



## Innovation and the GDPR: Much ado about quite a lot

Nicholas Martin<sup>a,\*</sup>, Max von Grafenstein<sup>b,c</sup>

<sup>a</sup> Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Straße 48, 76139 Karlsruhe, Germany

<sup>b</sup> Alexander von Humboldt Institute for Internet and Society (HIIG), Französische Straße 9, 10117 Berlin, Germany

<sup>c</sup> Einstein Center Digital Future at swthe University of the Art, Bundesallee 1-12, 10719 Berlin, Germany

### ARTICLE INFO

#### Keywords:

GDPR  
Innovation  
Regulation  
Economic impacts  
Data protection

### ABSTRACT

This paper critically reviews the extant empirical economics literature and findings on the GDPR's impact on innovation. It concludes that while the topic has been studied surprisingly little, and some more-widely discussed papers have significant flaws, the available evidence suggests that on balance the GDPR is having a significant negative impact on innovation in Europe. While it has also had positive innovation effects, European firms ironically seem not to have benefited much from these. The paper concludes with a discussion of possible reforms.

### 1. Introduction

It has often been claimed that the GDPR harms innovation. Yet despite a growing empirical literature on the GDPR's economic effects, its impact specifically on *innovation* has been studied surprisingly little. This paper reviews the evidence. Its original working title was "*Much Ado about Little?*" as we expected to find modest impacts at most. Unfortunately, the evidence did not support this. "Little" became "quite a lot". While rigorous econometric evidence on innovation impacts is limited and several widely-discussed papers have serious methodological flaws, on balance the available information suggests the Regulation is having a significant negative impact.

There are positive impacts. In some circumstances, GDPR compliance may facilitate AI adoption. A new data protection compliance software industry can be traced directly to the GDPR. Troublingly for European policymakers, much of this entrepreneurship seems to have happened in America, not Europe. Overall, innovation-stimulating effects do not outweigh innovation-hindering ones.

The evidence implies a need for significant reform to the GDPR. A better balance needs to be struck between individual interests in data protection, and collective interests in technology development and growth. Reform should focus on making it easier to collect, use and share data. Negative externalities from digital technology are real, and demand regulatory action. But tools other than data-protection law may be better suited to address these.

### 2. Innovation and data

Following the OECD Oslo Manual [1], we understand "innovation" as new or significantly improved products, services or processes. This includes business, public-sector and non-profit innovations. The empirical literature related to the GDPR has mainly focused on business innovation and to a lesser extent, scientific research. Our review follows this focus.

All innovations likely require data of some kind, but not all require *personal* data. The GDPR applies only to personal data. Innovations that *only* use non-personal data thus seem less likely to be impacted by the GDPR, though even these are likely created by humans in processes that generate personal data (e.g. lab access controls) and thus may be affected by the GDPR. More broadly, digitisation and the fact that most products, processes and services interact with humans, suggest that the share of innovations using or interacting with "personal data" is likely growing, at least under the current very broad definition of what constitutes "personal data".

Among innovations that process<sup>1</sup> personal data, some may be considered "data-driven" in the sense that this processing is central to their value proposition, while in others it is more incidental [2]. Plausibly, the more personal data-driven an innovation, the more exposed to GDPR impact it should be. But personal data may play critical roles also at certain points in the creation of innovations that are not ordinarily considered "(personal) data-driven", e.g. pharma, robots pharma, robots or industrial equipment (human-machine interaction).

\* Corresponding author at: Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Straße 48, 76139 Karlsruhe, Germany.

E-mail address: [nicholas.martin@isi.fraunhofer.de](mailto:nicholas.martin@isi.fraunhofer.de) (N. Martin).

<sup>1</sup> "Data processing" generically describes all handling and manipulating of data, from collection to erasure.

At the firm level, as legions of failed data projects testify, “more data” does not seem to automatically lead to “more innovation”. Rather, whether more data promotes more innovation, depends on the individual firm’s capacity to use it.

Another level is the (macro) economy, which is the level this review (and the papers it studies) focuses on. Even if “more data” does not automatically translate into more innovation at the individual-firm level, it is possible that at the macro level, aggregating across all firms, more data enables more innovation overall. Given the central role of digitisation (i.e., data processing) in contemporary techno-economic development, this appears *prima facie* plausible.

At first stab, that would sit uncomfortably with regulations which impose rules on and thus tends to restrict data processing. Yet real-world data use and regulatory impacts thereupon are complex. By improving data quality, trust or prompting company-internal transformation, even regulations whose first-order effect is to restrict processing might, at second order, enable more or more valuable processing. In short, the real-world consequences of regulations like the GDPR is an empirical question.

### 3. The GDPR

Processing personal data offers firms, individuals and society benefits, but exposes individuals to risks, from abstract privacy violations to harmful real-world consequences if data is used against them. Structurally, individuals confront often-overwhelming power imbalances vis-à-vis corporate and public-sector data controllers.

The GDPR became law in 2016 and applicable in May 2018. It represents an attempt to resolve this tension by defining rules for lawful data processing, that aim to mitigate risks and reduce power imbalances between data subjects and controllers, while also promoting the free flow of data across the Union. Few of its rules are wholly new. Rather, it builds on the 1995 EU Data Protection Directive and also sets the framework within which other more specific regulations, like the 2002 ePrivacy Directive, are applied.

