPN);
- default use for each employee (without individual activation) for all other technical measures;
- usage by 10 percent of employees for the measures 'lockable cabinets' and 'visual protection';
- each site has one gate, one staff member per gate, two trained staff members per position and an external contractor for the measures 'gate staff for visitor registration' (day and night);
- the implementation of one special protection zone per site for the measure 'special protection zone'.

2. Costs in Low Risk, Risk and High Risk Processing

The individual state of the art privacy measures were categorised in low risk, risk and high-risk processing based on the recommendations of e.g. ENISA and TeleTrust mentioned in Section II 1. Using the same assumptions mentioned in Sec. III 1, the costs were estimated as follows (See Table 6 Appendix).

Recurring costs of potential new employees were left out of the calculation. This results in a range of costs ranging from 14.2k € OTC and 2k € RC for a low-risk processing of an organisation with 10 employees to 2.48m € OTC and 2.58m € RC for a high-risk processing of an organisation with 5,000 employees. As one would expect, these estimates also show that in each organisation group an increase in the risk of processing is associated with greater implementation costs for privacy measures. This is because additional risk usually leads to additional (or different) measures. For example, transport encryption (email server and VPN) is implemented for low risk processing, whereas for high risk processing these measures are also accompanied by email content encryption.

3. Costs per Employee of different Organization Sizes

When calculating the costs of privacy measures per employee, the total implementation costs are as follows (See Table 7 Appendix).

9 The detailed cost table can be accessed through <https://www.sit.fraunhofer.de/edpl-annex-cost-table/>.

These figures suggest that the risk of processing has different impact depending on the the relationship between organizational size and costs of implementation. For example, the recurring costs per employee for low risk of processing are twice as high for small organisations compared with large organisations (200 € vs. 100 € respectively), whereas the recurring costs for high-risk processing are an order of magnitude higher for smaller firms (in between 7.8k € and 20.1k € vs. 516 €). Larger firms can exploit economies of scale to address a high-risk of processing. For example, the initial training of the company's data protection officer does not scale with the number of employees. Further, the individual costs per employee of hiring external privacy training falls when purchased for many employees and an organisation learns how to optimise the training process. Even though some cost items increase with the size of an organisation, such as the costs of using individual access tokens per employee for the works council, this does not outweigh the two aforementioned reasons.

The decrease in costs per employee is less dramatic when comparing estimates between medium and large organisations. For low risk processing the figures are comparable for one-time costs of measures for low risk processing (436 € for group 2 vs. 440 € for group 3). The same economies of scale are present for high risk processing – recurring costs are more than three times higher for medium sized organisations compared to large (in between 1.8k € and 1.9k € vs. 516 €). Taken together, these results suggest larger firms derive comparative advantage from the costs of implementing measures for high risk processing.

4. Validity and Generalisability

To find out how confident the interviewees were about their answers, they were asked to categorise their certainty. 26 out of 27 interviewees stated that they are sure or at least relatively sure about the cost estimation. Asked to what extent it was possible to generalise the costs of privacy measures of their organisation are in relation to organisations of similar size and with the same level of risks to the rights and freedoms of their data subjects, 24 out of 27 interviewees answered that their own cost can be generalised or at least there is rather the possibility of generalisation than not.

IV. Risks to the Rights and Freedoms of Natural Persons

This Section covers two data sources for quantifying risks to the rights and freedoms of natural persons.[10]

1. Compensation

To quantify the average amount of compensation granted by courts to data subjects under the GDPR in conjunction with national law, the research looked into publicly available case law.

Compensation awards granted to data subjects specifically for infringements of (only) Article 32 of the GDPR could not be identified. This can be interpreted as organisations being highly unlikely to be held liable for infringing Article 32 in a public case, although this says little about those cases eventually settled outside court.

