Received: 26 June 2023 | Accepted: 19 February 2024

DOI: 10.1111/ecin.13213

ORIGINAL ARTICLE

Economic Inquiry

Privacy regulation and firm performance: Estimating the GDPR effect globally

Carl Benedikt Frey[1,2] | **Giorgio Presidente**[2,3]

[1]Oxford Internet Institute, University of Oxford, Oxford, UK

[2]Oxford Martin School, University of Oxford, Oxford, UK

[3]Institute for European Policy-Making, Bocconi University, Milan, Italy

Correspondence
Carl Benedikt Frey.
Email: carl.frey@oii.ox.ac.uk

Funding information
Citi for generous

Abstract

This paper examines how privacy regulation shaped firm performance. Controlling for firm and country-industry-year unobserved characteristics, we compare the outcomes of firms at different levels of exposure to EU markets, before and after the enforcement of the General Data Protection Regulation (GDPR) in 2018. We find that the GDPR had the unintended consequence of harming the profitability of companies targeting European consumers through the cost channel. Technology firms experienced a 2.1% decline in profits, but not in sales. The GDPR increased extra expenses, added to firms wage bills, and accelerated patenting in GDPR-related technology fields. The main burdens have been borne by smaller companies.

KEYWORDS

firm performance, GDPR, innovation, patenting, privacy regulation

JEL CLASSIFICATION

L5, O3, M3

1 | INTRODUCTION

Personal data is an important factor of production in modern economies. It is also a contentious topic for governments and policy makers seeking to balance the data privacy concerns of citizens against the vitality of their economies. Against this background, the European Union passed the General Data Protection Regulation (GDPR) in April 2016. The regulation, which came into force in May 2018, now governs the processing of EU residents' personal data. The key objective was to give individuals more control over their data, making it harder and more expensive for companies to extract. Thus, while the GDPR has received much praise for safeguarding the data rights of individuals, concerns have been raised over its consequences for European competitiveness. And those concerns are not just European, but extend

Abbreviations: AI, Artificial Intelligence; EU, European Union; GDPR, General Data Protection Regulation; ICIO, Inter-Country Input-Output; ICT, Information and Communication Technology; IPC, Intellectual Property Classification; OECD, Organisation for Economic Co-Operation and Development; OLS, Ordinary Least Squares; PPML, Pseudo Poisson Maximum Likelihood; R&D, Research and Development; USD, United States Dollars; WIPO, World Intellectual Property Innovation.

Managing Editor: Silke Forbes

to companies targeting EU markets. According to Forbes, for example, by 2018, U.S. Fortune 500 companies had already spent 7.8 billion USD on compliance.[1]

So far, however, evidence on the economic consequences of the GDPR has mostly been anecdotal, or has centered on web-based outcomes (Aridor et al., 2023; Congiu et al., 2022; Godinho de Matos & Adjerid, 2022; Goldberg et al., 2023; Janssen et al., 2022; Johnson et al., 2023). These efforts, to be sure, are laudable, but as emphasised by Goldberg et al. (2023), a problem with online outcomes is that their measurement is likely biased, precisely because individuals might not consent to websites recording their data following the introduction of stricter privacy rules. In addition, by focusing on online metrics, the existing literature leaves out many important financial outcomes, not least compliance costs caused by the regulation. This could hide the broader impacts of the GDPR and deliver a misleading picture to policymakers interested in its potential unintended consequences.

To fill this empirical void, we examine the impact of the GDPR on firms profits and sales across 31 countries and 22 industries. For our analysis, we use an unbalanced panel of 276,638 patenting firms from ORBIS IP over the period 2011 to 2020. Because companies selling goods and services to EU consumers are subject to the GDPR regardless of where they are incorporated, the global coverage of the ORBIS database makes it particularly suitable for our purpose of analyzing the impact of the GDPR on firm performance.

To identify appropriate treatment and control groups, inspired by Yuan and Li (2019), we create a novel measure of firm exposure to the GDPR based on inter-industry linkages from the OECD Inter-Country Input-Output (ICIO) Tables.[2] For each 2-digit industry-country pair, we calculate the share of output sold to European consumers and use this share to quantify how exposed firms are to the regulation. This is important because the GDPR only concerns personal data.[3] Specifically, by exploiting the breakdown of the ICIO Tables into goods shipped to businesses for intermediate use and final household consumption, we are able to exclude business-to-business transactions which are unlikely to be directly affected by the regulation, and focus our analysis on end consumers. A further important advantage of this approach is that it allows us to control for time-varying, country-industry unobserved heterogeneity, which accounts for potential pre-trends in firms' performance within specific industries.

Conceptually, the GDPR might in principle affect firm performance in two ways. First, it requires companies to develop GDPR compliant processes and technologies, which creates costs and reduces profits. Second, if users incur a cost when prompted to give consent to using their data, they might reduce online purchases, lowering overall sales. In addition, assuming that data is an important input for targeted advertising, which has served to boost sales in the past, a sudden increase in the cost of storing and processing data associated with the GDPR might lead to poorly targeted advertising, which in turn harms performance.

We proceed to investigating the relative importance of these channels. Doing so, we find that the GDPR adversely impacted firm performance mainly through the cost channel. Specifically, our baseline estimates suggest that companies in ICT with a greater exposure to EU customer markets experienced a 2.1% reduction in profits in response to the enforcement of the GDPR, while sales were left unaffected, implying that the new regulation affected companies adversely primarily by adding compliance costs. We bolster this interpretation by showing that the GDPR also increased companies extra expenses, though not operating expenses, suggesting that the negative impact of the GDPR likely is transitory. Such an interpretation rhymes with our finding that the negative impact on profits tapers off a year after the enforcement of the regulation. We also show that firms relying on European digital companies for intermediate consumption saw a decline in profits in response to the new regulation, as they increased R&D expenditure and accelerated patenting to develop GDPR-compliant technologies, which are likely to be one-off investments.

While the relationships identified are robust across a host of specifications, we cannot rule out that exposure to the GDPR, as we measure it, is correlated to unobserved factors. Therefore, we do not necessarily interpret the link between the GDPR and firms' performance as causal. Nevertheless, we continue with caution, utilizing the available data to its fullest to mitigate endogeneity concerns. For instance, a key concern with our approach is that our exposure measure might capture shocks to the EU economy other than the GDPR, like Brexit. Indeed, a firm in the United States selling a large share of output to EU consumers would experience lower profits in this case. Similarly, a foreign firm reliant on EU imports might experience lower profitability if the price of inputs from European markets increases. Hence, for each country-industry pair, we calculate the share of exports and imports to and from each 2-digit EU industry to weight EU changes in value added. The inclusion of demand shifters hedges our estimates against potential confounding shocks unrelated to the GDPR, though it requires us to drop EU companies, for which such changes would be endogenous. This way, we focus our analysis on non-European companies.[4]

To probe the robustness of our results further, we perform several placebo exercises in which we replace our enforcement dummy with alternative year dummies. Reassuringly, these robustness checks do not pick up preexisting trends unrelated to the GDPR that might drive our results. In addition, we perform a series of falsification tests, showing that our exposure variable does not capture any impact among non-digital manufacturing firms or mining companies, where most firms engage in business-to-business transactions, meaning that they are unlikely to be affected by the regulation.

Our paper relates to two literatures. First, a growing body of work examines the economic effects of the GDPR (Aridor et al., 2023; Bessen et al., 2020; Brill, 2011; Campbell et al., 2015; Goldberg et al., 2023; Jia et al., 2021; Johnson et al., 2023; Peukert et al., 2022). For instance, Goldberg et al. (2023) find that the GDPR adversely impacted web traffic and e-commerce sales, while Aridor et al. (2023) provide evidence that it decreased consumer traffic in the online travel industry. In addition, Peukert et al. (2022), Lefrere et al. (2020), and Johnson et al. (2023) show that data privacy regulation reduced data sharing online, but had the unintended consequence of increasing market concentration among web technology vendors. Finally, Jia et al. (2021) document a negative impact of the GDPR on venture capital and angel investments in technology companies. What these studies have in common is that they focus on individual industries, and mostly on online outcomes. We add to this literature by providing the first systematic evidence of the impacts of the GDPR on companies actual profits and sales across a wide range of countries and industries.