Compared to the pre-GDRP legal framework, the Regulation introduces three regulatory innovations:

- 1) A more comprehensive implementation of the so-called risk-based approach. The key provisions here are Articles 25 and 35 of the GDPR, according to which data controllers must implement all requirements of the GDPR according to the risks of data processing in its technical and organisational design.
- 2) The GDPR provides significantly expanded options for data controllers and processors to reduce the legal uncertainty that inevitably results from the cross-sectoral and risk-based approach (in particular Art. 40 ff.). Unfortunately, despite the legislative mandate to take the needs of SMEs into account (see Art. 40(1) und 42(1)), the data protection authorities have made the relevant procedures so complex that they have hardly been used to date.
- 3) Drastically increased penalties for infractions, up to €20 million or four percent of worldwide turnover of the (mother) company.

Given its broad approach, the GDPR is a principles-based regulation. This means that it does not set out detailed rules for every possible data processing, but defines high-level legal principles. Those applying the law must interpret these (numerous) principles and undefined terms according to the specific case. This approach is not unreasonable given that the regulation’s subject matter is rapidly evolving, that it regulates future events, to prevent future damage from occurring [3–5], and that risks from information processing are highly contextual [6].

With respect to *innovation*, the GDPR’s key stipulations are:

- It sets conditions for lawful processing of personal<sup>2</sup> data: each processing needs a legal basis (e.g. consent), its purpose must be specified in advance and be transparent and fair. Personal data must be minimised (e.g. via anonymisation) and its accuracy, integrity and confidentiality ensured. Processing cannot exceed legal basis and purpose. (Article 5–6).
- Firms must be able to implement defined information duties and data subject rights (DSRs). (Articles 11–22).
- Firms must implement appropriate technical and organisational measures to minimise risks to data subjects’ fundamental rights, conduct risk assessments when risks are high, and notify data subjects and supervisory authorities of data breaches. (Articles 25, 32–33, 35).
- Firms must document the above and be able to demonstrate compliance (Articles 5, 24, 28, 30)

This has two consequences for companies and organisations handling personal data:

Firstly, they must be able to “govern” data and document compliance: Obtain and manage legal bases like consents; map, track and control data flows through their systems; tag data so it can be linked to legal bases and purposes, and DSR requests acted on. They must be able to control and monitor data access, how and why data is processed; ensure security, conduct risk assessments, assess the scale of any data breaches and notify affected parties and authorities. This generally requires implementing a data-governance system; usually a suite of at least partly automated privacy-compliance software tools and platforms.

Secondly, the GDPR in practice limits how easily and extensively organisations can process personal data, because satisfying its requirements can be laborious and sometimes impossible (e.g. if data subjects refuse consent or simply cannot be contacted). This is not because the GDPR prohibits any particular use of data outright: it doesn’t. In principle, almost any data usage can be legal – provided it has a legal basis, the processing does not exceed the stated purpose, safeguards data subjects’ rights, and does not violate other GDPR stipulations. Processing that fails to do this, conversely, is illegal.

### 4. Impact mechanisms

The GDPR might impact innovation through several mechanisms, both negative and positive.

Firstly, on the negative side, it may reduce access to or ability to use certain inputs to innovation, in particular data and investment:

- *Data availability*. The need for a legal basis and secondary-processing restrictions implied by purpose limitation, reduce access and ability to use data. Anonymisation, encryption and other security and data-minimisation procedures can degrade data’s information value or make it cumbersome and technically-demanding to analyse. This may obstruct data-dependent innovation. Startups or firms without direct access to end users or pre-existing data stores may be especially affected. Reduced data availability may also reduce marketing effectiveness – particularly relevant for young firms.
- *Investment availability*. Innovation requires capital. Young companies are particularly dependent on outside investors. Beyond capital, specialised Venture Capital (VC) investors provide innovators with advice and networks [7]. If investors believe the GDPR adversely affects certain technologies or business models, it becomes harder for these to raise money or access VC’s non-financial benefits. In turn, this should reduce innovation in these areas and potentially in aggregate.

Secondly, it may alter cost structures relevant to innovation, in

<sup>2</sup> Unless otherwise indicated, “data” refers to “personal data” throughout.

particular compliance burdens:

- *Compliance costs and complexity.* Resources spent on compliance are unavailable for innovation. Businesses can ringfence innovation and instead reduce other budgets. But if compliance rises directly on innovation-related activities – e.g. because additional risk assessments, complex documentation or legal agreements become necessary – ringfencing may be difficult. Compliance for an innovation project may become too challenging, prompting its abandonment.

Thirdly, it may shift the larger competitive balance between different types of companies in ways that are material to innovation:

- *Uneven playing field.* The mechanisms listed above likely disproportionately affect smaller, younger companies. Larger, older firms regularly have more capital, legal and technical expertise, customer/user relations and larger data stores, making coping with the GDPR easier. They may also more easily offshore functions to laxer jurisdictions. Innovation however tends to come from new firms. Uneven playing fields favouring incumbents thus likely reduce innovation.