However, a benchmark for compensation awards in general can be found by looking at rulings related to other aspects of the GDPR. 13 cases were analysed in this regard. One data subject was awarded compensation of 50 € by the organisation itself, even before the court spoke its verdict,[11] one court decided on a maximum amount of a specific infringement, which was set to 1k €.[12] Another three courts granted compensations of 250 €, 2.4k €, and 5k €.[13] In eight court decisions, the data subject was not granted a compensation.[14] Thus, an average award of 1.7k € when the award is granted can be determined and

10 All data mentioned in this section was extracted from the databases in August 2020 and this represents a cut-off for the sample window. Therefore, the estimates of this section can change as court decisions are challenged, new fines can be imposed and new cases can be brought to court. Given the relatively small sample size, these developments will change the presented point-estimates, especially if the distribution of fines is heavy-tailed.

11 AG Diez, judgment of 7.11.2018 - 8 C 130/18.

12 ArbG Lübeck, judgement of 20.6.2019 - 1 Ca 538/19.

13 Rechtbank Amsterdam, judgment of 2.9.2019 - 7560515 CV; ÖOGH, judgement of 22.2.2020 - 9 ObA 120/19s; ArbG Düsseldorf, judgment of 5.3.2020 - 9 Ca 6557/18.

14 OLG Innsbruck, judgment of 13.2.2020 - 1 R 182/19b; LAG Düsseldorf, judgment of 11.03.2020 - 12 Sa 186/19; OLG Dresden, decision of 11.12.2019 - 4 U 1680/19; LG Karlsruhe, judgment of 2.8.2019 - 8 O 26/19; LG Frankfurt, judgment of 20.12.2018 - 2-05 O 151/18; AG Hannover, judgment of 9.3.2019 - 531 C 10952/19; LG Lübeck, judgment of 11.4.2019 - 12 O 270/18; OLG Dresden, decision of 11.6.2019 - 4 U 760/19.

that in a majority of cases no compensation is granted.

For the estimation of the risk to the rights and freedoms of data subjects, also the legal costs an organisation needs to pay in case compensation has been granted to the data subject was considered by usingan online calculator for legal costs[15]. Building on a calculation of the average legal costs for the court decisions analysed where a compensation has been granted to the data subject and on what the data subject asked to receive and on how much compensation was granted, average costs of 1.6k € were determined. Adding the average award (1.7k €) to the average legal costs (1.6k €), the average total compensation is 3.3k €.

2. Administrative Fines

Classifying the fines in the database according to the number of employees of the prosecuted organisation reveals that the average fine for[16]
- small companies is 5.6k € (980-20k €),
- medium companies is 77k € (2.5k-460k €), and
- large companies is 9m € (2k-204.6m €).[17]

Estimating the likelihood of administrative fines, Figure 1 (Appendix) shows how the fine amounts are distributed across time starting when GDPR came into effect. Fines were relatively infrequent in the first months, but then were relatively stable (between 1 and 8 per month).

A common approach to estimating likelihood is to standardise the sample of observed harms, in this case administrative fines issued by data protection authorities, by the population of organisations who were exposed to the harm. Given differing reporting biases in the sample and the population estimates[18], caution should be taken against false precision emerging from these estimates. Relative comparisons are nevertheless valuable. The majority (62.5%) of the fined organisations were large companies even though these organisations comprise a minority of the population of organisations, which suggests that likelihood increases with organisation size.

The 2017 Eurostat figures[19] on the number of enterprises across the (then) EU 28 estimate there are 22.6 m small, 1.69 m medium and 47.8 k large businesses according to our definition. Taking this as the population of possible organisations creates problems discussed below. Nevertheless, these figures can be used to provide a rough first-pass estimate of likelihood for organisations to be addressed by an administrative fine.