Second, while it has been recognised that privacy regulation might affect innovation (Goldfarb & Tucker, 2012), the empirical literature has mostly focused on the *adoption* of specific technologies in healthcare, showing that privacy regulation, which restricts the ability of hospitals to release health information, reduced their adoption of data-intensive medical technologies (Miller & Tucker, 2009, 2011, 2018). In contrast, we examine the effects of data privacy on innovation, documenting an increase in patenting in response to the enforcement of the GDPR in technology industries. Specifically, while Janssen et al. (2022) document a decline in product innovation—measured by the number of apps distributed on Google Play—following the introduction of the GDPR, we document an increase in process innovation, as companies responded by developing GDPR-compliant technologies and processes.[5]

Finally, it must be noted that while we document large negative impacts of the GDPR on firm performance, there might be offsetting benefits to consumers concerned with their privacy, which are left unaccounted for. Thus, in the end, our study is agnostic about the overall welfare implications of data privacy regulation.

The remainder of this paper is structured as follows. Section 2 provides an overview of the GDPR and its implications for companies. Section 3 describes our data and empirical strategy for elucidating the impact of the GDPR on firm performance. Next, in Section 4, we present our results from estimating the effect of the GDPR on firms' profits, sales, and costs. Section 5 further sharpens the focus on the cost side by exploring how companies have responded to the regulation in terms of developing GDPR-compliant technologies. Finally, in Section 6, we outline our conclusions.

2 | THE GENERAL DATA PROTECTION REGULATION

Firms operating within the European Union are subject to its GDPR, which establishes the rules for how the personal data of EU residents may be processed, including browser cookies and IP addresses. The GDPR also applies to firms that are incorporated outside EU countries, provided they target consumers that live in the European Union. While the regulation was passed in April 2016, it only became enforceable in May 2018, giving companies two years to adjust to the changes being introduced. The objective underpinning its adoption was to give individuals more control over their personal data, while at the same time encouraging companies to limit their use of such data for activities like marketing, or to process the data based on an appropriate legal basis, like consent.

By specifying the legal basis under which a company may or may not process personal data, the GDPR affects companies in several ways (Johnson, 2022; Johnson et al., 2023; Skiera et al., 2022). For example, since its introduction, websites are prohibited from sharing user data with third parties, without the consent from each user, and valid consent must be affirmative, which makes data collection more costly and reduces companies' ability to extract personal data. It also gives EU residents the right to access, update, correct, delete, and port their personal data, meaning that firms wanting to process personal data must invest in building, inventing or buying IT systems that fulfil people's rights. In addition, companies that target EU residents are required to encrypt and anonymise any personal data it stores, and must audit their internal data processes to ensure compliance. This includes appointing a data protection officer to oversee data management activities. The compliance costs imposed on companies are in other words significant, especially for those whose business model relies on the processing of personal data. According to PwC (2018), some companies have spent over 10 million EUR annually on GDPR compliance alone since the law became enforceable in May 2018.

However, the cost of failing to comply can be even larger. Fines for non-compliance can reach the larger amount of 20 million EUR or 4% of global revenue. By applying fines to global revenue, rather than revenue from EU countries, the GDPR incentivises multinationals targeting EU residents to abide by its rules, even if most revenue is generated elsewhere. Large fines have already been leveraged on a number of companies across a host of industries, including Google (50 million EUR), H&M (35 million), Telecom Italia (27.8 million), British Airways (22 million), and Marriott (20.4 million). We note that between January 2020 and 2021, the data protection authorities recorded 121,165 data breach notifications—an increase by 19% from the previous year. Over the same period, GDPR fines rose by nearly 40% (DLA Piper, 2021).[6]

In the light of these costs, we conclude that there are compelling incentives for companies to reduce their processing of personal data in response to the adoption of the GDPR. We proceed to investigating its effects on firms' performance across the globe.

3 | DATA AND METHODOLOGY

In the below, we describe the construction of our dataset, discuss our measurement of companies exposure to the GDPR, and outline our empirical strategy.

3.1 | Exposure to the GDPR

To capture the extent to which companies target EU consumers, we begin by constructing a novel GDPR exposure measure based on information on trade flows across 36 2-digit ISIC Rev. 4 industries and 64 countries, from the OECD Inter-Country Input-Output (ICIO) Tables.[7] The ICIO Tables are similar to standard input-output tables. However, they include cross-country industry data on both imports and exports.[8] They also provide a breakdown of products and services sold directly to final consumers, which we exploit to construct our main exposure variable. Such distinction is crucial for our purposes, as it allows to exclude business-to-business transactions that are unlikely to be directly affected by the GDPR, which targets the collection and processing of *personal* data. The ICIO tables also provide information on goods and services sold as intermediate inputs to businesses (business-to-business), which we exploit for robustness checks, as well as to obtain additional results in Section 4.3.

While companies in ICT will be most exposed to the new regulation, the GDPR applies to all companies targeting EU residents, meaning that firms in a host of industries will be affected. Our strategy is to let the data determine its extent of impact across the largest possible number of industries. However, industries other than manufacturing, mining, and ICT are 1-digit industries—like agriculture or wholesale and retail trade. As will be discussed in greater detail, a crucial feature of our empirical specification is the inclusion of country-industry-year fixed effects. To purge our estimates from the broadest set of confounders, while preserving sufficient variation in our data, we focus on industries with available 2-digit industry variation, leaving us with 23,600 companies in ICT, 251,266 manufacturing companies, and 1772 companies in mining.

For each country-industry pair, we calculate the share of products and services sold to EU consumers over total sales to consumers, which we denote by $S_{c,i}^{EU}$. We set 2010 as the base year and use the corresponding file from the ICIO repository. Table 1 presents summary statistics of $S_{c,i}^{EU}$ aggregated for all sectors, as well as for ICT, manufacturing, and mining separately. It shows that on average across all sectors, non-EU companies sell 17% of their output to EU consumers. We note that some countries do not trade at all with the EU, while others sell almost 90% of their output to EU markets. As expected, most of the trade happens across manufacturing industries. In the ICT sector, which plays a central role in our analysis, the exposure variable has a much lower mean. But while the mean is less than 1%, it is subject to substantial variation, which we shall soon turn to exploit. Finally, as expected, most companies in mining do not sell any output to EU consumers. The exceptions are companies in Colombia, India, Kazakhstan, Mexico, Norway and Russia, which according to the ICIO tables sell more than half of their production to EU consumers, including salt, fertilisers, and peat.

Figure 1 shows $S_{c,i}^{EU}$ by country for the three sub-industries of the ICT sector.[9] As already noted, there is substantial variation in exposure across both countries and industries. Importantly for our identification strategy, we do not find evidence that some countries or sub-industries are systematically more exposed to EU consumer markets due to, for

TABLE 1 GDPR exposure variables: summary statistics.

	Obs	Mean	Std. dev.	Min	Max
Sales in all sectors to EU households	1,102,045	0.1695001	0.102941	0	0.8930916
Sales of manufactured goods to EU households	1,102,045	0.1541933	0.1065883	0	0.8930916
Sales of ICT to EU households	1,102,045	0.0067925	0.047078	0	0.388087
Sales of mining products to EU households	1,102,045	0.0010937	0.0215522	0	0.7347566

Note: This table presents summary statistics of our GDPR exposure variables, based on the country-industry shares of output sold to EU consumers in the base year (2010).

Sources: ICIO, OECD.

instance, distance from the EU or the tradability of different products. We observe a similar level of dispersion in manufacturing and mining, as presented in Appendix Figures A1 and A2, respectively.