There are also mechanisms through which the GDPR might positively affect innovation:

- *Demand for new technologies* to help firms achieve compliance or overcome hurdles the Regulation creates [8,9]
- *Trust.* If the GDPR increases users' trust, they may be more likely to adopt new technologies or try unknown firms' products.
- *Data portability.* The GDPR gives users a right to port their data between service providers. This could promote innovation, mainly by increasing competition.

## 5. Empirical findings

To identify empirical papers relevant to the question of the GDPR's impact on innovation, we searched Scopus,<sup>3</sup> perused [10] and the texts referenced in the papers we studied. We supplement these with additional survey evidence (mainly for Germany).

The economics literature on the GDPR – reviewed excellently in [10] – is heterogenous. Only a small number of papers directly studies the GDPR's impact on *innovation outcomes*, i.e. on changes in the rate at which new products, patents or processes are innovated, new technologies adopted, or innovation activities like clinical trials or other innovation projects engaged in. But more papers study or have systematic evidence on how the GDPR has affected the impact mechanisms described above, viz. data availability, investment, compliance burdens, the competitive playing field, as well as, on the positive side, demand for new technology, trust, and data portability. Negative change in these variables (impact mechanisms) does not, by itself, prove that innovation has declined. However, negative change in the impact mechanisms would suggest that innovation has become harder and the larger innovation environment negatively impacted. If direct measures of innovation outcomes also indicate a decline in innovation (and both can be related to the GDPR), then that would be strong evidence that it is having a negative effect on innovation.

We first discuss the evidence for direct innovation outcomes, both at the cross-sectoral and the technology/sector-specific level. Then we assess evidence for effects on the impact mechanisms.

Methodologically, almost all papers employ a so-called “differences in differences”-design, which is standard in academic econometrics today. Roughly summarised, they take a treatment population (e.g. European firms) and a control population (e.g. US firms) and observe

their behavior (e.g. investment) or outputs (e.g. innovations) over a pre-treatment and a post-treatment period (e.g., before May 2018 and after May 2018). The statistical analysis then focuses on whether the treatment population manifests statistically-significant differences in the outcome of interest (e.g. investment, innovations) after the treatment event (e.g. GDPR becoming applicable), compared to both the pre-treatment period, and the control population. Statistical controls are applied to rule out that variables other than the treatment (GDPR) are driving the results. Variables that were affecting the treatment population already *before* the treatment event can by definition be ruled out as explanations for post-treatment changes.<sup>4</sup>

### 5.1. Innovation outcomes

#### 5.1.1. Cross-sectoral outcomes

The digital-economy association BitKom [11–16] and the Center for European Economic Research ZEW [17,18,25] have separately conducted multiple representative surveys of German businesses on the GDPR's effects. Results differ in size but consistently find negative innovation effects.

Since 2020, in BitKom's annual surveys [11–16], consistently between 56 % and 100 % (!) of responding companies report that in the prior 12 months, the GDPR caused innovation projects to fail or not be attempted in the first place. Interestingly, when the question was first asked in 2019, only 14 % of respondents gave this answer, suggesting the GDPR's effects may have taken time to filter through. These are stark numbers. Further data points in [11–16] paint a similar picture.

ZEW's findings are slightly less grim. In 2019, 35 % of ZEW respondents reported that the GDPR had “complicated”, <5 % that it “facilitated” innovation, 40 % that it had *no effect*. Negative effects were highest in finance/insurance, media and professional services (~40 %–59 %); positive effects in ICT (~15 % positive vs. ~35 % negative) [17]. Other ZEW surveys have similar numbers.

The surveys strongly suggest that the GDPR is exacting *some* cost on innovation. But they do not tell us how large this cost is, nor what its consequences really are.<sup>5</sup> To address these questions, [17,18] study the ZEW data econometrically. They find that at least to 2020, the GDPR did *not* negatively impact *total* innovation output (new products/process), as measured in sales shares and cost reductions. But it *did* prompt changes in innovation focus. Firms switched from “radical” innovations (novel products that had not previously existed) to “incremental” innovations (products new to the firm but not the market). The effect is small, but statistically significant: sales from incremental innovations rose 1,8 %; sales from radical innovations fell 0,9 %. The effect is driven by firms that are smaller, younger and/or in services and knowledge-intensive sectors as well as B2B markets. The GDPR also disproportionately affects firms which intensively use digital technologies.

These findings are based on data for 2019/2020. They do not tell us about subsequent developments [17,18]. interpret their results as suggesting a Porter Hypothesis-like effect,<sup>6</sup> wherein the GDPR forced firms to re-organise data-management and IT processes, fortuitously revealing opportunities to improve existing products. Indeed, [20] find that

<sup>4</sup> Concretely, this means the 1995 Data Protection Directive and the 2002 ePrivacy Directive can be ruled out as causes of post-GDPR changes. (It is possible though that a change is caused by the *interaction* of the treatment [GDPR] with a pre-existing variable [e.g. ePrivacy Directive].)

<sup>5</sup> Technically, they also do not prove causality.

