MIS Quarterly Executive

Volume 20 | Issue 3 Article 4

September 2021

Learning from Enforcement Cases to Manage GDPR Risks

Saeed Akhlaghpour

Farkhondeh Hassandoust

Farhad Fatehi

Andrew Burton-Jones

Andrew Hynd

MIS Quarterly Executive

Learning from Enforcement Cases to Manage GDPR Risks

The European Union's General Data Protection Regulation (GDPR) is a groundbreaking data privacy and security law that affects organizations globally. Noncompliance can incur potentially hefty penalties, but compliance is not a box-ticking exercise and requires a risk-based approach. Based on an analysis of 93 cases of GDPR enforcement, we have identified 12 types of risk and their associated mitigation measures and risk indicators. We also describe the strategic actions that can be taken to manage GDPR risks.[1,2]

Saeed Akhlaghpour
The University of Queensland (Australia)

Farkhondeh Hassandoust
Auckland University of Technology (New Zealand)

Farhad Fatehi
Monash University (Australia)

Andrew Burton-Jones
The University of Queensland (Australia)

Andrew Hynd
Holding Redlich Lawyers (Australia)

The EU GDPR Is Reshaping the Data Protection Landscape

On 25 May 2018, the European Union (EU) General Data Protection Regulation (GDPR) came into effect and marked a significant milestone in the evolution of data protection legislation and practice. Unlike other privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the GDPR is not confined by industry sector, technology, or geography.[3] It applies to all organizations (public or private) processing the personal data of EU data subjects (individuals), regardless of an organization's location. Together with high-profile cases, such as the hack of three billion Yahoo accounts,[4] the data breach that allowed Cambridge Analytica to harvest 50 million Facebook profiles[5]

SIM WHERE IT LEADERS CONNECT

KELLEY SCHOOL OF BUSINESS INDIANA UNIVERSITY

1 Michelle Kaarst-Brown is the accepting senior editor for this article.

2 The authors thank Michelle Kaarst-Brown, Gabriele Piccoli, the members of the review team, and David Seabrook for their constructive feedback and guidance throughout the review process.

3 See, for example, two recent articles that discuss the GDPR's relevance to Blockchain and IoT technologies: 1) Rieger, A., Lockl, J., Urbach, N., Guggenmos, F. and Fridgen, G. "Building a Blockchain Application That Complies with the EU General Data Protection Regulation," *MIS Quarterly Executive* (18:4), December 2019, pp. 263-279; and 2) Bilgeri, D., Fleisch, E., Gebauer, H. and Wortmann, F. "Driving Process Innovation with IoT Field Data," *MIS Quarterly Executive* (18:3), September 2019, pp. 191-207.

4 See Larson, S. "Every Single Yahoo Account Was Hacked: 3 Billion in All," *CNN Business*, October 4, 2017, available at https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/.

5 See Cadwalladr, C. and Graham-Harrison, E. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 18, 2018, available at https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

DOI: 10.17705/2msqe.00049

and Edward Snowden's revelations of mass surveillance,[6] the GDPR has created a strong push for privacy regulations around the globe. The introduction of California's Consumer Privacy Act (CCPA) and Brazil's new privacy regulations were inspired by the GDPR, and other countries such as India, Japan and Australia are preparing stronger data privacy legislation.

The GDPR is a complex and significant piece of legislation. The official GDPR document is lengthy, comprising 99 articles and 173 recitals. It is significant because it substantially broadens and strengthens data subjects' rights, including the right to be informed, the right to access one's personal data, the right to the erasure of data and the right to data portability. It also introduces certain rights relating to automated decision-making (Articles 12 to 23). The GDPR has mandatory breach notification requirements with a tight deadline of no later than 72 hours after an organization first becomes aware of a breach (Article 33). Finally, it introduces unprecedented penalties (Article 38) of up to €20 million ($23.7 million)[7] or 4% of an organization's global annual turnover (whichever is greater). The latter is significant enough to get the immediate attention of CEOs, CIOs and executives. In this article, we provide advice on how organizations can mitigate the risks of being fined for breaches of the GDPR. This advice is based on our analysis of 93 cases where firms were fined by data protection authorities (Appendix A describes our research methodology).

However, the GDPR is not all about restrictions, sanctions and fines. The goal of the GDPR is to foster trustworthy innovation through harmonizing, or bringing into conformity with each other, the data protection laws of the 27 EU member states. The GDPR aims to regulate a complex data environment rife with technological challenges associated with data leaks, data breaches and shadow IT where unknown data is being collected and used within an organization (and among its network of suppliers and customers). It also addresses transactional challenges and challenges arising from country-level differences, standard contractual clauses, cloud storage and security, and cross-border data flows beyond the EU. By providing a standard set of EU-wide data protection laws, the GDPR eases the burden of dealing with these challenges because an organization only needs to interface primarily with one regulator (known as "the lead supervisory authority") based in the same country as its main establishment. This unprecedented feature of the GDPR is referred to as the *one-stop-shop* mechanism. Moreover, as described below, the GDPR offers substantive, though qualified, discretion to businesses through its risk-based approach. Before describing the findings of our analysis of cases involving GDPR fines and the lessons that can be learned from them, we provide a brief introduction to the GDPR and its emphasis on a risk-based approach to compliance.

GDPR Overview

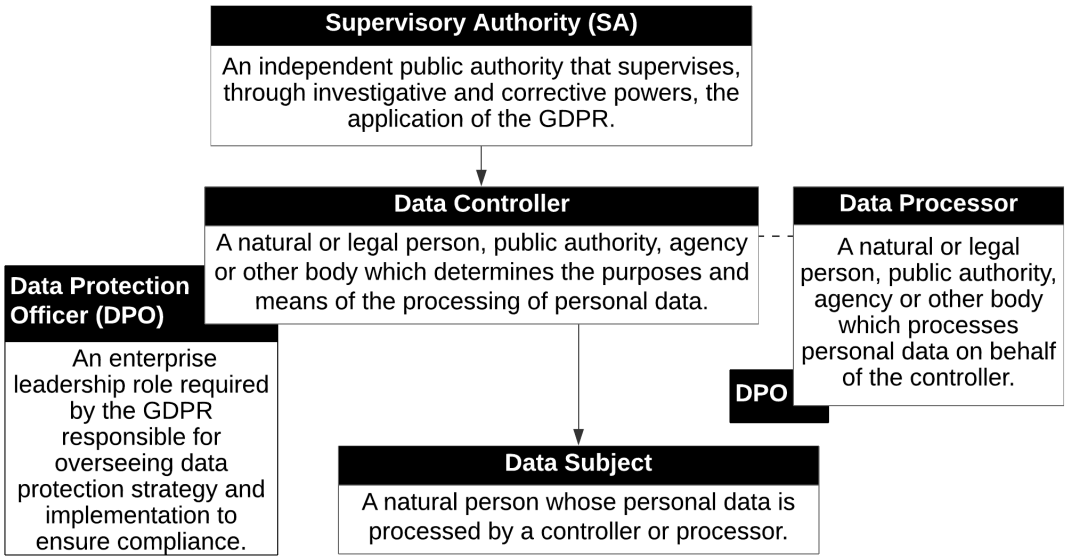
The GDPR is a landmark in the evolution of the EU's privacy framework for the protection and privacy of EU residents' personal data. Below, we provide a condensed overview of the most important points of the GDPR to set the stage for the rest of this article, in which we describe how the challenges of conforming with the regulation can be overcome. The full GDPR document comprises 11 chapters and 99 articles, which are summarized in Appendix B. The GDPR regulates the treatment of personal data—i.e., any information that directly or indirectly can identify a data subject (a natural person). It establishes rules to enforce data subjects' rights against abusive personal data processing. These rights include the *right of access*, which allows data subjects to request confirmation from organizations (i.e., data controller) as to whether or not their personal data is being processed, and if so, where and to what purpose. Organizations must also provide a copy of such data in an electronic format, free of charge, upon request. In addition, the contentious *right to be forgotten*[8] allows individuals to request the erasure of their data, if the data is no longer

6 Rossi, A. 2018. "How the Snowden Revelations Saved the EU General Data Protection Regulation," *The International Spectator* (53:4), November 2018, pp. 1-17.