Finally, it must be noted that while the regulation was passed in April 2016, it only became enforceable in May 2018, giving companies two years to adjust to the changes being introduced. To capture the timing of the regulation, we multiply $S^{EU}_{c,i}$ with a dummy taking the value 1 from 2018 onward, $\mathbb{1}\{t \geq 2018\}$. Thus, we follow a large literature using the timing of regulatory enforcement as an event study (Aghion et al., 2009; Autor et al., 2006; Lu et al., 2017; Lu & Yu, 2015; Moser & Voena, 2012; Watzinger et al., 2020). Specifically, we define the variable $GDPR_{c,i,t}$, which measures exposure to the GDPR for firms in each 2-digit industry i in country c as:

$$GDPR_{c,i,t} \equiv S^{EU}_{c,i} \cdot \mathbb{1}\{t \geq 2018\} \tag{1}$$

3.2 | Firm data

We next turn to constructing our firm-level dataset from ORBIS IP (ORBIS hereafter), provided by the Bureau Van Dijk. In addition to providing matched patent data for a large number of companies around the world, ORBIS also contains information from companies balance sheets and financial statements, including profits and sales. Because companies in a wide range of non-EU countries are also exposed to the GDPR (Figure 1), in terms of the three ICT related industries discussed above, the global coverage of the ORBIS database makes it particularly suitable for our purpose of exploring the GDPR effect on firm performance.

Bajgar et al. (2020) has examined the coverage and representativeness of the balance sheets' information provided by ORBIS in great detail. They show that the ORBIS database suffers from one important limitation, which is that the firms in the dataset are disproportionately large, old, and productive. This means that we have good coverage of large top-performing firms but an under-representation of firms at the bottom-end of the productivity distribution. Another concern is that firms appearing and disappearing in the dataset reflects changes in coverage rather than actual entry and exit. For our purposes, however, these drawbacks are not major concerns since we are interested in average within-firm changes in outcomes, as opposed to business dynamics and changes in the size distribution of companies.

We begin by performing extensive data cleaning following Kalemli-Ozcan et al. (2019) and Bajgar et al. (2020).[10] We further restrict our sample further so that each firm has non-missing observations for all outcome variables considered. As noted in Section 2, the GDPR might have a substantial impact on firms' *costs*. A virtue of our dataset is that we also have information on gross profits, which allows us to capture compliance costs, unlike the existing literature which focuses more narrowly on the revenue impact of the GDPR or relies proxies of sales based on online activity (Aridor et al., 2023; Goldberg et al., 2023; Johnson et al., 2023).

In addition, to mitigate endogeneity concerns as discussed further below, we drop EU companies. This approach yields an unbalanced panel of 276,638 patenting firms operating in 22 2-digit industries and 31 countries for the period 2011 to 2020, leaving us with over one million observations. Based on this sample, Table A1 presents the summary statistics of the main variables used in our empirical analysis. In terms of annual coverage, every year between 2011 and 2018 includes approximately 10% of total observations. For the year 2019, this figure somewhat declines to around 5%, while 2020 contains only 0.3% of our sample. This gives us 2 years of good data coverage to identify the impact of the

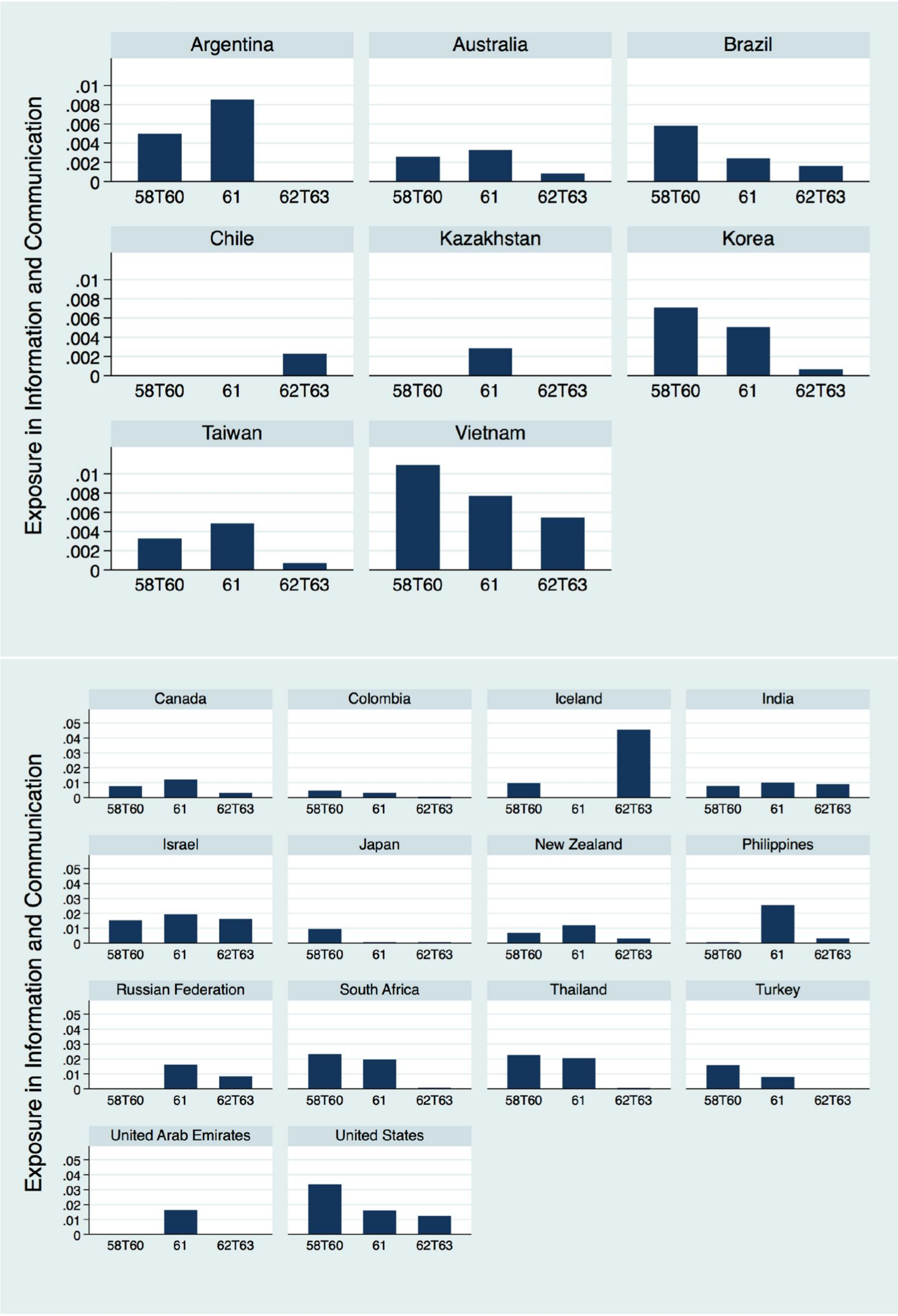

FIGURE 1 GDPR exposure across countries and industries based on the ICT sector. This figure shows the country-industry share of ICT industry output sold to EU consumers in the base year (2010). Industry "58T60" includes "Publishing activities", "Motion picture, video and television program production, sound recording and music publishing activities", and "Programming and broadcasting activities"; industry "61 - Telecommunications", and industry "62T63", which includes "Computer programming, consultancy and related activities" and "Information service activities". Industry codes are based on ISIC rev. 4, available at https://unstats.un.org/unsd/classifications/Econ/Download/In%20Text/ISIC_Rev_4_english_structure.Txt. Sources: ICIO, OECD.