<sup>6</sup> The Porter Hypothesis suggests that by prompting firms to innovate and adopt new processes and technologies, environmental regulation may ultimately increase their competitiveness relative to the status quo ante [19].

<sup>3</sup> Search string: “GDPR” AND (“Innovation” OR “econ” OR “AI” OR “artificial intelligence” OR “medic” OR “self-driv” OR “autonomous vehicle”)

GDPR-mandated data/IT reorganisation facilitated AI adoption in large US financial corporations (see below).<sup>7</sup> However, these are among the world's richest, technologically most-sophisticated firms. More average companies, such as those that populate [17–18]'s sample, might not similarly benefit. Puzzlingly, in [17–18], even the firms that describe the GDPR as *obstructing* innovation experienced an average 1.6 % increase in sales from incremental innovations (and a 1.2 % drop in radical-innovation sales). These firms nevertheless describe the GDPR as “preventing/hampering” innovation, suggesting that they do not consider GDPR-induced incremental innovations to be particularly valuable, and not as valuable as the radical innovations foregone.

Rather than a Porter effect, an alternative interpretation of [17–18] is that in 2018–2020, firms altered existing products and services to make them GDPR-compliant. Often, these changes may have been substantial enough to qualify as “innovations”, yet did not deliver *additional* value *beyond compliance*, that customers were willing to pay extra for or that otherwise strengthened companies' competitive positions. While technically sales from incremental innovations went up, survey respondents may not have valued this much. Hence it did not shift their perception that the GDPR was hampering innovation, since they were also experiencing drops in (more valuable) radical innovations. This would be consistent with [21] who find that the GDPR prompted increased R&D and patenting of compliance-related technologies (i.e. “PETs”, see below) even while total new patent numbers remained unaffected, implying compositional changes.

The effects [17–18] document are small. A critical question is whether they are enduring. A small one-time drop in radical innovations that soon reverses is unlikely to do lasting damage to European competitiveness. Conversely, even small effects can do lasting damage if they endure over time and compound. While not strictly causal, this is what makes the BitKom survey evidence [11–16] so concerning: high and rising numbers of firms reporting that innovations fail or must be abandoned due to the GDPR.

### 5.1.2. Artificial intelligence

There is a conceptual debate about the GDPR's compatibility with AI [22–24] but limited empirical work. The cited surveys suggest real incompatibilities. In 2024, 52 % of BitKom survey respondents said the GDPR “obstructed” their use of AI, up from 34 % in 2022/2023. Of these, around half explained that the GDPR “complicated” training models with “enough data”, though 44 % also claimed that it provided “legal certainty” [14–16]. ZEW numbers are less drastic but directionally similar: in 2024, 24 % of German information-economy firms reported that the GDPR “hindered or prevented” AI use, up from 13 % in 2020 [25].

Conversely, [20] find that five years after May 2018, among major US financial corporations, those with higher European market share (which [20] treat as proxy for GDPR exposure) have higher technical investments in machine learning and AI, and more revenue-enhancing ML/AI innovations.<sup>8</sup> The data standardisation, integration and governance capabilities necessary for effective AI use, [20] suggest, overlap with the data-governance capabilities the GDPR demands. Left to themselves, companies often hesitate to undertake the costly and disruptive organisation-wide digital transformations needed for effective AI use. The GDPR effectively forced companies to commit to such transformation programs, overcoming institutional inertia and enabling subsequent growth in effective AI deployment.

This is an intriguing argument and findings. The question is whether it generalises beyond [20]'s sample ( $N = 11$ ) (!), all US-based. The GDPR

applies only to their European operations. Plausibly, the “Brussels Effect” [26] causes them to apply GDPR-like standards to operations elsewhere too, but greater regulatory freedom in America may still facilitate AI adoption. Plausibly, they inhabit a sweet spot available to few other – especially, few European – companies: able to use the GDPR to overcome institutional inertia to modernise data governance, but also able to exploit weaker US regulation to optimise AI use.

Major financial corporations are atypical: they have deep financial, legal and technical resources, compliance expertise, and are based in multiple jurisdictions [20]. Their regular business processes provide them vast amounts of data. They may find it easier to comply with the GDPR and navigate its restrictions than smaller firms.

While not a GDPR study, [27] underscore the critical role of data access for AI firms and privacy regulations' impacts thereupon. They study the California Consumer Privacy Act's impact on firms offering voice-AI products. By restricting data trading, the CCPA advantages firms that possess significant inhouse data stores and collection capabilities (e.g. large pre-existing customer bases). After CCPA passage, these firms experience greater gains in customer satisfaction – suggesting superior technology development – financial performance, and invest more. The GDPR's rules related to data access are stricter than CCPA. If anything, we should therefore expect the GDPR to have stronger negative effects than those documented for CCPA.

One solution to this would be developing less data-dependent AI [28]. explore this, using patent data to 2021. They classify AI patents into “data-intensive” (Deep Learning) and “data-saving” approaches (rules-based, Bayesian, transfer learning, synthetic data). After 2017, EU companies increased patenting for data-saving and reduce patenting for data-intensive AI. But – at least until the end of their time period, 2021 – the effect is small: +1.6 % data-saving, –1.5 % data-intensive patents, and hardly alters US companies' wide lead also in data-saving patents. More worryingly, despite the uptick for data-saving patents, EU firms' total AI patenting falls by 1.1 % after 2018 [28].