7 Currency conversion rate as of July 2021; in the rest of this article, all currency amounts are expressed in euros, but can be converted to U.S. dollars by multiplying by 1.185.

8 For a review of the issues surrounding the right to be forgotten and possible alternative approaches, see Garcia-Murillo, M. and MacInnes, I. "Così fan tutte: A Better Approach than the Right to be Forgotten," *Telecommunications Policy* (42:3), December 2017, pp. 227-240.

Figure 1: Main Roles Defined in the GDPR



relevant to the purpose for which it was collected, or should they wish to withdraw consent. In these cases, organizations must halt further dissemination of the data and must prevent third parties from processing it. Similarly, the *right to explanation* entitles individuals to receive sufficient information about automated decision-making[9] so as they can make an informed decision on whether to opt out (*the right to object*). The GDPR also promotes *privacy by design* which requires organizations to consider data protection from the inception of and throughout the system development lifecycle, not just adding it retrospectively.

The GDPR also requires organizations to appoint a *data protection officer* (DPO) who can demonstrate the organization's compliance with the regulation and interact with the national data protection authorities (DPAs), and especially the DPA that is designated as the lead supervisory authority (SA) of the organization. Figure 1 illustrates the main roles defined in the GDPR.

The GDPR Requires a Risk-Based Approach

One of the key features of GDPR is its emphasis on a risk-based approach. It requires organizations to shift from passively following bureaucratic requirements to actively and reflectively implementing the law, taking into account each particular situation and the risks to the individuals concerned. In the words of EU regulators, "compliance should never be a box-ticking exercise, but should really be about ensuring that personal data is sufficiently protected." The risk-based approach is encapsulated in Articles 24 and 25(1) of the GDPR. Article 24 sets out the risk-based responsibility of organizations (controllers of data), and Article 25(1) lists the measures that organizations should adopt to meet this responsibility:

- Article 24(1) (responsibility of the controller): "*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and*

9 A framework and recommendations for explainable AI in accordance with the GDPR, can be found in Asatiani, A., Malo, P., Nagbøl, P. R., Penttinen, E., Rinta-Kahila, T. and Salovaara, A. "Challenges of Explaining the Behavior of Black-Box AI Systems," *MIS Quarterly Executive*, (19:4), December 2020, pp. 259-278.

to be able to demonstrate that processing is performed in accordance with this Regulation …"

- Article 25(1) (data protection by design and by default): "*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall … implement appropriate technical and organisational measures … in an effective manner and to integrate the necessary safeguards into the processing …*"

The GDPR's risk-based approach requires organizations to implement abstract legal rules in a proportionate, contextualized manner. On the one hand, the approach gives organizations the discretion not to take measures when this would be impossible or disproportionately burdensome. On the other hand, it ensures that they carry out a genuine risk assessment for each case and offer sufficient protection of the rights and freedoms of data subjects.[10] The lessons learned from our research on cases of GDPR enforcement fines will help organizations to identify relevant risks and implement the "appropriate technical and organisational measures" required by Articles 24 and 25.

Overview of Our Research into GDPR Enforcement and Fines

Compliance with the GDPR became a legal requirement on May 25, 2018, but it took time before enforcement fines started to surface. In our research, we analyzed 93 cases of GDPR enforcement fines issued between July 2018 and October 2019 in 23 EU countries (see Figure 2, which depicts the number of fines and the total fine amounts for each of the 23 countries). The maximum fine was €50 million, levied on Google in France, and the minimum fine was €230 for sending incorrect pay slips to an employee in the Czech Republic. Further details on each of the 93 GDPR enforcement cases and the fines imposed can be found in the supplementary online material available at https://osf.io/ywbqz/.

Figure 2 indicates that different national DPAs have adopted differing enforcement approaches. For example, many of the Central and Eastern European DPAs, such as those in Hungary and Romania, have issued a larger number of fines (indicated by the taller bars), but the total amounts of the fines are small (the euro amounts of the fines for each country are listed in Table 1). In contrast, DPAs in countries such as the U.K. and France were more likely to go after big companies such as Google and Marriott Hotels, and issue larger fines (indicated by the larger circles). Improving the consistency of GDPR enforcement across all countries is currently a key target of EU regulators.[11]

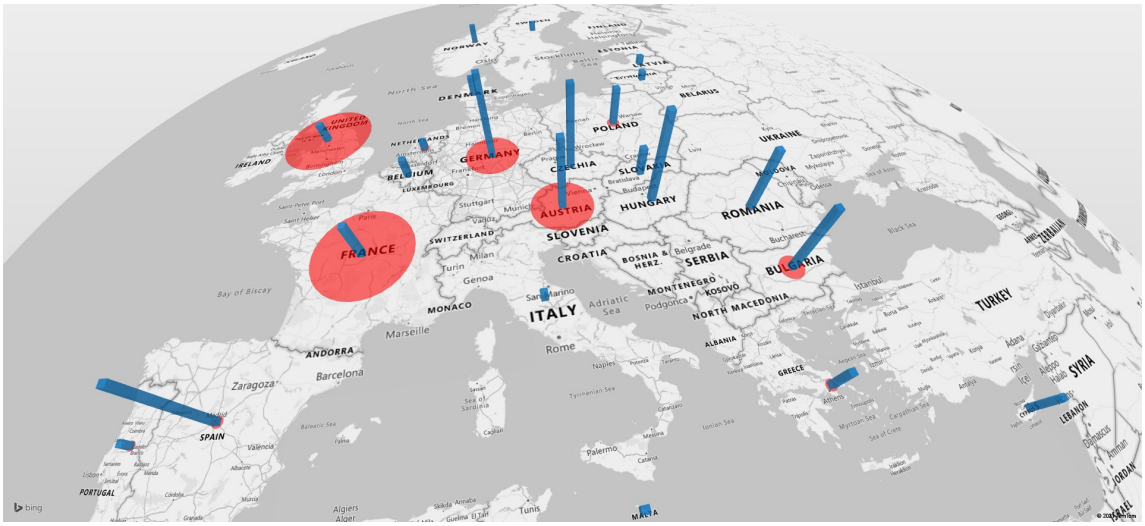
National DPAs have been generally lenient in enforcing GDPR during the first few years, partly because of the adverse impacts of the Covid-19 global pandemic on businesses.[12] However, "big stick" penalties, such as 4% of annual global revenue or €20 million, are still on the table. Moreover, the ongoing and long legal proceedings currently underway (e.g., the Irish DPA's multiple investigations into Facebook practices) could lead to large fines. Moreover, the alarming recent announcement by the Norwegian DPA that it intends to fine the online dating app, Grindr, €10 million—equivalent to 10% of its turnover—indicates that DPAs are prepared to issue large fines. In addition to monetary fines, DPAs have the authority to stop an organization's data processing if it violates the GDPR. Halting certain business operations can arguably cause more severe impacts on organizations than imposing fines.