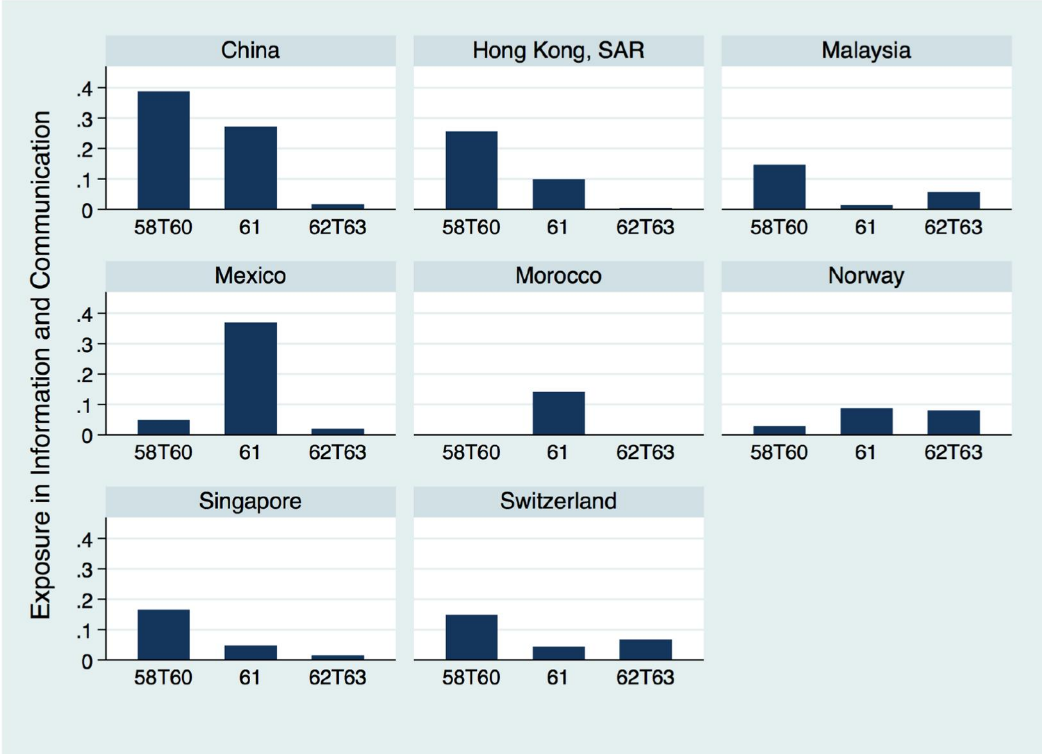

FIGURE 1 (Continued)

GDPR. It also means that we do not have to be concerned about potential confounding effects from the COVID-19 pandemic.

3.3 | Empirical strategy

In our analysis, we run the following regression:

$$Y_{f,c,i,t} = \beta_0 + \beta_1\, GDPR_{c,i,t} + u_f + u_{c,j,t} + u_{i,t} + \varepsilon_{f,c,i,t} \qquad (2)$$

where $Y_{f,c,i,t}$ represents an outcome of firm f, operating in country c, within a 2-digit industry i, in year t. The term $GDPR_{c,i,t} = S_{c,i}^{EU} \cdot \mathbb{1}\{t \geq 2018\}$ is similar to a "shift-share" variable, where the identification of β_1 is based on differential firm-level outcomes before and after 2018 (the "shift") for firms with varying exposure to EU consumer markets (the "share").

Our identification strategy builds on the assumption that $GDPR_{c,i,t}$ does not pick up shocks other than the GDPR. In particular, we assume that there are no differential characteristics or pre-trends affecting firms more reliant on EU consumer markets relative to others. To that end, we include firm fixed effects u_f, to absorb all time-invariant unobserved differences and mitigate the possibility of issues related to the use of an unbalanced panel. In addition, to alleviate concerns over the violation of the parallel-trend assumption, in model (2) we include country-1-digit industry-year fixed effects, $u_{c,j,t}$, where j corresponds to either mining, manufacturing, or ICT.[11] We further note that $u_{c,j,t}$ acts as a country-industry-specific price deflator and absorbs the confounding effect of different currencies. It also mitigates the potential endogeneity in the timing of policy adoption and enforcement (i.e., non-random treatment timing), although the adoption of the GDPR is unlikely to be driven by concerns over economic performance, as the EU recognized the need for data protection already in 1995, when it passed the European Data Protection Directive in response to the proliferation of the Internet. Since identification of β_1 is based on country-2 digit industry-year variation, we cannot include fixed effects with the same level of variation. However, we can still account for common 2-digit industry shocks (e.g., advances in technology) by including 2-digit industry-year fixed effects, $u_{i,t}$, in model (2).

A final concern is that EU-specific shocks unrelated to the GDPR naturally would affect more firms with stronger trade relationships with the EU. For instance, an exchange rate shock might affect the performance of the companies in the Euro area, and as a result the performance of all firms with strong trade relationships with the EU. To account for potential EU shocks unrelated to the GDPR, we calculate the share of exports and imports with 2-digit EU industries for each country-2-digit-industry pair. We use such shares to weight EU industry-specific changes in value added calculated as:

$$D_{cit}^{EU} = \sigma_{cij} \cdot \Delta VA_{jt}^{EU}$$

where σ_{cij} is the share of total trade from country-industry pair $\{c, i\}$ with EU industry j in the base year, and ΔVA_{jt}^{EU} is the log-change in real value added between $t-1$ and t in EU industry j.[12] Clearly, we exclude European firms from the sample to avoid the endogeneity of D_{cit}^{EU} and EU firm performance in their respective industries. We also normalize our exposure variable to have zero mean and unitary standard deviation, so that we can interpret β_1 as the impact of the GDPR on firms profits and sales in industries that are highly exposed to EU consumers. Since the $GDPR_{c,i,t}$ varies at the country-2-digit-industry-level, we cluster errors accordingly across all specifications.

4 | THE GDPR AND FIRM PERFORMANCE

In principle, there are two key channels through which the implementation of the GDPR can affect firm performance: (i) by adding compliance costs, or (ii) if users incur a cost when prompted to give consent to using their data, then there might be a reduction in online purchases. Compliance costs naturally reduce profits, but do not necessarily affect sales. A reduction in online purchases, in contrast, would reduce sales.

We next turn to exploring the impacts of the GDPR on companies through these channels. Table 2 presents our main results, which are obtained by estimating Equation (2). In columns 1 and 2 we present our estimates for all firms in ICT, manufacturing, and mining. The coefficient for profits in column 1 is negative but not statistically significant, while the coefficient for sales in column 2 is positive, but also insignificant. In other words, we do not find any significant average impact of privacy regulation on financial performance across our full sample. However, as expected, the EU demand shifters have a positive and highly significant coefficient, in line with the simple intuition that economic conditions within the EU affect the performance of firms relying more on the consumer market of the European Union.

TABLE 2 Estimating the GDPR effect on profits and sales.

	(1) Profits	(2) Sales	(3) Profits	(4) Sales
Exposure to GDPR (sales of all sectors to EU households)	−0.012	0.016		
	(0.030)	(0.011)		
Exposure to GDPR (sales of ICT to EU households)			−0.021***	0.004
			(0.007)	(0.004)
EU industry demand shifter	0.022***	0.006***	0.022***	0.006***
	(0.005)	(0.002)	(0.005)	(0.002)
Observations	1,055,037	1,056,159	1,055,039	1,056,159
R-squared	0.672	0.944	0.672	0.944
Plant FE	Yes	Yes	Yes	Yes
Country × 1-dig-industry × year FE	Yes	Yes	Yes	Yes
2-dig-industry × year FE	Yes	Yes	Yes	Yes

Note: This table shows OLS estimates based on Equation (2). The dependent variables are expressed in logs. Exposure to the GDPR is the 2010 (base year) share of output sold to European consumers in each country-2-digit industry pair, interacted with a dummy taking value 1 from 2018 onward. Standard errors are clustered at the country-2-digit industry-level.