These diverse pieces of evidence suggest that the GDPR is imposing a drag on EU firms' AI development and deployment.

### 5.1.3. Medical innovation

Medical researchers have debated the GDPR extensively, often voicing concern [29–33]. Anecdotal evidence strongly suggests that the GDPR and/or national laws have complicated medical research significantly, likely reducing research activity. Reporting on data sharing at a major German university research hospital, [34] recount that despite strong political pressure and researchers' enthusiasm for sharing medical datasets, very little data was ultimately shared, due to complex compliance. Data minimisation requirements greatly reduced the data's reuse value. They attribute this to local German applications of the GDPR, noting Dutch and Austrian GDPR applications seem to be more supportive of clinical data sharing [34]. [35] claims that strict Italian GDPR applications “are preventing most observational or translational research projects in Italy”. A Scandinavian consortium concluded that during a three-year project, “our research consortium *spent more time ensuring GDPR compliance than on actual research activities.*” (emphasis added) [36]. [37,38], among others, suggest GDPR restrictions on international data sharing are hampering medical research and drug development.

[39] attempt to provide systematic quantitative evidence for a negative effect on clinical trials, arguing that the GDPR caused them to

<sup>7</sup> The ZEW information-economy [25] and the BitKom [9–16] surveys also provide evidence that the revisions to internal processes which the GDPR forced on firms led to efficiency gains. However, these gains do not seem to have cancelled out most respondents' overall negative evaluation of the GDPR.

<sup>8</sup> They also have larger increases in revenue and operating income.

move out of Europe. However, this study is marred by serious methodological problems.<sup>9</sup> Interestingly [40], studying medical registry research in Finland before and after the GDPR and the 2020 Finnish Secondary [Data] Use Act, respectively, find that the GDPR did *not* negatively affect registry-based research, but the (national) Secondary Use Act *did*.

In summary, little systematic quantitative evidence exists for a negative impact of the GDPR on medical innovation, but numerous anecdotal and case-based accounts suggest that it is obstructing medical research and innovation, possibly significantly. Lack of quantitative evidence can thus hardly count as evidence of absence. On the contrary, given the wider evidence for a negative impact of the GDPR on innovation and medical data's special status under Art. 9, it would be surprising if the GDPR was not obstructing medical research. US evidence supports this. [41–43] demonstrate that US state privacy laws hindered data-based medical technologies' adoption, harming patient health. That said, national law also impacts sharing of medical data, and the extant evidence hints at variation in how member states apply the GDPR in this area.

#### 5.1.4. Apps

A notably widely cited paper is [44] who study App innovation using Google Playstore data, finding that around 2018 one third of apps exited the Playstore and entry of new apps fell by half. They attribute this to the GDPR [44]. However, [45] cast serious doubt on this. They point to (non-privacy-related) changes to Google's review process, a deliberate purge of low-quality Apps, no comparable exit patterns from Apple's App Store, and the fact that Europe accounts for <18 % of Playstore App revenue as reasons to doubt [44]'s argument.

#### Data availability

##### 5.1.5. Cross-sectoral evidence from cloud use

[46] study how European firms' use of a global cloud-computing provider changes after May 2018, compared to the provider's US customers. After May 2018, a gap opens up. By 2020, European firms are storing 26 % less data and using 15 % less compute than US firms, relative to pre-GDPR trends.

[46] show that what is happening here is that from ~2018 on cloud use (storage, compute) grows more slowly among the provider's EU

<sup>9</sup> [39] tests whether after GDPR, a statistically significant change in the number of clinical trials registered in (1) EU countries and countries with data protection adequacy agreements with the EU on the one hand, and (2) countries subject to *neither* the GDPR *nor* the California Consumer Privacy Act, on the other hand, occurred. To do this, they collect data on the number of clinical trials registered in each group of countries in two time periods: 2011–May 24, 2018, and May 25, 2018–July 31, 2021. Using this first period (2011–May 24, 2018), they compute a linear trend for each country group, to predict how many clinical trials ought to have taken place in the following period (May 25, 2018–July 31, 2021), had the 2011–2018 trend held. Then they test whether the difference to the number of trials that actually occurred after GDPR is statistically significant (F-test). They also apply the Chow test for structural stability. The problems with this are: Firstly, they group EU countries with countries that merely have adequacy agreements, treating these identically. But unless the “adequacy”-countries all also implemented the GDPR (which they didn't) or a comparable law ([39] don't say) on May 25<sup>th</sup>, 2018, there is no reason to expect them to manifest similar trends as the EU. (Indeed, trial numbers fall in “adequacy” countries from early 2018 on, but merely level off in the EU. It is not obvious why the GDPR should have *weaker* effects in the EU than in “adequacy” countries.) Secondly, they do not justify their choice of time periods. Yet visual inspection shows that clinical trial numbers fluctuated considerably between 2011 and May 2018. Deriving a single trend from these ~6.5 years and comparing it to the following ~3 years thus seems arbitrary, raising questions of omitted variable bias. Thirdly, they do not test for alternative explanations. Especially, they do not control for Covid, which could have depressed clinical trial numbers in the 2018–2021 period.

customers than the US customers. In fact, European demand for cloud services *quadruples* between 2018 Q2 and 2022 Q2 [47]. But US cloud use apparently grows *even faster*, creating the gap [46] identify. They attribute this to the GDPR increasing European firms' “cost of data” by, they estimate, 20 %. If correct, this would be very concerning, as it suggests that the GDPR is preventing European companies from becoming more data-based.