Based on these simplified estimates, companies should expect a fine every 5,000,000 years (for small companies), 100,000 years (for medium-sized companies), and 1,200 years (for large companies) depending on company size. Weighting the average fine by the likelihood suggests the expected fine for small, medium, and large organisations is less than a cent, less than a euro, and around 7.5k € respectively. Even if the accuracy is false, it raises the question of whether a rational small company should expend resources mitigating this risk when approximately half go bankrupt within five years[20]

V. Decision Factors in Adopting Privacy Measures

Subsection 1 draws together the estimates in the previous Section to analyse appropriate privacy measures according to Article 32 of the GDPR. This case study addresses one consideration, legal compliance, in adopting privacy measures. Subsection 2 adds context by asking data protection officers about additional factors.

15 Lawyers' Association of Germany <https://anwaltsblatt.anwaltverein.de/de/apps/prozesskostenrechner> accessed 12 April 2021.

16 The unknown companies that we mentioned in Sec. II 2 c would not significantly change the results regardless of the actual organisation size. The average fine was just 30k € with a range of 500-105k € for the 14 companies whose size we could not establish. Reporting biases mean these are unlikely to be large companies who are more likely to find their way into media reports or be forced to report to shareholders.

17 The large company figure falls to 1.1m € if two outliers relying on the turnover based maximum fine were removed. Note, the maximum fine under Article 32 is the greater of 10m € or 2% of worldwide turnover; Art. 83 para. 4 GDPR; Cedric Burton in Christopher Kuner, Lee Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR) – A Commentary* (2020) Art. 32 637.

18 Daniel Woods, Tyler Moore, and Andrew Simpson, 'The County Fair Cyber Loss Distribution: Drawing Inference from Insurance Prices' (2019) Workshop on the Economics of Information Security, 2.

19 Eurostat, 'Annual enterprise statistics by size class for special aggregates of activities (NACE Rev. 2)', <https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=sbs_sc_sca_r2&lang=en> accessed 12 April 2021.

20 Emmanuel Quansah and Dale E. Hartz, 'Strategic adaptation: leadership lessons for small business survival and success' (2021) American Journal of Business, 1.

1. Appropriateness in Article 32

By quantifying the costs of privacy measures and the risk to the rights of data subjects via legal actions, question of appropriateness can be considered relying on identified costs of exemplary, state of the art privacy measures. The estimates of implementation costs of each can be seen in Table 8 (Appendix). These single figures are derived using the same hypothetical organisations as in Tables 3-5. Table 8 also shows the estimates for the likelihood and impact of legal actions. The expected compensation award would be less than a cent regardless of organisation size. This suggests the costs of implementation are far greater than the risk of legal action. This is even more striking given these categories do not capture all relevant organisational and technical measures, which means the figures from Section III as well as the following table under-estimate the true costs of a complete set of state of the art privacy measures.

Since data subjects suffer harm regardless of whether a violation is prosecuted, a second set of risk estimates was carried out in which the likelihood is more in line with survey data. Assuming the likelihood of violating data subject rights is 0.25[21] and impact remains the same, then the expected risk for small, medium, and large organisations are 2.23k €, 20k €, and 2.25m € respectively. Although the expected risk is still lower than implementation costs, the lack of balance could result from uncertainty in our estimates for large organizations. Even when using the frequency of incident rather than frequency of fine, it still appears that small organizations overspend.

To further validate the above estimates, interviewees had been asked whether the organisation has ever considered the financial consequences of a (real past or fictitious future) data breach. Most organisations (16 of 27) had not done so.

Of the organisations who answered yes, two large organisations only considered the maximum fines under GDPR (250m € for one of them based on 2 % of its total worldwide annual turnover of the preceding financial year). Multiple interviewees expect less than the maximum fine. One of the small organisations did not expect administrative fines higher than 4-digits, one of medium organisations expected all costs including fines to be 30-150k € for a medium-sized data breach, and two large organisations expected administrative fines around 500k €.

The participants who provided concrete estimates of fine sizes are all comparable to the mean for each organization size from the database analysis.[22] Even the negative responses provide partial validation in that small and medium sized organisations may rationally not estimate fines when expected losses are less than a euro. The maximum observed fines, respectively, 20k € and 460k € would not be catastrophic for these organisations. Two interviewees explicitly said that fines under the GDPR are 'negligible' while others stated the expected cost is relatively smaller than security losses. This points to additional drivers in the adoption of decisions regarding privacy measures.