In columns 3 and 4, we sharpen our focus on companies in ICT. We note that in this case, the coefficient for profits is negative and significant at the 99% statistical level. It implies that profits were 2.1% lower among the firms most exposed to EU consumer markets after the enforcement of the GDPR. At the same time, the coefficient of sales in column 4 is very small and not statistically significant. We take these findings to suggest that the GDPR reduced firm performance primarily through the cost channel, rather than by reduced online activity, putting downward pressure on sales.[13]

Of course, it might be that non-EU producers do not sell their products and services online to EU consumers directly, but rather through EU retail firms. If that is the case, this would manifest itself through a reduction in European companies' sales. To explore this possibility, we estimate our specification using two alternative samples. The first includes also EU companies, while the second focuses exclusively on firms based in the EU. Despite the endogeneity concerns discussed above, this test is informative in ruling out the possibility that a reduction of online traffic due to the GDPR is responsible for the decline in firms' financial performance.

The results from this exercise are presented in Appendix Table A2. We note that when we keep EU companies in columns 1–2, the results are qualitatively identical to the baseline—i.e., the GDPR has a negative effect on profits but not on sales. In columns 3–4, we go one step further and estimate our regression specification in a sample of EU companies only. Also in this case, the compliance cost channel remains the only relevant one. Thus, endogeneity issues notwithstanding, we take this evidence to suggest that a decrease in online traffic due to the GDPR is unlikely to have hampered firm performance. Moreover, we note that the absent impact on sales rhymes with previous studies. For instance, Zhuo et al. (2021) finds that online activity did not decrease significantly after the GDPR came into force, just likeAridor et al. (2023) does not find any significant impact on revenues of an online travel intermediary. Finally, Goldberg et al. (2023) presents estimates of the impact of the GDPR on e-commerce revenues. Focusing on a restricted sample of 1500 firms using Adobe Analytics, they only find a small impact on revenues (−0.6%).

4.1 | Pre-trends

To further alleviate the concern that our exposure variable picks up shocks unrelated to the GDPR, or reflects pre-trends affecting firms with high exposure to EU consumer markets disproportionately, we exploit industry heterogeneity in a number of ways. First, if our exposure variable based on ICT sales captures EU trends unrelated to the GDPR, then the same should be true for other tradable industries with an even stronger exposure to EU consumer markets, like manufacturing. Second, industries relying at most marginally on marketing and online advertising, such as mining, is unlikely to be strongly affected by the GDPR.

Building on this intuition, we run our baseline specification for mining and manufacturing separately as falsification tests. The results from this exercise are presented in Appendix Table A3. We note that the coefficients for profits and sales in both industries are statistically insignificant. We find the results of these placebo regressions reassuring. Indeed, if an economy-wide shock unrelated to the GDPR is captured by our exposure measure based on ICT sales to EU consumers, it should also affect the sales of manufactured goods to EU consumers.

To further check whether our estimates might be affected by pre-trends, we run a series of tests in which we replace $\mathbb{1}\{t \geq 2018\}$ with dummies for each year of our sample—i.e., $\mathbb{1}\{t \geq 2012\}$, $\mathbb{1}\{t \geq 2013\}$, etc. The findings for each alternative year dummy are presented together in Appendix Figure A3, which plots the resulting point estimates and 99% confidence intervals. Reassuringly, the coefficients are not statistically significant before 2017, when it becomes negative and significant. The fact that our design picks up a negative trend in profits already in 2017 is not surprising since firms are likely to have incurred compliance costs in advanced of the actual enforcement of the regulation. Indeed, the very purpose of adopting the GDPR and making it enforceable only from 2018 was to give firms time to adjust and invest in becoming compliant.

We further note that the coefficient becomes statistically insignificant beginning in 2019. This speaks to the intuition that most costs associated with the GDPR are likely to be transitory, echoing also the short-lived effects of the GDPR documented by Johnson et al. (2023). The large and very imprecisely coefficient estimated for 2020, on the other hand, simply reflects the sharp decline in the number of observations (see Section 3). We conclude that our baseline estimates do not simply pick up confounding shocks. Indeed, we find no evidence of significant differences in profitability between treated (i.e., firms highly exposed to EU markets) and untreated firms before the policy shock. This reassures us of the validity of the parallel pre-trends assumption.

4.2 | Compliance costs

We next explore the nature of the compliance costs generated by the GDPR, which might stem, for instance, from the hiring specialised personnel, or expenditure on new IT systems to manage personal data securely. To do so, we exploit available measures of firm expenses in ORBIS, allowing us to shed some light on the types of costs associated with the GDPR. Our results are presented in Table 3. We note that the GDPR did not increase operating costs (column 1), but rather extra expenses (column 2), which are not recurring and thus not directly related to core business of the company. This is consistent with the view discussed above—that the GDPR has incurred new fixed costs, due to, for instance, one-off updating of IT systems. In addition, we find that the wage bill of companies is also positively affected by the GDPR (column 3). This is unsurprising since one requirement of the regulation is the hiring of a dedicated data protection officer to ensure GDPR compliance. It also speaks to anecdotal evidence of companies hiring extra personnel for the handling personal of data.[14]

4.3 | ICT imports

Besides generating compliance costs, the GDPR might have reduced profits by making it harder to gather and process personal data. Indeed, it is possible that the GDPR has made personal data "scarce" and thus more expensive. To explore this possibility, we include in Equation (2) a variable measuring the exposure of firms to imports of IT products and services from EU companies. Formally, this variable is defined as:

$$GDPR_{c,i,t}^{impICT} \equiv M_{c,i}^{EU} \cdot \mathbb{1}\{t \geq 2018\}$$

where $\equiv M_{c,i}^{EU}$ is the share of ICT products and services imported from EU companies in the base year. The results from this excise are presented in Table 4. We note that companies exposed to ICT imports from Europe have been adversely impacted in terms of profitability (column 1). The coefficient is statistically significant and larger in magnitude than our baseline exposure variable. We take this to imply that the GDPR has acted as a tax on data for digital firms within the EU, generating costs that have been passed on to ICT-using companies around the world. Although the coefficient of $GDPR_{c,i,t}^{impICT}$ (−0.022, s.e. = 0.01) is larger than the coefficient of $GDPR_{c,i,t}$ (−0.016, s.e. = 0.007), the latter is still statistically significant. This suggests that both compliance and "input costs" are responsible for the negative impact of the GDPR on firms' financial performance.

TABLE 3 Estimating the GDPR effect on corporate expenses.

	(1) Operating expenses	(2) Extra expenses	(3) Cost of employees
Exposure to GDPR (sales of ICT to EU households)	0.004	0.209***	0.101**
	(0.004)	(0.016)	(0.048)
EU industry demand shifter	0.002*	0.015	0.002
	(0.001)	(0.017)	(0.002)
Observations	930,927	510,123	353,650
R-squared	0.951	0.636	0.864
Plant FE	Yes	Yes	Yes
Country × 1-dig-industry × year FE	Yes	Yes	Yes
2-dig-industry × year FE	Yes	Yes	Yes

Note: This table shows OLS estimates based on Equation (2). The dependent variables are expressed in logs. Exposure to the GDPR is the 2010 (base year) share of output sold to European consumers in each country-2-digit industry pair, interacted with a dummy taking value 1 from 2018 onward. Standard errors are clustered at the country-2-digit industry-level.

TABLE 4 Estimating the GDPR effect of ICT imports from EU companies.

	(1) Profits	(2) R&D expenses
Exposure to GDPR (sales of ICT to EU households)	−0.016**	0.005
	(0.008)	(0.031)
Import of ICT from (EU companies)	−0.022**	0.073**
	(0.010)	(0.032)
EU industry demand shifter	0.022***	−0.000
	(0.005)	(0.010)
Observations	1,055,039	114,184
R-squared	0.672	0.849
Plant FE	Yes	Yes
Country × 1-dig-industry × year FE	Yes	Yes
2-dig-industry × year FE	Yes	Yes

Note: This table shows OLS estimates based on Equation (2). The dependent variables are expressed in logs. Exposure to the GDPR is the 2010 (base year) share of output sold to European countries in each country-2-digit industry pair, interacted with a dummy taking value 1 from 2018 onward. Import of ICT from EU companies is the share of ICT goods and services imported from European firms, interacted with a dummy taking value 1 from 2018 onward. Standard errors are clustered at the country-2-digit industry-level.