Plausibly, there is a growing gap between EU and American cloud use. The GDPR likely is obstructing data use. Unfortunately, [46] suffers from critical shortfalls and *cannot* be taken as evidence for a GDPR-induced slowdown in data usage. Nor can their estimate for the GDPR increasing the “cost of data” by 20 % be accepted.

Analytically, [46] is based on the premise that the GDPR raised the marginal “cost of data” more than of compute, prompting firms to reduce data collection/storage in favour of compute, as they optimize costs at the margin [46]. then uses a production function and observed shifts in firms' storage/compute ratio to estimate the increased “cost of data” supposedly caused by the GDPR. But contrary to their claims, the GDPR does not regulate “data”, but data *processing*, which includes computation (Articles 1(1), 2(1), 4(2)). There is no reason to believe that the GDPR raises the marginal cost of data storage more than of compute. Accordingly, it is hard to see how one might calculate a GDPR-induced increase in the marginal cost of data from shifting storage/compute ratios. Indeed, it is doubtful whether the obstacles to data usage the GDPR creates are best understood – or modelled – as marginal-cost increases and resultant marginal reductions in data usage. Rather, anecdotal and survey evidence suggest that perceived de facto prohibitions and legal uncertainty are the main blocks to data use and data sharing, not that data has become several marginal increments too expensive [34,48,49].

Slower growth in cloud use in Europe would require explanation. Curiously, the greatest drop [46] find is among manufacturers (–40 % data storage, –32 % compute). Services and software firms see much lower drops. But that the GDPR should affect manufacturing most and services and software least, is implausible<sup>10</sup> and contradicted by surveys [17]. This suggests something other than the GDPR may be driving [46]'s findings. The AI boom, which goes together with rapid cloud-use growth, offers a strong alternative explanation. In the U.S., AI investment accelerates from 2018 on, more than doubling by 2020. In Europe, it stagnates and even drops [50]. This exogenous technological shock may explain much of the difference. While the GDPR likely has impacted AI in Europe, it is hardly plausible to reduce the far greater AI investment in America to the GDPR.

##### 5.1.6. Medical data

There is strong anecdotal evidence that the GDPR and national legislation have reduced the availability of medical data or at least slowed its growth, by obstructing data sharing and reuse (Section 5.1.3). The magnitude of this effect and its downstream impact remain to be quantified. The exact roles of the GDPR, its varying national applications, and separate national legislation, too, remains to be determined.

##### 5.1.7. Online data

Many papers examine effects on personalized advertising and tracking online. Details vary but a fairly consistent picture emerges: Immediately after 25 May 2018, web-based user tracking fell sharply. Over the following 6–18 months then, it largely – if not always fully – recovered, though personalized advertising-related tracking may have taken a more enduring albeit small hit. [51] find that European

<sup>10</sup> It is implausible that manufacturers systematically use more personal data than software or services companies. Moreover, the personal data manufacturing companies use is likely disproportionately employee or customer data, for which obtaining consents, contractual agreements or even legitimate-interest grounds for processing should be fairly easy.

websites' webtech use falls ~15 % on average immediately after May 2018 (~24 % drop for advertising-related webtech) but largely returns to pre-GDPR levels by year's end (advertising webtech remains ~6 % down) [52] document that 3rd party cookies served to European visitors on European news/media websites fall from ~87 cookies on average just before 25 May 2018, to ~32 cookies just after, then recover to ~58. Cookies served to non-European visitors quickly exceed pre-GDPR numbers. Others have similar results<sup>11</sup> or find no decrease at all: [55] documents that tracker numbers on European websites remain higher than on non-European websites and continue to grow after May 25. At most, the GDPR somewhat slowed tracker growth.<sup>12</sup> [56] find that the GDPR made little difference to the number of trackers apps contain.

On balance then, the GDPR seems to have led to a small decrease in the digital tracking Europeans are subjected to and made it easier to opt out of tracking entirely for those who wish, by refusing consent. Non-consent rates for online tracking have been estimated at between ~5 % and ~15 % [57,58]. Non-consent options can make data sets cleaner, as privacy-conscious users who previously used obfuscation tech now just opt out of tracking. Remaining tracked users can be observed better, making their data more valuable [59]. Indeed, when obliged by the GDPR to re-elicited consents, firms with established customer relationships have been able to get customers to consent to increased data collection when they perceived this to offer value to them [60].

These findings suggest that so far, the GDPR has not caused dramatic declines in the amount of online behavioural data available to European firms. Is all well then? Not necessarily. Online consent interfaces are commonly designed to nudge users to agree to maximal data collection. This contradicts the GDPR's spirit and arguably letter. There are efforts to regulate this more strictly. If the GDPR has so far not caused online data collection to collapse, this is likely partly because regulatory forbearance has allowed firms to exploit grey areas to the maximum.