We also asked respondents whether the organisation experienced data breaches in the past for which under current law there was an obligation to report to the concerned supervisory authority. Two answered yes, two said yes with exactly one breach, three said yes but only very few breaches, and two answered yes with at least 100 breaches. One of the latter only realised they needed to act by hiring an external data protection officer after these 100 breaches. The remaining 18 all answered no. The fact that more data breaches in a sample of 27 organisations were determined during the research conducted than all fines issued under the GDPR shows how prosecution likelihood is far lower than incident likelihood.

2. Additional Factors

Considering Article 32 in isolation, Table 8 suggests implementing privacy measures is not rational based on the risk of legal action alone. Yet, all our interview participants implemented *some* measures. Details of the responses help to explain this seeming contradiction by identifying additional drivers of adoption decisions.

Seven participants reported improved business performance due to the implemented measures beyond compliance, eight reported no such additional

21 Claudia Biancotti, 'The price of cyber (in)security: evidence from the Italian private sector' (2018) Workshop on the Economics of Information Security, 10.

22 The only exception are the large organisations as already explained above (n 23) for which the mean is inflated significantly by two outliers issued by the UK regulator.

benefits, and the remaining participants commented without committing to an answer. Preventing security harms like reputation damage and intellectual property loss was repeatedly identified by participants as a driver. Nine said measures were necessary for customer acquisition. The role of VPN in enabling employees to work (eg from home, during travel), privacy training in making processes more efficient, and updated availability measures in saving energy were mentioned by just one or two respondents.

Quantifying the relative importance of each driver, two respondents reported that the measures were implemented without any consideration for privacy risk, with one explaining that implementation was down for information security management reasons. However, the same respondent argued that they would implement additional measures if deemed necessary by data protection law.

More evidence that organisations are more likely to be guided by the low actual risk of privacy harm than to be proactive on the basis of the legal requirement alone, can be found in responses to why measures are *not* implemented. Seven interviewees stated that not implementing measures is a result of risk management. One organisation's management decided against such measures because there was such a low likelihood of occurrence, which supports the likelihood analysis. Some responses suggested the organisations had not internalised the risk-based logic of Article 32, six interviewees stated that they only implemented measures that deemed absolutely necessary, and two interviewees stated that costs are the first priority in the decision for or against measures.

It remains to be emphasised that the GDPR does not allow a purely economic weighing in favor of implementation costs. Rather, the implementation costs may be considered when selecting privacy measures so that they are implemented in an *appropriate manner* as a result. The focus of data protection considerations is and remains the protection of the rights and freedoms of the data subjects.[23]

VI. Limitations

Implementation costs are deterministic, which means we are confident about individual estimates like the cost of a data protection officer. This confidence is shared by the participants as all, but one stated they were at least relatively sure about the costs. The challenge lies in identifying the right/appropriate set of state of the art privacy measures since the risk-based approach to Article 32 of the GDPR avoids specific prescriptions. As mentioned before, the privacy measures that we quantified are not exhaustive. Consequently, the described costs should be seen as an under-estimate.

Risk to data subjects is stochastic unlike costs. Consequently, negative outcomes are difficult to observe because most organisations do not observe realised harms. For example, none of the interviewed organisations experienced a fine under the GDPR (whereas all incurred implementation costs). This was addressed in Section III.3 by sampling from the population of organisations that violated Article 32.

However, the organisations in the public fines database are likely to show systematic differences. For example, it is more likely that organisations implementing relatively less privacy measures are included as they face a higher likelihood of violation and higher fines according to the GDPR. The amount of the fines is likely inflated relative to a typical organisation as a result.[24] Organisations should adjust estimates based on their position relative to peers. The results presented in this contribution show how implemented measures differ with organisational size, which can support risk managers in adjusting risk estimates. Further, authorities may require organisations to implement privacy measures in addition to any fine (Article 58 para. 2 lit. d, f. i of the GDPR), which was not reflected in the estimates of the cost of violating Article 32.