10 Quelle, C. "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability-and Risk-Based Approach," *European Journal of Risk Regulation* (9:3), September 2018, pp. 502-526.

11 See, for example, *Data Protection as a Pillar Of Citizens' Empowerment and the EU's Approach to the Digital Transition: Two Years of Application of the General Data Protection Regulation*, June 24, 2020, European Commission, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0264.

12 See, for example, "ICO Fines British Airways £20m for Data Breach Affecting more than 400,000 Customers," *Information Commissioner's Office*, October, 16, 2020, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/. This notice cites Covid-19 impacts as a reason for a reduced fine.

Figure 2: Number of GDPR Fines (Bar Size) and Total Fine Amounts (Circle Size), by Country (n=93)



Circle size: Total Fine Amount (Total: €140 million); Bar size: No. of Fines (Total: 93; average of 4 per country)

Table 1: GDPR Fine Amounts by Country (n=93)

Country	No. of Fines Issued	Fine Amount	
France	4	€50,600,000	
United Kingdom	2	€48,900,000	
Austria	8	€18,071,900	
Germany	9	€14,790,107	
Bulgaria	8	€3,145,210	
Poland	4	€933,648	
Spain	10	€572,000	
Greece	3	€550,000	
the Netherlands	1	€460,000	
Portugal	1	€400,000	
Norway	2	€373,000	
Denmark	2	€260,850	
Romania	8	€324,000	
Hungary	10	€165,691	
Other Member States (9)	21	€237,824	
Total	**93**	**€139,884,230**	

Actions for Managing GDPR Risks and Impacts on Organizations

The risk-based approach to GDPR compliance puts the onus on executives to identify and manage risks appropriately. In complex cases, executives can consult with the DPA and conduct a detailed privacy impact assessment (as per Article 33). However, even for straightforward and standard operations, organizations need to evaluate risks and devise sufficient measures based on their own discretion. We contend that one way to identify GDPR-related threats and appropriate responses is to learn from the fines that have been imposed on other organizations. Such cases provide a historical picture of GDPR enforcement. Numerous actions can result in a fine by GDPR authorities, and these actions are all potential—yet hypothetical—risks. Once a DPA issues a fine based on an action, that risk is actualized. Reviewing the lessons learned from these cases of actualized risks enables organizations to identify appropriate risk-mitigation measures (e.g., to decide which risk areas to address and allocate the necessary resources). Figure 3 illustrates this risk-based approach to GDPR enforcement.

In our research for this article, we analyzed the patterns of GDPR violations and fines applied to date. This analysis revealed important risks that need to be minimized. We categorized these risks into 12 types spread across three broad action areas: *organizational practices*, *technology and data management*. Below, we describe each of the 12 types of risk and list the enforcement fines that have been imposed for each type. Based on the lessons learned from past GDPR enforcements, at the end of each risk description, we include a text box that lists the mitigation measures organizations can take and the potential key risk indicators (KRIs) that organizations can monitor.

As emphasized earlier, managers and executives need to consider their specific organizational context and develop and adapt our suggested risk mitigation measures and KRIs accordingly. These measures and KRIs can be used as pointers for further discussion and reflection in the specific organizational context. In the supplementary online material (https://osf.io/hg8ar/), we provide a detailed checklist derived from the lessons learned from the 93 GDPR fine cases that IT managers can use to help their organizations create appropriate risk mitigation measures and identify the KRIs they need to monitor.

Figure 3: Risk Management Based on GDPR Enforcement

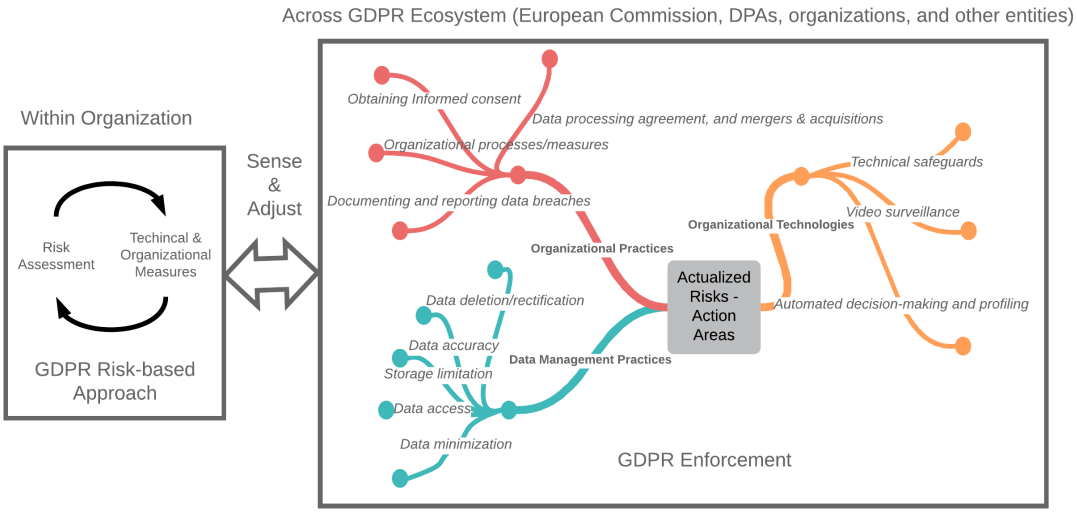


Table 2: Examples of GDPR Fines Resulting from Organizational Risks

Organizational Risk Type	Examples of Fines Imposed by DPAs
Obtaining Informed Consent	Google in France was fined €50 million because of its noncompliant processes for obtaining consent from users.
Documenting and Reporting Data Breaches	A payment service provider in Lithuania was fined €61,500 for processing more data than necessary to achieve the purpose and failing to report a data breach.
Data Processing Agreement, and Mergers and Acquisitions	Marriott Hotels in the U.K. was fined €23.9 million for failure to undertake sufficient due diligence when it bought a third-party company.
Organizational Processes and Measures	A Polish data broker company was fined €219,538 for failing to have proper processes for informing individuals that their data is processed.

Action Area 1: GDPR Risks and Impacts on Organizational Practices

GDPR compliance not only requires implementing organizational measures and processes to ensure information security, but also a good understanding of the roles and duties defined by the regulation, especially data controllers, data processors, DPOs and SAs. Chapter 4 of the GDPR (Articles 24-44) defines the legal obligations of these entities. Article 31 mandates that controllers and processors cooperate with the SA in the performance of its tasks. From our analysis of the GDPR fine cases, we identified four main types of organizational risk: obtaining informed consent; documenting and reporting data breaches; data processing agreement, and mergers and acquisitions; and organizational processes and measures. These four risk types are described below and examples of the fines imposed for each type are shown in Table 2.

Risks of Not Obtaining Informed Consent. Generally, the GDPR prohibits the processing of personal data, unless the data subject has consented to the processing or if the processing is expressly allowed by law. The basic requirements for obtaining valid legal consent are defined in Article 7 of the GDPR and specified further in Recital 32. Consent must be *freely given*, *specific*, *informed*, and *unambiguous*.