Users will consent to data collection by firms they have direct relationships to, that offer them direct benefits in return [60], but have also proven very reluctant to agree to more intrusive tracking (e.g. geolocation) or to third-party tracking. Here consent rates collapse dramatically (ibid.).<sup>13</sup> Yet it is precisely new companies, without established customer relationships, that likely most depend on access to third-party data and secondary processing. Legal regimes that obstruct this will generate structural biases in favour of incumbents and against new companies.

The – small – reduction in online data availability may have already extracted a –smallish – economic cost. Several studies find that website visits, ad- and e-commerce revenues all decreased by somewhere

between ~5 % and ~15 % compared to non-GDPR-affected websites, likely because marketing became less effective.<sup>14</sup>

At the lower bound, these are hardly dramatic numbers. Indeed, some studies document positive economic outcomes (Footnote 12). There are also occasional oddities in the data.<sup>15</sup> The numbers may partly reflect temporary effects like companies deleting old email marketing lists. At the upper bound though, these numbers would be concerning, especially if they endured. The true hit presumably lies somewhere in between.<sup>16</sup> This deserves continued study, but also implies a warning about possible effects of clamping down on current “grey area” practices.

Moreover, individual-level data collection, e.g. of geolocation, behaviour or health, enables population-level inferences and services (e.g. mobility, urban planning) that deliver value to society at large, if not necessarily to the individual data subject, for whom a particular service may be irrelevant. Data collection regimes that rely on individuals' immediate incentive to actively opt in to collection, or on altruistic data donations that in practice will almost certainly involve clunky interfaces and complex processes, and be geared exclusively to non-profit usage, are likely to result in reduced data availability for innovative companies.

## 5.2. Compliance

Surveys indicate enduringly high compliance burdens [14–16]. Even six years after May 2018, near-80 % of German companies had not managed to fully implement the GDPR. This is a remarkable number. ~80 % state that the GDPR has made business processes “more complicated” and increased compliance burdens relative to pre-GDPR. Only 12 % expect burdens to fall; 33 % to further increase. ~80 % view legal uncertainty as a key challenge [14–16].

We are not aware of empirical research systematically linking GDPR compliance burdens and innovation outcomes. Most problematic would be additional compliance burdens directly on innovation processes. It is virtually certain that these have risen whenever innovation activities touch personal data. The issue is likely not so much marginal-cost increases – though these matter too – as complex, time-consuming processes, uncertainty, requirements that substantially reduce information content (e.g. anonymization), outright prohibitions (e.g. due to purpose limitation), and inconsistent cross-national approaches. In theory, the GDPR's principles-based approach provides companies with flexibility. In practice, the lack of specific does/don'ts this entails, combined with the threat of very high fines and a culture, perhaps especially in the public sector, of extreme (compliance-) risk avoidance, seems often to produce paralysis: At one major European public institution, economists had to accept limits on webscraping price data, compromising data quality, to avoid accidentally collecting personal data from public product reviews.<sup>17</sup> As discussed, a medical-research consortium “spent more time

<sup>11</sup> [53] (finding third-party cookies that do not require consent fall in May/June 2018); [54] (trackers on a major European travel-industry ad network fall ~12.5% through to 31 July 2018); [61] (webtech use falls 7.6%–10.4% with some later recovery though not for third-party cookies) [53] and [54] study only the first months after May 2018; bounce-back may have happened later.

<sup>12</sup> Per the data in [55], faster growth in tracker numbers on non-European than on European websites already begins around January 2018. As non-European websites start with much lower tracker numbers, faster growth may simply reflect catch-up, and Europeans' slowing tracker growth a levelling off of the marginal benefit additional trackers offer.

<sup>13</sup> [60] find that only 4.7% of users agree to geolocation, 3.5% to third-party sharing. This is in a context where overall consent rates to some data collection jump from 57% to 72%, the company is well-known and customers have long-standing relationships to it. ~4-5% may represent an upper bound on consents to these kinds of more invasive collection and sharing.

<sup>14</sup> See [57,59,62,63,52] also document drops in page views and reach for European news/media websites, but argue that this is likely not due to the GDPR but longer-standing structural shifts in news consumption. Importantly, they find no evidence that this has negatively impacted survival rates, monetization strategies or content quality [60] find that in the wake of consent re-elicitation, sales, marketing efficiency and contractual lock-in all go up, as customers agree to share more data.

<sup>15</sup> [62] find that post-GDPR, websites related to “Heavy Industry and Engineering” experienced the largest drop in visitors (–45%). Yet those who visit industrial/engineering-related websites for professional reasons will likely carefully research targets using professional sources and search tools – and not be steered there via personalized ads. Industrial capital goods are rarely bought on impulse via personalised marketing. One wonders whether apparent post-GDPR traffic drops here really reflects falls in valuable traffic.

<sup>16</sup> The GDPR itself creates an observation problem that likely exaggerates the negative effect: users who do not consent remain unobserved and thus count towards declines – even if they did visit the site [57,62, Appendix F] attempt a solution.