The present sample relies on fines being reported publicly and discovered by the database curator. Additionally, the case law for compensation cannot capture out of court settlements. This leads to serious under-reporting as organisations settle to avoid costly legal battles to overturn precedent. Risk managers

23 Hielke Hijmans and Cedric Burton in Cedric Burton in Christopher Kuner, Lee Bygrave, and Christopher Docksey, *The EU General Data Protection Regulation (GDPR) – A Commentary* (Oxford University Press, 2020 Art 1 57 and Art 32 635; Robert Kazemi, *The General Data Protection Regulation in Legal Consultation Practice* (Deutscher Anwalt Verlagm 2019) 95.

24 The (unrealistic) hypothetical in which an organization implemented no privacy measures and hence had no implementation costs would likely face a much higher likelihood of being fined/expected fine as the organizations who were fined implemented at least some privacy measures.

may adjust for this by understanding their own exposure to each privacy practice with a precedent. For example, an organisation with Y company cars – for which location tracking has been subject to a compensation under GDPR – are exposed to Y times the compensation according to a decision of the Austrian Supreme Court[25] if they insist on using location tracking.

More fundamentally, this analysis relied on legal actions to estimate the risks to data subjects even though fines and compensation do not perfectly indemnify the harm to data subjects.

Even though the GDPR promises compensation for a range of damages (see Section IV 1), most of the awards related to a failure to obtain consent. This means past compensation awards provide little to no information about potential harm to data subjects regarding intangible harm like psychological damage.

VII. Conclusion

This contribution began with a narrow interpretation of Article 32 of the GDPR, which can be summarised as balancing the financial costs of state of the art privacy measures against the risk to data subjects. The estimated implementation costs can be used by organisations to baseline against peers of a similar size and sector, adjusting employee costs in the relevant Member State and keeping in mind the limited scope not including all protection goals under Article 32.

When comparing the height and likelihood of fines to the costs of implementing privacy measures, it seems that most organisations are over-implementing privacy measures. If instead the likelihood of a data security incident is used, (particularly large) organisations appear to be achieving a balance.

The appropriate balance can only be assessed with individualised risk assessments, which is the nature of a regulated risk-based approach. Organisations should consider the legal risk of finding an inappropriate balance, and how to document decisions in order to mitigate this risk. Again, it needs to be emphasised that the GDPR does not allow a purely economic weighting in favor of implementation costs but rather allows to take implementation costs into account when selecting privacy measures so that they are implemented in an *appropriate manner* as a result.

Turning to the aspect of risk for data subjects, the GDPR expects organisations to consider a range of privacy harms to data subjects (see Recital 75) for which courts have awarded no compensation. This forces organisations to assess potential harm to data subjects without any external reference points or internal informational advantage. This contribution offers guidance with regard to the three above-mentioned elements. However, regulators should offer further support to organisations in this assessment to increase the predictability of legal decisions regarding appropriate privacy measures, eg by adding legal definitions for terminology used in Article 32 (such as 'state of the art', 'implementation costs'). Such support could also take the form of guidelines of the European Data Protection Board, in which the individual factors that need to be considered when implementing privacy measures are further explained and weighted.

25 ÖOGH, judgment of 22 February.2020 - 9 ObA 120/19s.