In a landmark GDPR case (#1),[13] the French DPA (CNIL) imposed a €50 million fine on Google for its lack of transparency, inadequate information and lack of valid consent for ad personalization. Google stated that it obtains users' consent to process data for ad personalization purposes. However, CNIL took the view that the consent was not validly obtained, because the collected consent was neither "specific" nor "unambiguous." When creating an account with Google, a user could modify some options by clicking on the "More options" button. According to CNIL, however, forcing a user to click on several buttons, nudges the user toward giving consent. Also, the display of ad personalization was pre-ticked. Moreover, before creating an account, the user is asked to tick the boxes "I agree to Google's Terms of Service" and "I agree to the processing of my information as described above and further explained in the Privacy Policy." By ticking these boxes, the user gives consent in full for all the processing purposes carried out by Google (ad personalization, speech recognition, etc.). However, the GDPR requires that specific consent has to be given for each purpose.

Likewise, the GDPR mandates that companies must allow users to easily withdraw consent at any point. In another case (#5), a Polish firm was fined because its mechanism for consent

13 Throughout this article, the numbers in parentheses refers to the "Item #" in the supplementary online material, "A Summary of 93 GDPR Cases," available at https://osf.io/ywbqz/.

Lessons for Obtaining Informed Consent Risks

Risk mitigation measures

- Do not rely on "opt-out" consent mechanisms.
- Obtain separate consent for each purpose—for example, obtain separate consents for direct marketing of your products and for direct marketing of third-party products.
- Help users/customers to easily and clearly understand what they are consenting to—for example, by providing them with an overview of key points and allowing them to drill down into the finer details.
- Make withdrawal of consent as easy as giving consent.

Potential KRIs

- Ratio of number of consents obtained per user to number of business use cases with a user's personal data.
- Number of users who initiate the withdrawal process but do not finish it.

withdrawal (a link included in the commercial information) did not result in quick withdrawal. The DPA ruled that, after clicking on the link, messages addressed to the person wanting to withdraw consent were misleading. Another problem was that the firm forced users to state why they were withdrawing consent, and discontinued the withdrawal process if they failed to indicate a reason.

Risks of Inadequate Documentation and Reporting of Data Breaches. Article 33 of the GDPR (Notification of a personal data breach to the SA) and Article 34 (Communication of a personal data breach to the data subject) set out the obligation to report a data breach to both the SA and data subjects. The SA must be notified no later than 72 hours after the organization becomes aware of a data breach, and the data subjects must be notified without undue delay. These notifications must include the nature of the data breach, the name and contact information of the DPO, the likely consequences of the breach and the measures taken by the data controller to address the breach. However, a personal data breach need not be reported if it is unlikely to result in a risk to the rights and freedom of individuals. Even in such situations, the GDPR requires that organizations keep records of all personal data breaches.

Among our cases, there were organizations that had been fined for not notifying of a data breach in time. For example, a Lithuanian payment service provider was fined €61,500 for insufficient fulfillment of the GDPR data breach obligations. In this case, the data of 9,000 payment details involving 12 banks from different countries were publicly available on the internet from July 9-10, 2018, because of inadequate technical and organizational measures. The Lithuanian Data Protection SA found that not only did the payment service provider not notify it of the breach (#6), but it also processed more data than was necessary..

Risks from the Lack of a Data Processing Agreement, and from Mergers and Acquisitions. The GDPR mandates that organizations can deal with third parties who act as data processors or gain access to personal data only after signing a formal data processing agreement. Failure to conclude an agreement for

Lessons for Documenting and Reporting Data Breaches Risks

Risk mitigation measures

- Notify the SA within 72 hours of any personal data breach, and communicate the breach to the data subjects in plain language without undue delay.
- Record any personal data breaches, regardless of whether they are notifiable

Potential KRIs

- Unclear processes for documenting personal data breaches.
- Unclear processes and roles for determining notifiable data breaches.

Lessons for Data Processing Agreements, and Merger and Acquisition Risks

Risk mitigation measures

- Conduct proper due diligence when making a corporate acquisition, to assess not only what personal data has been acquired, but also how it is protected.
- Ensure the purpose of processing is not different from what is included in the agreement between the parties or entities involved in processing personal data.
- Finalize a data processing agreement before dealing with third parties that may get access to personal data.

Potential KRIs

- No due diligence performed on personal data protection in a past acquisition.
- No specific agreement signed on personal data protection before dealing with a third party

data processing is regarded as an infringement and may lead to a fine or sanctions. For instance, the mayor of a city in Poland was fined because the city dealt with a company that hosted the resources of the city's public information bulletin without a data processing agreement in place (#8).

Mergers and acquisitions can also result in fines relating to the lack of a proper data processing agreement. When planning a merger or acquisition, the due diligence should include an assessment of what personal data will be been handed over and how that data will be protected in the new organization. For example, Marriott International, Inc. was fined €23.9 million (reduced from an initial fine of €110 million) after it acquired Starwood Hotels (#9). A cybersecurity incident occurred in Starwood's systems in 2016 that resulted in a variety of personal data of approximately 339 million guest records being exposed. Marriott acquired Starwood in 2016, but this cyberincident was not discovered until 2018. An investigation by the U.K.'s Information Commissioner's Office found that Marriott failed to carry out sufficient due diligence when it acquired Starwood.

Risks from Failing to Implement Appropriate Organizational Processes and Measures. Articles 37-39 of the GDPR set out the designation, position and tasks of the DPO. These articles require organizations in which the core activities of the controllers or the processors consist of the processing of personal data to appoint a designated DPO. Failure to do so can lead to a fine or sanctions. For example, the Austrian DPA imposed a fine of €50,000 on a controller in the medical sector for not appointing a DPO after six months of processing personal data (#16). In another case, the Romanian National SA fined a bank €130,000 for disclosing the identities and addresses of more than 300,000 data subjects (#15). The SA found that this breach was caused by a failure to implement appropriate organizational controls over processing operations and for failing to employ the necessary safeguards for protecting personal data.

Action Area 2: Technology-Related GDPR Risks and Impacts

New technology offers new opportunities for unauthorized data collection and use, and this threat is the principal problem that GDPR seeks to address. The opening statements of the GDPR mention the new challenges posed by "rapid technological developments and globalization"

Lessons for Organizational Processes and Measures Risks

Risk mitigation measures

- Appoint a DPO and publish the DPO's contact details.
- Devise a breach-detection process, carry out a risk-impact assessment and put a reporting procedure in place to ensure timely actions.

Potential KRIs

- DPO not appointed or DPO contact information not publicly available.
- Unclear processes for data breach detection, risk-impact assessment and reporting of events.

Table 3: Examples of GDPR Fines Resulting from Technology-Related Risks

Technology-Related Risk Type	Example of Fines Imposed by DPAs
Technical Safeguards	A Bulgarian revenue agency organization was fined €2.6 million for having inadequate technical safeguards to properly protect data security
Video Surveillance	A Swedish school was fined €18,630 for using facial recognition technology to monitor the attendance of students.
Automated Decision- Making and Profiling	The Austrian national postal service was fined €18 million for unlawful processing of a customer's large-scale marketing data.

and the unprecedented scale of organizations' use of personal data. Article 1 states:

> *"Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data."*

Our analysis of GDPR fine cases identified three types of technological risk—technical safeguards, video surveillance, and automated decision-making and profiling. These three types of risk are described below and examples of the fines imposed for each type are shown in Table 3

Risks from Inadequate Technical Safeguards. Article 32 of the GDPR requires organizations to consider "the state of the art" in implementing technical and organizational measures for data security. Although the GDPR does not explicitly require personal data to be encrypted, it does require organizations to adopt "appropriate technical and organizational measures," giving "pseudonymisation and encryption of personal data" as examples of such measures.