4.4 | Size heterogeneity

While our results so far show that the GDPR has reduced firm performance on average, they are silent about its impact by firm size. As is well-known, large firms typically have more technical and financial resources to comply with regulations (Brill, 2011), invest more in lobbying (Bombardini, 2008), and are more able to obtain consent for personal data processing from individual consumers (e.g., Goldfarb & Tucker, 2012; Johnson et al., 2023; Peukert et al., 2022). Indeed, in response to the GDPR, Facebook has notably expanded its global workforce, recruiting approximately 1000 professionals including engineers, managers, and lawyers. Furthermore, the company significantly increased its EU lobbying budget in 2017, doubling the expenditure from the previous year coinciding with the announcement of GDPR. And this trend is not unique to Facebook; as reported by LobbyFacts.eu, Google, Facebook, and Apple are now listed among the top five corporate entities in terms of lobbying expenditures in the EU, each allocating annual budgets exceeding €3.5 million. Thus, it stands to reason that small companies might be disproportionately negatively affected by the regulation.

However, as discussed in Section 3.2, the ORBIS database tends to be skewed towards larger and more productive firms, which means our sample is not ideally suited for analyzing issues related to firm size. Nevertheless, bearing these data constraints in mind, we explore the heterogeneity in our sample, employing different measures of firm size, including sales, employment, and total assets. Specifically, we construct a dummy variable equal to 1 if the company is larger than the country average value of the respective measure. This approach helps us to account for cross-country structural differences in business demographics, as well as the fact that the values of sales and total assets are expressed in different currencies across countries. Since non-EU country-industry pairs with a high exposure to EU markets might be over-populated by large companies, as larger companies are more likely to export, for this exercise we keep European firms in our sample in an attempt to mitigate the issue of representativeness.[15]

Our results are presented in Appendix Figure A4, which report the estimated marginal impact for small and large firms, and the associated 90% confidence intervals.[16] In Panel (a), we consider size as measured by sales, revealing no differential impact. When we measure size in terms of employment, as in Panel (b), however, we note that the point estimate is roughly 2% points larger in absolute terms for small firms relative to their larger counterparts. Finally, since employment might not accurately capture size when it comes to digital firms, Panel (c) exploits total assets (tangible and intangible) as a proxy of firm size. Also in this case, the negative estimated coefficient for small firms is negative and statistically significant, while the coefficient for large firms turns out insignificant. Overall, even in a sample that is overwhelmingly skewed towards large and productive companies, we find support for the view that the GDPR has disproportionately adversely affected smaller companies. We further note that sales are not affected by the GDPR, irrespective of the size measure employed, consistent with our baseline results. That said, we emphasize that these findings must be interpreted with caution because of the sampling constraints highlighted above.

5 | GDPR-INDUCED INNOVATION

To gauge how firms have responded to the surge in input costs and compliance requirements brought by the GDPR, column 2 of Table 4 explores its impact on their R&D expenditure.[17] The coefficient of the input measure $GDPR_{c,i,t}^{impICT}$ is positive and significant, suggesting that firms have intensified their innovative efforts to cope with more expensive imported ICT goods, which has seemingly reduced their profits.

More broadly, there are good reasons to believe that companies have devoted significant resources to the development of GDPR-compliant processes and technologies. Taking a closer look at some recent patent documents, we note that these include applications for technologies like a "System and method for providing general data protection regulation (GDPR) compliant hashing in blockchain ledgers", which guarantees a user's right to be forgotten in compliance with the GDPR. Another example is a "Data Consent Manager", displayed in Appendix Figure A7, which is a computer implemented method for managing consent for sharing data. The patent document notes that failing to comply with the GDPR "can result in adverse consequences for any persons or organizations found to be mishandling data", which the technology sets out to mitigate.

Crucially, for our purposes, ORBIS provides a unique identifier for the applying firm which is linked to each patent application. This allows us to track companies and their inventive efforts each year. However, since only a subset of all patenting companies report information on their industry of operation, which we need to implement our empirical specification (2), we are only able to match 50% of the total number of patenting companies in ORBIS.

To identify GDPR-related patents, we follow a keyword-based approach, similar to Agrawal et al. (2019). Specifically, we use PATENTSCOPE, provided by the World Intellectual Property Organization (WIPO), which allows us to keyword search 95 million patent documents globally.[18] Importantly, as shown in Appendix Figure A5, PATENTSCOPE delivers a technical description and the Intellectual Property Classification (IPC) code for each patent.[19] We deem patents to be plausibly affected by data privacy regulation if they contain, in any section of the patent document, words such as "privacy", "data sharing", "data consent", "user data", or "personal data". Based on this approach, we note that the vast majority GDPR-related patents fall into two IPC codes: "G06 - Computing; calculating or counting"; and "H04 - Electric communication techniques".

Panel A of Appendix Figure A6 shows the results from a search for records including at least one term, which yields 884,625 patents. The only IPC codes not included in categories G06 and H04 are "A61K - Preparations for medical, dental or toilet purposes" and "C12N - Microorganisms or enzymes", which represent less than 5% of the patents identified. Reassuringly, these patterns are extremely consistent across different queries. For example, in Panel B of Appendix Figure A6, we report the results for patents containing all of the above mentioned search terms, which yields 9493 patent documents. Also in this case, the categories G06 and H04 account for almost the entire set of patents identified. The one exception is "G16H - Healthcare informatics", which accounts for roughly 2% of all patents. Finally, we search for different combinations of two or more terms. Panel C of Appendix Figure A6 shows the results of a query for "privacy" and "data", which yields a total of 225,148 patents. In this case, the only IPC code outside the broader G06 and H04 categories is "A61B - Diagnosis' surgery; identification", which accounts for about 1% of total patents.

Having computed the number of GDPR-related patents over time, we regress patent counts on our exposure variable using a Pseudo Poisson Maximum Likelihood (PPML) estimator, which is needed to deal with count dependent variables, and is more robust when datasets contain many zeros (Correia et al., 2020). The results from this exercise are presented in Table 5.[20] As shown in column 1, we find no statistically significant impact of the regulation on total patent counts, neither for the baseline exposure measure, nor for exposure to imports of IT products and services from EU companies. However, for the latter, the impact on GDPR-related patents in column 2 is positive and statistically significant. This suggests that rather than sourcing data analytics products from EU companies, whose quality (price) might have been reduced (increased) by the GDPR, non-EU companies might be developing their own GDPR-compliant technologies for their operations in EU markets. Whether the increase in patenting, which seemingly reflects adjustment to the new regulatory environment, will lead to higher productivity growth in the future, is a topic we leave for future research.[21]

TABLE 5 Estimating the GDPR effect on patenting.

	(1) Total patents counts	(2) GDPR-related patent counts
Exposure to GDPR (sales of ICT to EU households)	0.012	−3.971
	(0.015)	(4.095)
Import of ICT from (EU companies)	−0.020	0.540**
	(0.029)	(0.272)
EU industry demand shifter	−0.000	0.130**
	(0.003)	(0.066)
Observations	273,467	2295
Plant FE	Yes	Yes
Country × 1-dig-industry × year FE	Yes	Yes
2-dig-industry × year FE	Yes	Yes

Note: This table shows PPML estimates of the impact of the GDPR on innovation. The dependent variables are expressed in counts of patents. Exposure to the GDPR is the 2010 (base year) share of output sold to European consumers in each country-2-digit industry pair, interacted with a dummy taking value 1 from 2018 onward. Import of ICT from EU companies is the share of ICT goods and services imported from European firms, interacted with a dummy taking value 1 from 2018 onward. Standard errors are clustered at the country-2-digit industry-level.