Table 1: Summary of Pre-Interviews

Interviews	22 June and 3 July 2020, via online video conferencing system, ca. 30 minutes on average
Aim of interviews	Initial cost assessing of 'personnel ', 'providers ', 'hard- and software' and 'other costs' for each of the individual measures
Interview partner	Employees of each, 'purchasing', 'data protection officer', 'legal', 'HR', 'works council', 'building management', 'administration', 'IT/IT management'
Documentation	Summarized transcription, usually right after the interview

Table 2: Summary of Interviews

Validation of interview guideline	21 July and 22 July 2020, via online video conferencing system, ca. 30 minutes on average
Interviews	22 July and 31 July 2020, via online video conferencing system,[a] ca. 60 minutes on average
Aim of interviews	Validation of pre-assessed costs
Interview partner	27 organisations (three interviews in each of the branches and each of the organisation sizes selected) that are all based in the EU and operate in one or more states of the EU, with either the managing director, the data protection officer (or -coordinator) or the information security officer of the organisations
Documentation	Summarised transcription, usually right after the interview

a Except for two interviews that both were carried out through a combination of telephone and email exchange.

Table 3: Summary of Costs of Technical Measures

Type of cost	Group 1: 10 employees, 1 site	Group 2: 250 employees, 2 sites	Group 3: 5,000 employees, 5 sites
Individual measure: Transport encryption – E-Mail-Sever			
One-Time Costs	€ 338 € 150-525	€ 400 € 275-525	€ 463 € 400-525
Recurring Costs, per annum	€ 188 € 80-295	€ 263 € 230-295	€ 263 € 230-295
Individual measure: Transport encryption – VPN			
OTC	€ 2.100 € 1.800-2.500	€ 7.500 € 6.600-8.400	€ 114.000 € 102.000-127.000
RC, p.a.	€ 1.900 € 750-3.100	€ 25.200 € 18.900-31.500	€ 500.000 € 375.000-625.000

RC, per new employee	€ 23 € 20-25	€ 23 € 20-25	€ 23 € 20-25
Individual measure: E-Mail encryption			
OTC	€ 4.400 € 4.100-4.700	€ 17.700 € 16.200-19.200	€ 232.000 € 202.000-262.000
RC, p.a.	€ 208 € 195-220	€ 2.300 € 2.000-2.600	€ 43.900 € 37.600-50.100
RC, p.n.e.	€ 45 € 40-50	€ 45 € 40-50	€ 45 € 40-50

Table 4: Summary of Costs of Organizational Measures

Type of cost	Group 1: 10 employees, 1 site	Group 2: 250 employees, 2 sites	Group 3: 5,000 employees, 5 sites
Individual measure: Written commitment to data protection by all employees			
OTC	€ 590 € 50-1.100	€ 3.500 € 2.700-4.300	€ 68.900 € 35.800-102.000
RC, p.n.e.	€ 7 € 0-13	€ 10 € 7-13	€ 15 € 7-20
Individual measure: Initial training of the company data protection officer			
OTC	€ 5.300 € 4.800-5.900	€ 2.000 € 1.900-2.300	€ 7.600 € 6.800-8.400
Individual measure: Annual training of the company data protection officer			
OTC	€ 5.300 € 4.800-5.900	€ 2.000 € 1.900-2.300	€ 7.600 € 6.800-8.400
RC, p.a.	€ 1.600 € 1.500-1.800	€ 2.000 € 1.900-2.300	€ 3.600 € 1.900-5.300
Individual measure: General employee privacy training			
OTC	€ 425 € 0-850	€ 750 € 650-850	€ 750 € 650-850
RC, usually p.a.	€ 993 € 465-1.500	€ 35.700 € 9.300-62.100	€ 441.000 € 170.000-713.000
Individual measure: Test at the end of the training			
OTC	€ 1.300 € 1.200-1.400	€ 2.000 € 1.800-2.100	€ 3.300 € 3.100-3.500

RC, usually p.a.	€ 198 € 170-225	€ 4.900 € 4.300-5.600	€ 99.200 € 86.000-113.000
Individual measure: Additional task-related employee privacy training			
OTC	€ 750 € 650-850	€ 16.400 € 14.400-18.400	€ 750 € 650-850
RC, usually p.a.	€ 700 € 600-800	–	€ 515.000 € 225.000-805.000
Individual measure: (Written) privacy instructions for employees			
OTC	€ 11.200 € 6.600-15.700	€ 26.600 € 17.500-35.600	€ 240.900 € 60.500-421.000
RC, p.n.e.	€ 35 € 30-40	€ 35 € 30-40	€ 25 € 10-40