At 26% of the total, fines resulting from insufficient technical and organizational measures to ensure data security constituted the second largest category of fines in the cases we analyzed (the largest category was 32% for fines resulting from insufficient legal bases for data processing). Our analysis showed that a major shortcoming of technological safeguards is storing sensitive personal data in unencrypted form. In the Marriott case (#9), 5.25 million unencrypted passport numbers of guests (on top of 18.5 million encrypted ones) were stolen, resulting in a fine of €23.9 million. An additional 339 million guest records were also stolen, including full names, mailing addresses, phone numbers, email addresses and arrival/departure information.

Our findings confirm that companies that encrypt sensitive information must ensure that they use a strong encryption method and put the associated technical controls in place. The Hungarian DPA imposed a fine (#46) on an organization for using the MD5 encryption algorithm, which it found was insufficient to protect sensitive data. (MD5 is now considered a weak hash method by industry standards.) Likewise, in the high-profile British Airways data breach in 2018 (#45), where external hackers stole sensitive personal data, the company initially faced a hefty fine of €215 million[14] because the DPA found there were technical shortcomings in the airline's website. The hackers were able to bypass the website controls and modify (by adding just 22 lines of code) the Modernizr library (a common JavaScript module) used on the site. This enabled the hackers to divert traffic from British Airways's website to a fraudulent site from which they harvested the personal details (including name, address, logins, payment card data and travel bookings) of 500,000 customers.

14 The fine was subsequently reduced to €25 million partly due to the impact of Covid-19 on the airline sector.

Lessons for Technical Measures Risks

Risk mitigation measures

- Encrypt (using strong encryption algorithms along with practices such as adding salt) all of the sensitive personal data the organization collects and stores.
- Make sure the security technology is up to date and that the latest software updates are installed.
- Implement a system to force users to have strong passwords.

Potential KRIs

- Number of systems without encryption of personal data.
- Number of critical systems without up-to-date security updates.

In another case related to technical safeguards (#42), a platform affiliated with the Italian Five Star Movement was penalized for using an outdated content management system that was vulnerable to cyberattacks. The platform had several authentication-related weaknesses, including unsalted[15] hashes and weak passwords.

Video Surveillance Risks. When considering data privacy, most managers will likely focus on data fields such as passwords, purchase histories, personal messages and phone numbers. However, in the context of the GDPR, data privacy applies to all sources of information that may identify individuals. That includes pictures and videos from CCTV recordings and even dashcam footage (dashcams record vehicle registration numbers and people's faces).

For example, in December 2018, an Austrian sports betting café was fined because there was insufficient notification about the coverage of its video surveillance camera, which was also recording images of a large part of the adjacent sidewalk (#50).[16] Surveillance of a public space and even the workplace in this way without proper notice, is not permitted under the GDPR.

Risks Related to Automated Decision-Making and Profiling. The GDPR specifies grounds for restricting the use of data, such as the right of a data subject to object at any time to the processing of personal data. This processing includes using personal data for automated decision-making and profiling. Profiling involves the automated processing of an individual's personal data to analyze or predict that person's attributes—e.g., performance at work, health, personal preferences, economic situation and behavior.

The Austrian national postal service was fined €18 million for creating profiles of more than three million customers. These profiles contained information about users' home addresses, personal preferences and habits. The DPA found that the organization was processing data related to the frequency of the packages that were delivered to a certain address and registering how frequently users move to a new address,

15 In cryptography, salt is random data that is used as an additional input to a one-way function that hashes data, a password or pass-phrase. Salts are used to safeguard passwords in storage.

16 There have been similar CCTV-related fines in France (#54), Hungary (#49), Romania (#15) and Sweden (#55). There was also a dashcam-related fine in Austria (#52).

Lessons for Video Surveillance Risks

Risk mitigation measures

- Ensure there is adequate signage about the areas being filmed by CCTV cameras.
- Keep logs of video surveillance processing operations.
- Delete personal image data recorded by CCTV cameras within the recommended timeframe (e.g., 72 hours in Austria), or provide a justification for an extended storage period.

Potential KRIs

- No signage about CCTV coverage.
- Number of CCTV cameras that capture video beyond the perimeter of the organization.
- Number of old CCTV recordings stored without documented justifications..

Lessons for Automated Decision-Making and Profiling Risks

Risk mitigation measures

- Conduct a risk assessment before starting any new automated decision-making or profiling.
- Use anonymized data in profiling activities.
- Inform users and customers about the automated decision-making and profiling that takes place in the organization, where this data is obtained from and what data is used to create profiles.

Potential KRIs

- Number of automated decision-making processes that have not been risk-assessed.
- Number of automated decision-making processes that use nonanonymized data.
- Number of automated decisions not explained in the user agreement or privacy policy.

without any legal basis to do so. Similarly, companies in Cyprus were fined for using the Bradford factor (a human resource management model for measuring worker absenteeism) for profiling and monitoring employees' sick leave.

Action Area 3: GDPR Risks and Impacts on Data Management Practices

Article 5 of the GDPR states: "Data shall be … processed lawfully, fairly and in a transparent manner in relation to the data subject." This article, which is also referred to in Articles 12, 13 and 14, requires organizations to inform data subjects about data processing operations, such as data storage period, restricting processing of personal data to the minimum necessary, and the existence and the predicted consequences of automated decision-making. Moreover, organizations are obliged to inform data subjects about their rights, including access to their personal data, requests for rectification or erasure of personal data and the right to question the accuracy of their personal data. They also need to consider "data minimization" mechanisms to ensure that any personal data is not collected or processed above the minimum necessary and is in compliance with data storage time and accessibility measures.

Our analysis of GDPR fine cases revealed five types of GDPR data management risk: data access, data minimization, storage limitation, data deletion or rectification, and data accuracy. These five types of risk are described below and examples of the fines imposed for each type are shown in Table 4.

Data Access Risks. The GDPR *data access* principle gives data subjects the right to receive additional information on how their personal data is being processed. It therefore obliges organizations to provide users and customers with transparent and easily accessible information about the use of their personal data. Meeting this requirement includes providing data subjects with the means to submit electronic requests, responding to their requests within a predetermined deadline and providing sufficient details to justify any request refusals.

Several of our cases involved companies that had been fined for noncompliance with the GDPR data access principle. For example, a hospital in Cyprus (#61) was fined €5,000 because a patient complained that her request to access her medical file was not satisfied by the hospital (the file could not be identified by the hospital). We also analyzed data-access-related fines in Bulgaria (#60) and Hungary (#63).

Data Minimization Risks. The GDPR's data minimization principle requires organizations to limit the processing of personal data to the minimum necessary. They are not allowed to collect additional personal data that is not needed for offering a specific service. Organizations that are not transparent about how they collect and process personal data can be fined or sanctioned for violating the minimization principle. For example, a hospital in Portugal (#70) was fined €400,000 for allowing indiscriminate access to an excessive number of users' personal data. There are also cases of fines or sanctions resulting from data minimization risks being applied in Belgium (#68) and the Czech Republic (#67).