6 | CONCLUSIONS

The GDPR has been celebrated globally. According to *The New York Times*, for example, the new privacy law makes Europe "the world's leading tech watchdog."[22] In Silicon Valley, leading technology companies have been forced to comply with the regulation to be able to target customers in Europe. Meanwhile, countries like Brazil, Canada and South Korea have followed suit, passing similar data protection laws beginning in 2020. "If we can export [the GDPR] to the world, I will be happy", Vera Jourova, the European commissioner in charge of data privacy, recently explained.

Given that the GDPR is swiftly becoming the blueprint for privacy protection globally, understanding its economic consequences is crucial. To the best of our knowledge, this paper provides the first systematic evidence on the impact of the GDPR on firm performance across a wide range of countries and industries, comprising the bulk of the real economy. Our analysis builds on the simple intuition that the GDPR can affect firm performance in two ways: either by adding costs, or by lowering sales, if users incur a cost when prompted to give consent to using their data.

We find the first channel to be quantitatively more important across all specifications. Unsurprisingly, we also find that digital technology companies have carried the main burden of privacy regulation. Indeed, our estimates suggest that technology firms targeting EU markets experienced a 2.1% reduction in profits. We further bolster this finding by showing that the GDPR also increased non-operating expenses as well as firms wage bills. This speaks to anecdotal evidence suggesting that several technology companies have deployed large teams to overhaul their privacy settings and to redesign products to become GDPR-compliant. Facebook, for example, has reportedly added some 1000 engineers, managers, and lawyers globally in response to the new regulation.[23] Yet in line with pioneering work by Goldberg et al. (2023), Campbell et al. (2015) and Peukert et al. (2022), documenting that smaller firms have faced more significant challenges due to the GDPR across various dimensions, our findings also suggest that smaller companies have suffered more in terms of profitability.

Moreover, in addition to adding compliance costs, we show that the GDPR has reduced the profits of companies relying on inputs from digital companies within the European Union. We take this to imply that the GDPR has acted as a tax on data, which has been passed on to companies reliant on data-intensive inputs, like targeted advertising. Additionally, we observe that in response to rising costs associated with compliance and inputs, companies have boosted their investments in research and development, particularly in the area of privacy technology. This increase in R&D expenditure and a surge in patent applications for privacy technologies have further contributed to a decrease in these companies' profits.

That said, our findings must interpreted with caution. First, the GDPR has only recently become enforceable and the negative impacts on firm performance we observe may in large part reflect temporary adjustment costs. For example, the increase in patenting in response to the regulation, documented above, is likely to reflect one-off investments in new GDPR-compliant technologies, which put downward pressure on profits in the short-term. Second, if the GDPR gradually becomes a global standard as more countries adopt similar regulations, companies targeting EU markets will become less disadvantaged over time. Finally, while we find that the GDPR has had large negative impacts on firm performance, it must be noted that our estimates are silent on its aggregate welfare effects, which must also account for potential benefits to citizens concerned with data protection. We deem this to be a fruitful future line of inquiry.

ACKNOWLEDGMENTS

We are grateful to Citi for generous funding and to Arshia Mehta and Leopoldo Lazcano for excellent research assistance. We also thank the participants of the OMPTEC working group for valuable suggestions.

DATA AVAILABILITY STATEMENT

The data that supports the findings of this paper are partially subject to third-party restrictions. After obtaining a license from Bureau van Dijk, the data can be downloaded from https://login.bvdinfo.com/R0/Orbis. The openly accessible data used in the paper can be obtained from https://doi.org/10.3886/E197921V4.

ENDNOTES

[1] Smith, O. (2018). The GDPR Racket: Who's Making Money From This $9bn Business Shakedown. Forbes, May 2. Moreover, Bessen et al. (2020) examines how AI startups (of which most are US-based) responded to the GDPR and finds that "These startups are reallocating their limited resources and creating new positions to deal with the implications of this regulation." They also find that "firms with customers in Europe are significantly more likely to create a new position to handle GDPR-related issues or to reallocate firm resources due to GDPR."

[2] Specifically, Yuan and Li (2019) analyze EU hospitals' financial performance based on their reliance on data to capture their GDPR exposure.

[3] Personal data is defined as any information that relates to an identified or identifiable living individual (https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en).

[4] However, we also present robustness tests in which we keep EU companies.

[5] Martin et al. (2019) also finds that GDPR negatively impacted startups by leading to product abandonment and restricting access to essential data for AI development.

[6] DLA Piper (2021). GDPR fines and data breach survey: January 2021. https://www.dlapiper.com/en/us/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/.

[7] Specifically, the ICIO Tables are based on 819 industries, comprising all sectors of economic activity, which have been aggregated by the OECD. For example, "Mining", "Manufacturing" and "Information and Communications" (ICT) correspond to the 1-digit industries B, C and J in ISIC rev. 4, which in turn consist of several 2-digit industries. ICT, on the other hand, consists of the following codes: (i) "58T60", including "Publishing activities", "Motion picture, video and television program production, sound recording and music publishing activities", and "Programming and broadcasting activities"; (ii) "61 - Telecommunications", and (iii) "62T63", which includes "Computer programming, consultancy and related activities" and "Information service activities". In similar fashion, "Manufacturing" is composed by sixteen sub-industries, while "Mining" has three sub-industries.

[8] The diagonal blocks of the ICIO Tables are standard input-output tables, while the off-diagonal blocks represent inter-country flows.

[9] We group countries in different panels based on their exposure to improve readability.

[10] See Appendix B 1 for a detailed description of the data cleaning procedure.

[11] For instance, the fixed effects would absorb the impact of shocks affecting Chinese manufacturing firms, which are highly exposed to EU consumers, but not Mexican manufacturing firms, which are less exposed.

[12] Industry value added is the value added-weighted average across EU countries.

[13] Consistent with a negative impact on profitability, Jia et al. (2021) find that financing deals, especially for data-related business-to-consumer technology ventures, were negatively impacted by the GDPR.

[14] Satariano, A. (2018). G.D.P.R., a New Privacy Law, Makes Europe Worlds Leading Tech Watchdog. The New York Times, May 24.

[15] We verify that in the sample the average firm size is lower for EU firms than for non-EU ones. Specifically, we note that the EU/non-EU ratio of small firms is 47%/44% in terms of sales, 40%/17% in terms of employment, and 50%/40% in terms of total assets.

[16] The point estimates for small and large firms correspond, respectively, to the main effect of exposure to the GDPR, and the sum of the latter to the coefficient of an interaction term between exposure and the size dummy. The complete tables are available upon request.

[17] The reduced sample size is due to the fact that only a limited number of companies report R&D expenses in ORBIS.

[18] https://patentscope.wipo.int/search/en/search.jsf.

[19] IPC codes allow us to classify patents by increasing level of detail, using the following categories: section, class, sub-class, main group, and sub-group.

[20] The reduced sample size is due to the fact that we are only able to match 50% of the total number of patenting companies, as well as the fact that the PPML estimator drops firms that never apply for GDPR-related patents.

[21] The evidence provided by Janssen et al. (2022), however, shows that the GDPR reduced the number of apps available on Google Play. Hence, the negative effect on product innovation, together with the positive effect on process innovation documented above, provides a complex picture. That said, since process innovation eventually runs in to diminishing returns without the introduction of new varieties, and the development GDPR-compliant processes might merely add costs, there are good reasons to believe that the overall impact on productivity will be negative. Such an interpretation is consistent with the findings of Blind et al. (2022), suggesting that the GDPR is associated with less radical and more incremental innovation.

[22] Satariano, A. (2018). G.D.P.R., a New Privacy Law, Makes Europe Worlds Leading Tech Watchdog. The New York Times, May 24.

[23] Satariano, A. (2018). G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. The New York Times, May 24.