Table 5: Summary of Costs of Technical and Organizational Measures

Type of cost	Group 1: 10 employees, 1 site	Group 2: 250 employees, 2 sites	Group 3: 5,000 employees, 5 sites
Individual measure: Security locks with individual key/token per employee			
OTC	€ 4.800 € 3.700-6.000	€ 69.200 € 48.900-89.600	€ 1.700.000 € 1.300.000-2.000.000
RC, p.n.e.	€ 62 € 15-110	€ 17 € 15-19	€ 51 € 13-90
Individual measure: Lockable cabinets			
OTC	€ 1.000 € 850-1.200	€ 20.700 € 15.600-25.800	€ 358.000 € 308.000-409.000
Individual measure: Visual protection in the building			
OTC	€ 641 € 515-768	€ 6.100 € 1.400-10.800	€ 116.000 € 22.800-209.000
Individual measure: Access authorization concept			
OTC	€ 3.200 € 2.700-3.600	€ 9.400 € 6.700-12.100	€ 99.500 € 82.200-116.000
RC, p.n.e.	€ 18 € 15-20	€ 13 € 5-20	€ 18 € 15-20
Individual measure: Gate staff for visitor registration (day)			

OTC	€ 3.200 € 2.900-3.400	€ 4.300 € 4.000-4.600	€ 7.100 € 6.700-7.600
RC, p.a.	€ 73.800 € 69.600-78.000	€ 147.000 € 139.000-156.000	€ 369.000 € 348.000-390.000
Individual measure: Alarmsystem			
OTC	€ 3.600 € 2.700-4.400	€ 9.900 € 8.200-11.500	€ 32.700 € 29.900-35.500
RC	–	€ 3.500	€ ca. 8.800
Individual measure: Setting up special protection zones			
OTC	€ 18.200 € 18.100-18.200	€ 36.000 € 35.900-36.000	€ 89.400 € 89.300-89.400
Individual measure: Gate staff for visitor registration (night)			
OTC	€ 2.400 € 2.200-2.600	€ 3.600 € 3.300-3.800	€ 6.100 € 5.500-6.800
RC, p.a.	€ 122.000 € 114.000-131.000	€ 245.000 € 228.000-262.000	€ 612.000 € 570.000-654.000
Individual measure: Video surveillance			
OTC	€ 14.800 € 11.900-17.700	€ 35.600 € 26.100-45.100	€ 116.000 € 66.500-165.000

Table 6: Costs in Low Risk, Risk, and High-Risk Processing

For an organization doing a low-risk processing[a]	in group 1 are 14.2k € (OTC) & 2k € (RC), in group 2 are 109 k € (OTC) & 25k € (RC), in group 3 are 2.2m € (OTC) & 500k € (RC);
For an organization doing risk processing[b]	in group 1 are 25.2k € (OTC) & 78.4k € (RC), in group 2 are 139k € (OTC) & 211k € (RC), in group 3 are 2.46m € (OTC) & 1.31m € (RC);
For an organization doing high risk processing[c]	in group 1 are in between 25.2k € and 78.2k € (OTC) & in between 78.4k € and 201k € (RC),[d] in group 2 are in between 259k € and 277k € (OTC) & in between 461k € and 463k € (RC), in group 3 are 2.48m € (OTC) & 2.58m € (RC).

a For a low-risk processing, the research approach assumed the implementation of the following individual measures in accordance with the aforementioned literature: transport encryption (email server and VPN), written commitment to data protection by all employees, initial training of the company data protection officer, security locks with individual key/token per employee and lockable cabinets.

b For a risk processing, the research approach assumed the implementation of the following individual measures in accordance with the aforementioned literature and in addition to the measures implemented for a low-risk processing: annual training of the company data protection officer, general employee privacy training, visual protection in the building, access authorization concept, gate staff for visitor registration (day), alarm system.