Storage Limitation Risks. The GDPR requires that organizations do not keep data for longer than required for the purposes for which it was collected. They must therefore determine how long personal data will be stored

Table 4: Examples of GDPR Fines Resulting from Data Management Risks

Technology-Related Risk Type	Example of Fines Imposed by DPAs
Data Access	A Polish sports association was fined €12,950 for failing to respond to referees' request to remove data from its website in a timely manner.
Data Minimization	A Portuguese hospital was fined €400,000 for allowing staff members access to patient data that was unnecessary to perform their jobs.
Storage Limitation	A German real estate company was fined €14.5 million for storing tenants' personal data for longer than required.
Data Deletion or Rectification	A Greek telecoms service provider was fined €200,000 for failing to delete the data of customers who wanted to opt out of telemarketing calls.
Data Accuracy	A Spanish company was €60,000 for disclosing a customer's data to a third party by mistake.

Lessons for Data Access Risks

Risk mitigation measures

- Ensure that data access requests are processed within the predetermined deadline (within one month of receiving the request in most cases).
- Inform data subjects if their personal data is being transferred to an international organization or a third country.
- Have the ability to providing data subjects with a copy of their personal data that is being processed.
- Provide automated responses to inquiries to remove the risk of data subjects lodging complaints with the DPA.

Potential KRIs

- Number of data access requests not processed within the predetermined deadline.
- Number of international organizations with access to users' personal data.
- Number of user complaints about late responses to data access requests.

and document the criteria for determining that period. Noncompliance with this GDPR principle can result in fines. For example, a furniture and home accessories company in Denmark was fined €200,850 for overriding the storage limitation principle (#73). The Danish DPA carried out a supervisory visit to the company and found that it had processed approximately 385,000 customers' data for a longer period than necessary for the purposes for which the data was collected. The company had also failed to specify the deadline for deleting customers' data in its new CRM system and had not documented the procedures it would follow for that deletion. Personal data in its old system had never been deleted. There was also a case of a fine related to the data storage limitation principle in Hungary (#75).

Data Deletion or Rectification Risks. The GDPR requires organizations to delete or rectify an individual's personal data whenever that person requests this, even if there are no specific grounds for the request such as data incompleteness or inaccuracy. To comply with the data deletion principle, companies should implement organizational and technical processes for deleting or rectifying personal data within established time limits (this also applies to third parties that process users' personal data).

Noncompliance with the data deletion or rectification principle can result in fines. For example, a delivery service provider in Germany received a fine of €195,000 for failing to erase the accounts of 10 former customers, even though those customers had not been active on the company's delivery service platform for several

Lessons for Data Minimization Risks

Risk mitigation measures
- Do not collect data that is not needed for the identified purposes.
- Optimize data collection and processing workflow to use personal data only for explicitly stated purposes.
- Apply data screening to eliminate unnecessary data.

Potential KRIs
- Percentage of collected data fields without an explicit purpose.
- Number of staff with access to personal data.

Lessons for Storage Limitation Risks

Risk mitigation measures
- Delete personal data when it is no longer needed.
- Implement and document organizational and technical measures to delete personal data at the end of the storage limit period.

Potential KRIs
- Percentage of users' data without a specific storage limit period.
- Percentage of users' data not deleted after storage limit period.

years (#79). In addition, eight former customers had complained about unsolicited advertising emails from the company despite asking to opt out of such emails. There were also several cases of fines resulting from noncompliance with the data deletion or rectification principle in the Czech Republic (#78), Germany (#79), Latvia (#80), Poland (#77) and Spain (#4 and #82).

Data Accuracy Risks. The GDPR requires organizations to maintain accurate data and enables users to question the accuracy of their personal data. Specifically, the data collected must accurately represent the user and the user's relationship with the organization, must be kept up to date and inaccuracies must be rectified upon discovery. Examples of inaccuracies can range from something as simple as an outdated home address to more complex instances such as incomplete data not required for fulfilling a processing purpose.

Breaches of the data accuracy principle can result in fines or sanctions. For example, an energy supplier in Spain was fined €60,000 (#92) for an error in modifying data in a contract (i.e., mismanaging data accuracy) that led it to breach the principle of confidentiality—the error meant that the complainant's personal data was disclosed to another person who was subject to a restraining order from the complainant. There were also several cases of fines resulting from noncompliance with the data accuracy principle in Bulgaria (#93) and Romania (#89), where organizations were penalized for processing data without providing effective mechanisms for verifying and validating its accuracy (e.g., using

Lessons for Data Deletion or Rectification Risks

Risk mitigation measures
- Delete or rectify data immediately after a user request.
- Document and enforce data deletion procedures for fulfilling users' deletion requests without delay.

Potential KRIs
- Number of incomplete instances of deletion or rectification of users' personal data.
- Unclear organizational and technical processes for deletion or rectification of personal data within the predetermined time limit.

Lessons for Data Management Practices Risks

Risk mitigation measures

- At the data collection stage, take reasonable measures to ensure the accuracy of data collected from users.
- Ensure users are notified if discrepancies are discovered in her/his data.
- Establish processes for preventing inaccurate data (verifying and validating data accuracy) and correcting any inaccurate data.

Potential KRIs

- Number of correction requests received.
- Percentage of personal data items without designed verification and validation measures.

a wrong email address that resulted in sending personal data to the wrong person).

Strategic Actions for Managers and Executives

Organizations can use the lessons learned for each of the 12 types of GDPR risk discussed above to inform their efforts to ensure compliance with the GDPR and assign the necessary resources. To provide managers and executives with actionable guidance, we have created a master checklist of specific questions and actions. This checklist is available in the supplementary online material, available at https://osf.io/hg8ar/. Answering "no" to any of these questions suggests an opportunity to act today to avoid paying tomorrow.

The tactical actions provided by our checklist are complemented by the four overarching strategic actions described below. Together, these tactical and strategic actions provide a solid foundation for managers and executives as they grapple with the challenges posed by the GDPR.

1. Adopt GDPR's Risk-Based Approach When Dealing with Personal Data

The risks and actions discussed in this article are by no means EU-centric. The GDPR has global implications. Regardless of an organization's location, the GDPR has set a high bar for managing any EU resident's personal data. Virtually any organization that deals with personal data must prepare to comply with GDPR requirements. According to a 2020 survey of 2,800 organizations across the globe, only 3% believed that the GDPR did not apply to them (while only 55% were ready for GDPR).[17]

Given the technical and even moral challenges of defining two sets of data protection policies and practices for EU and non-EU consumers, organizations should consider extending the rights that are at the heart of the GDPR to all of their customers worldwide. Microsoft was one of the first firms to announce such a policy.[18] Like any other data protection initiative, complying with the GDPR starts with the organization knowing what personal data it controls, mapping data flows, and assessing privacy risks and impacts on individuals. The lessons learned from our research into GDPR-related fines, together with the risk mitigation measures and risk indicators we identified for each of the 12 types of GDPR risk and the supplementary online checklist of questions, provide a good starting point for an organization's GDPR compliance journey.

2. Ensure Your Organization Keeps Track of Ongoing Developments in the GDPR Landscape

Our analysis identified a comprehensive set of risks associated with the GDPR based on the past enforcement record. But no GDPR checklist can be complete and the GDPR landscape is constantly evolving. For example, in the first three years after the GDPR came

17 "From Privacy to Profit: Achieving Positive Returns on Privacy Investments," *Cisco Systems*, January 2020, available at https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf.