REFERENCES

Aghion, P., Blundell, R., Griffith, R., Howitt, P. & Prantl, S. (2009) The effects of entry on incumbent innovation and productivity. *The Review of Economics and Statistics*, 91(1), 20–32. Available from: https://doi.org/10.1162/rest.91.1.20

Agrawal, A., Gans, J. & Goldfarb, A. (2019) *The economics of artificial intelligence: an agenda, Technical report*. National Bureau of Economic Research.

Aridor, G., Che, Y.-K. & Salz, T. (2023) The effect of privacy regulation on the data industry: empirical evidence from GDPR. *The RAND Journal of Economics*, 54(4), 6952–7730. Available from: https://doi.org/10.1111/1756-2171.12455

Autor, D.H., Donohue, J.J., III & Schwab, S.J. (2006) The costs of wrongful-discharge laws. *The Review of Economics and Statistics*, 88(2), 211–231. Available from: https://doi.org/10.1162/rest.88.2.211

Bajgar, M., Berlingieri, G., Calligaris, S., Criscuolo, C. & Timmis, J. (2020) Coverage and representativeness of Orbis data. *OECD Science, Technology and Industry Working Papers*, 2020(6), 1–63.

Bessen, J.E., Impink, S.M., Reichensperger, L. & Seamans, R. (2020) *GDPR and the importance of data to AI startups*. NYU Stern School of Business.

Blind, K., Niebel, C. & Rammer, C. (2022) The impact of the EU general data protection regulation on innovation in firms. In: *ZEW-Centre for European Economic Research discussion paper (22-047)*.

Bombardini, M. (2008) Firm heterogeneity and lobby participation. *Journal of International Economics*, 75(2), 329–348. Available from: https://doi.org/10.1016/j.jinteco.2008.03.003

Brill, J. (2011) The intersection of consumer protection and competition in the new world of privacy. *Competition Policy International*, 7(1), 6–23.

Campbell, J., Goldfarb, A. & Tucker, C. (2015) Privacy regulation and market structure. *Journal of Economics and Management Strategy*, 24(1), 47–73. Available from: https://doi.org/10.1111/jems.12079

Congiu, R., Sabatino, L. & Sapi, G. (2022) The impact of privacy regulation on web traffic: evidence from the GDPR. *Information Economics and Policy*, 61, 101003. Available from: https://doi.org/10.1016/j.infoecopol.2022.101003

Correia, S., Guimarães, P. & Zylkin, T. (2020) Fast Poisson estimation with high-dimensional fixed effects. *STATA Journal*, 20(1), 95–115. Available from: https://doi.org/10.1177/1536867x20909691

Frey, C. & Presidente, G. (2024) *ECIN replication package for "Privacy regulation and firm performance: estimating the GDPR effect globally"*. Ann Arbor: Inter-university Consortium for Political and Social Research. Available from: https://doi.org/10.3886/E197921V4

Godinho de Matos, M. & Adjerid, I. (2022) Consumer consent and firm targeting after GDPR: the case of a large telecom provider. *Management Science*, 68(5), 3330–3378. Available from: https://doi.org/10.1287/mnsc.2021.4054

Goldberg, S., Johnson, G. & Shriver, S. (2023) *Regulating privacy online: the early impact of the GDPR on European web traffic and e-commerce outcomes*. forthcoming. American Economic Journal: Economic Policy.

Goldfarb, A. & Tucker, C. (2012) Privacy and innovation. *Innovation Policy and the Economy*, 12(1), 65–90. Available from: https://doi.org/10.1086/663156

Janssen, R., Kesler, R., Kummer, M.E. & Waldfogel, J. (2022) *GDPR and the lost generation of innovative apps, Technical report*. National Bureau of Economic Research.

Jia, J., Jin, G.Z. & Wagman, L. (2021) The short-run effects of the General Data Protection Regulation on technology venture investment. *Marketing Science*, 40(4), 593–812. Available from: https://doi.org/10.1287/mksc.2020.1271

Johnson, G. (2022) Economic research on privacy regulation: lessons from the GDPR and beyond.

Johnson, G., Shriver, S. & Goldberg, S. (2023) Privacy and market concentration: intended and unintended consequences of the GDPR. *Management Science*, 69(10), 5695–5721. Available from: https://doi.org/10.1287/mnsc.2023.4709

Kalemli-Ozcan, S., Sørensen, B.E., Villegas-Sanchez, C., Volosovych, V. & Yesiltas, S. (2019) *How to construct nationally representative firm level data from the Orbis global database: new facts and aggregate implications*. National Bureau of Economic Research.w21558.

Lefrere, V., Warberg, L., Cheyre, C., Marotta, V., Acquisti, A. et al. (2020) The impact of the GDPR on content providers. In: *The 2020 workshop on the economics of information security*.
Lu, Y., Tao, Z. & Zhu, L. (2017) Identifying FDI spillovers. *Journal of International Economics*, 107, 75–90. Available from: https://doi.org/10.1016/j.jinteco.2017.01.006
Lu, Y. & Yu, L. (2015) Trade liberalization and markup dispersion: evidence from China's WTO accession. *American Economic Journal: Applied Economics*, 7(4), 221–253. Available from: https://doi.org/10.1257/app.20140350
Martin, N., Matt, C., Niebel, C. & Blind, K. (2019) How data protection regulation affects startup innovation. *Information Systems Frontiers*, 21(6), 1307–1324. Available from: https://doi.org/10.1007/s10796-019-09974-2
Miller, A.R. & Tucker, C. (2009) Privacy protection and technology diffusion: the case of electronic medical records. *Management Science*, 55(7), 1077–1093. Available from: https://doi.org/10.1287/mnsc.1090.1014
Miller, A.R. & Tucker, C. (2018) Privacy protection, personalized medicine, and genetic testing. *Management Science*, 64(10), 4648–4668. Available from: https://doi.org/10.1287/mnsc.2017.2858
Miller, A.R. & Tucker, C.E. (2011) Can health care information technology save babies? *Journal of Political Economy*, 119(2), 289–324. Available from: https://doi.org/10.1086/660083
Moser, P. & Voena, A. (2012) Compulsory licensing: evidence from the trading with the enemy act. *The American Economic Review*, 102(1), 396–427. Available from: https://doi.org/10.1257/aer.102.1.396
Peukert, C., Bechtold, S., Batikas, M. & Kretschmer, T. (2022) Regulatory spillovers and data governance: evidence from the GDPR. *Marketing Science*, 41(4), 746–768. Available from: https://doi.org/10.1287/mksc.2021.1339
Skiera, B., Miller, K. & Jin, Y. (2022) *The impact of the General Data Protection Regulation (GDPR) on the online advertising market*. Bernd Skiera.
Watzinger, M., Fackler, T.A., Nagler, M. & Schnitzer, M. (2020) How antitrust enforcement can spur innovation: Bell Labs and the 1956 consent decree. *American Economic Journal: Economic Policy*, 12(4), 328–359. Available from: https://doi.org/10.1257/pol.20190086
Yuan, B. & Li, J. (2019) The policy effect of the general data protection regulation (gdpr) on the digital public health sector in the European Union: an empirical investigation. *International Journal of Environmental Research and Public Health*, 16(6), 1070. Available from: https://doi.org/10.3390/ijerph16061070
Zhuo, R., Huffaker, B. & Greenstein, S. (2021) The impact of the General Data Protection Regulation on internet interconnection. *Telecommunications Policy*, 45(2), 102083. Available from: https://doi.org/10.1016/j.telpol.2020.102083

SUPPORTING INFORMATION

Additional supporting information can be found online in the Supporting Information section at the end of this article.

How to cite this article: Frey, C.B. & Presidente, G. (2024) Privacy regulation and firm performance: estimating the GDPR effect globally. *Economic Inquiry*, 62(3), 1074–1089. Available from: https://doi.org/10.1111/ecin.13213