c For a high-risk processing, the research assumed the implementation of the following individual measures in accordance with the aforementioned literature and in addition to the measures implemented for a low risk and risk processing: email encryption, test at the end of

the training, additional task-related employee privacy training, (written) privacy instructions for employees, setting up special protection zones, gate staff for visitor registration (night), video surveillance.

d Respondents in group 1 and 2 tend not to implement all high risk measures or take alternative measures. Since both options are cheaper, the research assumed (1) a cost range in between the cost of a risk processing of group 1 and the weakly to not validated measures of high-risk processing for group 1 and (2) a cost range in between the cost of a high risk processing of all validated measures for group 2 and the not validated measures for group 2.

Table 7: Costs per employee of different organization sizes

In a low risk processing the costs of an organization per employee	of group 1 are 1.4k € (OTC) & 200 € (RC), of group 2 are 436 € (OTC) & 100 € (RC), of group 3 are 440 € (OTC) & 100 € (RC);
In a risk processing the costs of an organization per employee	of group 1 are 2.52k € (OTC) & 7.8k € (RC), of group 2 are 556 € (OTC) & 844 € (RC), of group 3 are 492 € (OTC) & 262 € (RC);
In a high risk processing the costs of an organization per employee	of group 1 are in between 2.52 k € and 7.8k € (OTC) & in between 7.8k € and 20.1 k € (RC),[a] of group 2 are in between 1k € and 1.1k € (OTC) & in between 1.8k € and 1.9k € (RC), of group 3 are 496k € (OTC) & 516 € (RC).

a For this calculation, the information of the aforementioned subsection regarding group 1 and 2 are valid, too.

Table 8: Summary Table

Estimate[a]	OTC/RC	Group 1: 10 employees	Group 2: 250 employees	Group 3: 5.000 employees
Implementation cost, low risk	OTC	€ 14.200	€ 109.000	€ 2.200.000
	RC	€ 2.000	€ 25.000	€ 500.000
Implementation cost, risk	OTC	€ 25.200	€ 139.000	€ 2.400.000
	RC	€ 78.400	€ 211.000	€ 1.310.000
Implementation cost, high risk	OTC	€ 25.200-78.200	€ 259.000-277.000	€ 2.480.000
	RC	€ 78.400-201.000	€ 461.000-463.000	€ 2.580.000
Mean compensation		€ 3.300[b]	€ 3.300[b]	€ 3.300[b]
Mean administrative fine		€ 5.600	€ 77.000	€ 9.000.000
Administrative fine frequency		~ 5.000.000 years	~ 100.000 years	~ 1.200 years
Expected adm. fine amount		€ < 0.01	€ < 1	€ ≈ 7.500

a Recurring costs of new employees are not calculated into the costs of this table. All other limitations are exactly as mentioned in the footnotes of the summary tables.

b Including legal costs

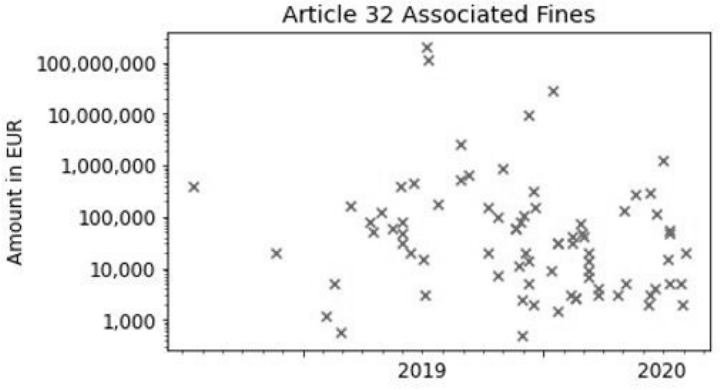

Figure 1: There are Few Clear Trends in Either the Frequency or Size of Fines Since mid-2019