18 See Brill, J. "Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data," Microsoft blog post, May 21, 2018, available at https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/.

into effect, there have not been many cases of administrative fines resulting from unlawful international data transfers.[19]However, one of the potentially critical challenges that organizations, especially multinationals, face is the transfer of EU residents' personal data to a third country outside the EU. Such transfers must guarantee "essentially equivalent" protections in the third country. Under the GDPR, there are only three ways of legitimizing data transfers: (1) adequacy findings[20] (Article 45); (2) appropriate safeguards (Article 46), implemented mainly through the Standard Contractual Clauses (SCC) developed by The European Commission; and (3) derogations or exemptions (Article 49).[21]

Like many other aspects of the GDPR, international data transfers are affected by new developments and regulator decisions. For example, a landmark 2020 ruling by the Court of Justice of the European Union (CJEU), widely known as Schrems II, invalidated the previous mechanism (The Privacy Shield Framework), used for data transfers between the EU and the U.S. At present, firms that perform such data transfers should adopt alternative procedures (e.g., contractual measures or technical measures such as encrypting personal data) that provide an equivalent level of protection. It is generally expected that the EU and U.S. will develop an improved mechanism to replace the Privacy Shield Framework. This is just one example of why IT leaders and DPOs need to monitor developments in the GDPR landscape. Although keeping up with GDPR developments can be challenging especially for small and medium-sized enterprises (SMEs), the risk-based approach in the GDPR does not grant exemptions based on organization size. DPAs are providing practical tools and information seminars to facilitate the implementation of the GDPR by SMEs.

3. Use GDPR Enforcement Evidence for Bringing Organizational Stakeholders Onboard

GDPR enforcement is not just about issuing fines. As stated by the European Data Protection Board (EDPB), DPAs are not "fining machines."[22] The primary objective of the GDPR is to change the culture and behavior of all actors involved in data protection for the benefit of data subjects. Nevertheless, the evidence from GDPR enforcement cases can be a useful tool, especially for IT leaders, for persuading the whole organization about the criticality of data protection, and for prompting managers to carry out proper risk assessments and identify risk mitigation measures.

Justifying investments in data protection technologies and processes has always been challenging for IT leaders. Data protection is a "negative deliverable" because it produces no immediate revenue or efficiency.[23] Data protection investments simply ensure that an organization is insulated from the effects of a probable, but uncertain, negative fallout of a data breach. However, highlighting the potentially massive GDPR fines (the greater of €20 million or 4% of global annual turnover) can help IT leaders build a business case for data protection investments and assigning organizational resources to relevant processes (data mapping, privacy impact assessment, etc.), to technologies (such as pseudonymization tools) and to services (legal counsel). IT leaders can also highlight that, in addition to fines, DPAs can issue sanctions, such as bans on processing, which could have even more detrimental impacts on the organization.

4. Adopt a Strategic Approach When Selecting and Interacting with a Lead DPA

As reflected in the findings of our study, although the GDPR provides harmonized rules across EU member states, there is still a considerable degree of fragmentation in

19 The only publicly announced fine in this category is a recent €8.15 million fine issued to a multinational telecoms company and its service providers by the Spanish DPA. See Brown, M. "European Supervisory Authority Issues €8.15m Fine for International Data Transfer and Processing Failings," *Lexology*, March 26, 2021, available at https://www.lexology.com/library/detail.aspx?g=6c8cd5cc-69dc-49eb-9660-f0177f5c6984.

20 Adequacy findings refer to the European Commission's recognition that a country outside the EU offers an adequate level of data protection. As of March 2021, The European Commission recognizes 12 countries, including Canada, Israel, Japan and New Zealand, as providing adequate protection.

21 Kuner, C. "Article 45 Transfers on the Basis of an Adequacy Decision," in *The EU General Data Protection Regulation (GDPR)*, C. Kuner, L. A. Bygrave, C. Docksey ((Eds.),Oxford University Press, 2020.

22 In a tweet on the official EDPB Twitter account, available at https://twitter.com/EU_EDPB/status/1276183710438699014.

23 Piccoli, G. and Pigni, F. *Information Systems for Managers*: with Cases, 4th edition, Prospect Press, 2019.

enforcement, with different jurisdictions using diverging approaches. In practice, harmonization of GDPR enforcement is still an elusive goal. The fragmentated approaches are partly due to the fact that the GDPR allows each EU member state to legislate in certain areas. One example is the age of consent for children in relation to IT services (Article 8), which varies between 13 (e.g., in Spain) and 16 (e.g., in Germany).

A second and arguably more important cause of fragmentation is the possibility of different interpretations of the GDPR provisions by member states and different policies for GDPR enforcement by different DPAs. For example, when determining GDPR fines, the German DPA employs a five-step model that takes into account parameters such as the organization's worldwide annual turnover, degree of severity of the offense and other offense-related circumstances. In contrast, the U.K. DPA, uses a nine-step model that considers factors such as seriousness, culpability, aggravating and mitigating factors, economic impact and "dissuasiveness" (being effective in persuading organizations not to commit similar violations).

We recommend that IT leaders take into account these country-level differences when selecting the DPA to act as their lead supervisory authority (SA). As explained earlier, the GDPR allows an organization to be regulated by one lead SA in the member state in which its main establishment is located. Businesses, especially multinationals, that can make a strategic decision about where to establish their main presence might select a country with a DPA with a reputation for a more partnering-based approach rather than a fine-based approach. For example, TikTok (the video-sharing social networking service) used to have its main EU presence in the U.K. and Germany. However, in 2020, TikTok moved its main establishment to Ireland so it could take advantage of the "one-stop-shop" facilities offered by the Irish DPA. Many other tech giants, including Facebook, Twitter, Microsoft and Apple, work with the Irish DPA as their lead supervisory authority. In summary, the GDPR's risk-based approach makes it imperative for businesses to be familiar with the specific approaches and practices of their lead SA. It is also possible to consult that SA if high-risk processing cannot be mitigated.

Concluding Comments

The fundamental objective of any regulation is to persuade those who are regulated to comply with the law. Penalty regimes and their associated deterrent capacity are central to influencing the decisions of "rational actors," (i.e., those who rationally calculate the costs and benefits of every action before making a decision), which includes board members and executives of organizations that are subject to the GDPR. The assumption is that rational actors will evaluate the likely benefits and costs of engaging in various types of behavior and reduce risks accordingly.

However, evaluating benefits, costs and risks is difficult if the law is ambiguous, and as we have shown in this article there is considerable ambiguity and fragmentation in GDPR enforcement. Each member state has its own DPA that investigates complaints and can issue fines and sanctions. Our case analysis reveals that DPAs in different countries adopt different practices in dealing with GDPR complaints and issuing fines.

In short, the problem for executives is that the GDPR, as a legal text, provides insufficient clarity for them to act. Moreover, the GDPR explicitly promotes a risk-based approach to data protection. When launching a new service or app or deploying technologies that will be processing or storing personal data, organizations should perform a risk assessment, and implement relevant safeguards and measures. There is no one-size-fits-all mechanism that will ensure compliance with the GDPR. Instead, executives can adjust their decisions relating to data protection by considering how DPAs and the courts enforce the GDPR. Based on our analysis of GDPR-related fines, this article aims to reduce the ambiguities around the GDPR and clarify the issues that executives must address to minimize their organization's risk.

The cost of not mitigating GDPR risks can be huge. As noted earlier, British Airways initially faced a €215 million GDPR fine for a security breach that compromised the personal data of roughly 500,000 customers. That fine was about 6% of the airline's 2018 profit and about €40 per record exposed. In addition, British Airways incurred costs for dealing with the problem, communicating with impacted customers, providing credit check services, dealing with

lawsuits, etc. These costs would have been between €50 to €70 per record, or another €250 million. Hence, the total cost of this one incident could have been about €500 million, or over 10% of the airline's 2018 profit. The cost of mitigating the risk by making sure the web software was secure and updated before it was allowed on the website would have been a tiny fraction of that cost. The key message in this article is that organizations must actively engage with the GDPR, rather than seeing it as a passive box-ticking exercise. They must act now to avoid nasty shocks in the future, including potentially crippling fines. Taking simple actions now can prevent costly infringements.

Appendix A: Case Analysis Methodology

We analyzed cases involving GDPR fines roughly one year after the law came into effect. Most of the cases were made public by a country's DPA. We collected, verified and merged data from several websites[24] that regularly track GDPR fines (reporting a total of more than €140 million in fines). Our final sample included 93 cases of GDPR fines issued between July 2018 and October 2019 in 23 EU countries. To understand the different reasons for these fines, we examined each case and compared, contrasted and classified the cases using established qualitative methods, following an iterative process.[25] For each case, we reviewed multiple texts explaining the fine (including statements by the DPA, court rulings and news items) until we reached a point

24 The main websites used in our review were: 1) https://en.wikipedia.org/wiki/GDPR_fines_and_notices; 2) http://www.enforcementtracker.com/; 3) https://edpb.europa.eu/edpb_en, https://easygdpr.eu/gdpr-fines/; and 4) https://www.lexology.com; and 5) https://iapp.org/.

25 Gioia, D. A., Corley, K. G. and Hamilton, A. L. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational Research Methods* (16:1), July 2012, pp. 15-31.

Appendix B: Summary of the GDPR's Chapters and Articles

Chapter (Articles)	Chapter Title	Description	Implications for CIOs and IT Departments
1 (1 - 4)	General provisions	The aims and scope of the GDPR; provides the essential definitions	• Implement data pseudonymization controls • Pay attention to online identifiers for profiling and identification
2 (5 - 11)	Principles	Rules of processing and protecting personal data and conditions for consent	• Process the data in a lawful manner • Obtain the consent only for the specified purpose and distinguish it from other matters • Provide consent forms in a clear and plain language
3 (12 - 23)	Rights of the data subject	Rights of data subjects, including rectification and erasure, restriction of processing and profiling	• Ensure any communication related to data processing in a concise, transparent, and easily accessible form • Install automated tools (e.g., for responding to data subject access requests in a timely manner)
4 (24 - 43)	Controller and processor	Roles of controller, processors and data protection officers, as well as code of conduct and certifications	• Communicate the data breach to the data subject without undue delay • Perform data protection risk assessment for personal data • Implement appropriate technical and organizational measures (e.g., security of processing using security tools) • Ensure the designation of a data protection officer (DPO) • Keep a log of who accessed what information for when authorities ask for an audit • Cooperate (on request) with the SA when required

(Continued) Summary of the GDPR's Chapters and Articles

Chapter (Articles)	Chapter Title	Description	Implications for CIOs and IT Departments
5 (44 - 50)	Transfers of personal data to third countries or international organizations	Rules for transferring personal data to be processed outside the European Union	• Determine if the organization stores or transfers EU residents' personal data in/to countries outside the EU • Limit the international transfer of data to countries where appropriate data protection is provided
6 (51 - 59)	Independent supervisory authorities (SAs)	Obligations, conditions, tasks and powers of a supervisory authority to be established in each member state	• Stay informed of the guidelines and updates published by SAs (especially the SA of the country of the main establishment of the organization)
7 (60 - 76)	Cooperation and consistency	How supervisory authorities should cooperate with each other and be consistent, as well as the role of the European Data Protection Board	• Be aware of the collaboration of SAs in the EU and consistency in their performance • Understand the structure and role of the European Data Protection Board
8 (77 - 84)	Remedies, liability and penalties	The rights of data subjects to judicial remedies and the fines and sanctions for controllers and processors	• Review the conditions of administrative fines and penalties • Consider implementing effective CRM to deal with complaints at the organizational level
9 (85 - 91)	Provisions relating to specific processing situations	Exceptions to the regulation and specific rules for each member state	• Implement security measures for public access to official documents that contain personal data • Realize specific conditions for the processing of national ID numbers • Adopt safeguards relating to processing for archiving purposes
10 (92 - 93)	Delegated acts and implementing acts	Delegating the acts by the commission and role of the committee	• Acknowledge the delegation of power by the European Parliament or Council to the commission • Adhere to the recommendations by the commission and/or committee
11 (94 - 99)	Final provisions	Relationship of the GDPR with previous directives and agreements, and possible amendments of the union legal acts	• Monitor the legislative changes and review their implications • Contribute to the proposals for possible legislative amendments

of saturation, where new texts were not adding significantly to our existing analysis. In most cases, there were sufficient texts in English.

About the Authors

Saeed Akhlaghpour

Saeed Akhlaghpour (s.akhlaghpour@business.uq.edu.au) is a senior lecturer in business information systems at the University of Queensland Business School, Australia, and a fellow of the Higher Education Academy. He holds a Ph.D. in management from McGill University, Canada. Saeed conducts research on data privacy and cybersecurity (especially in the healthcare sector) and on digital health transformation. He has published in top journals in the fields of information systems, medical informatics and management. He has received national research grants and his research has been mentioned in major news outlets including *The Courier Mail* and *ABC News*.

Farkhondeh Hassandoust

Farkhondeh Hassandoust (ferry@aut.ac.nz) is a lecturer in business information systems at Auckland University of Technology. Her research interests include information security and privacy, IS in healthcare and IS adoption/infusion. Her work has been published in journals and conferences including *Behaviour and Information Technology*, *Journal of the American Medical Informatics Association*, *Australasian Journal of Information Systems*, *European Conference on Information Systems* and *Pacific Asia Conference on Information Systems*. Her research has been supported by grants from Auckland University of Technology Vice-Chancellor's Scholarship, Contestable Research Fund and Internet New Zealand.

Farhad Fatehi

Farhad Fatehi (farhad.fatehi@monash.edu) is a research fellow (digital health) at Monash University, Australia, and an honorary fellow at Centre for Health Services Research at the University of Queensland. He has conducted research on the use of information and communications technology for improving healthcare, and new models of healthcare using digital technologies. His current research is focused on the development, implementation and evaluation of digital health solutions for behavior change in people with chronic conditions.

Andrew Burton-Jones

Andrew Burton-Jones (abj@business.uq.edu.au) is a professor of business information systems at the University of Queensland Business School. He obtained his BCom (Hons) and M. Information Systems from the University of Queensland and his Ph.D. from Georgia State University. Previously, he was an associate professor at the University of British Columbia. Andrew researches how organizations can use IT more effectively (especially in the healthcare sector), how to improve systems analysis and design methods, and how to improve theories and methods in the IS discipline. He is a Fellow of the Association for Information Systems and is currently editor-in-chief of *MIS Quarterly*.

Andrew Hynd

Andrew Hynd (andrew.hynd@holdingredlich.com) is a partner at Holding Redlich Lawyers, Australia, specializing in information technology and procurement. He has over 20 years of experience acting for a range of public and private sector organizations on IT projects, especially software licensing, implementation and support, cloud services, and privacy and data advice. He provides advice to local and international clients on privacy compliance issues, as well as a broad range of issues relating to data, including value capture, management, security and breaches. Andrew was listed in the 2019 to 2022 edition of *The Best Lawyers in Australia for Information Technology Law*.