<sup>17</sup> Personal communication.

ensuring GDPR compliance than on actual research activities.” [64]. Elsewhere, compliance prevented researchers from sharing almost any medical data [34].

### 5.3. Investment and uneven playing field

Weak VC investment is a longstanding European problem [65]. After 2018, VC investment in the EU initially continued to grow until 2021 [66]. However, [67–69] suggest the GDPR slowed its growth. After May 2018, VC investment in the EU falls sharply relative to trends in the U.S. and Rest of World. Compared to America and pre-GDPR trends, monthly EU deal numbers drop ~22%–~25%; average deal sizes by up to 33.8%. The effect is greater for younger and more data-reliant companies. It is driven by U.S. investors’ reduced activity. This implies that beyond reducing access to capital, the GDPR may also be harming European firms’ access to U.S. networks.

The drops [67–69] document are large numbers. If confirmed this would be worrying, especially as since 2021 VC investment in Europe has been declining also absolutely [66].

[70] first hypothesized that privacy/data protection regulation would affect market structure by advantaging large incumbents over small and new firms. As innovation tends to be disproportionately driven by the latter, this would indirectly affect innovation outcomes too. Detailed discussion of findings related to market-structure impacts is beyond scope. However, as noted throughout this text, numerous papers find that young/small companies are disproportionately affected.

### 5.4. “Privacy enhancing technologies”

By creating new compliance hurdles, the GDPR also creates a market for new technologies to overcome these [8,9]. Often labelled “Privacy Enhancing Technologies” (PETs), these can be divided into *data-governance tools* (DGTs) that address core GDPR compliance tasks (manage legal bases; map, track, control data flows, roles and access; implement DSRs; document compliance, etc.), and *privacy-preserving analytics* (PPAs). PPAs use encryption, statistical or hardware approaches to enable computation over restricted data, thus potentially solving constraints on data processing the GDPR creates.

Since the mid-2010s, prompted largely by the GDPR, DGTs have seen substantial entrepreneurial entry and the creation of several unicorns [71,72]. Strikingly though, the sector has largely come to be dominated by US firms. European companies are marginal. Based on qualitative research, [72] attribute this to the way the “Brussels Effect” created significant demand for DGTs in North America, while market fragmentation, limited demand and weak tech and VC sectors in Europe made scaling there difficult.

PPAs have attracted significant policy attention in Europe and America [73,74] PPAs encompass a number of different technologies (e.g. homomorphic encryption, multi-party computation, differential privacy, synthetic data, and trusted execution environments). However, despite considerable technical progress, commercialization has hitherto struggled, except for synthetic data.<sup>18</sup>

### 5.5. Trust

Reviewing the large literature on privacy, trust and technology adoption is beyond scope. Strikingly, only one empirical paper investigates whether the GDPR positively affected trust, coming to a negative result [75]. Two interview-based studies find that people strongly appreciate data to be stored in Europe, and that this has to do with the GDPR [76,77]. What is less clear is whether this has meaningful consequences. “Trust” arguably matters for many social-political outcomes, but with regard to innovation, it matters especially as a possible

determinant of decisions over technology adoption. Yet people routinely adopt technologies of – and share data with – companies and institutions they profess to have little trust in. The two arguably most technologically-advanced societies today – America and China – likely have lower levels of social trust than Europe. It does not appear to have obstructed innovation, suggesting that – for innovation at least – “trust” may be rather less important than sometimes claimed.

### 5.6. Data portability

[78–81] study data portability’s possible effects theoretically; [82] tries to predict them from historical patterns. They come to divergent conclusions. No empirical work on its actual effects on innovation is known to us. [83,84] find that in practice, users seem to make very little use of the right to portability. In practice, portability’s real effects may thus be negligible so far.

## 6. Conclusions and implications

Unfortunately, no comprehensive study of the GDPR’s effects on innovation across different sectors and technologies exists. Instead, the extant research provides snapshots across different areas. Not every paper can be accepted as valid. Nevertheless, the available evidence allows some conclusions.

Overwhelmingly, it suggests that the GDPR is impacting innovation negatively. Representative surveys find large, even overwhelming numbers of firms reporting innovations being abandoned or foregone, with AI especially obstructed. Econometric studies are consistent with this, finding reductions in radical innovations, AI development, and VC investment. Younger, smaller and more tech/data-heavy firms are particularly affected. Case-based and anecdotal accounts suggest medical research and innovation may be particularly badly hit. The occasional positive innovation effects the studies uncover do not alter this basic picture: certain types of incremental innovations may have risen, but firms seem not to consider these particularly valuable. Improved data governance likely facilitates AI adoption, but by itself seems not to make up for the GDPR’s overall negative effect on AI, except possibly for rather atypical companies, like large US banks. There is little evidence for increased trust driving higher technology adoption. Data portability seems to be little used. That a substantial data protection compliance software industry has developed is directly traceable to the GDPR. However, it seems dominated by US firms. European entrepreneurs appear to have rarely been able to seize this market opportunity.

Frustratingly, few studies provide quantitative estimates for the size of this hit to innovation. Surveys consistently suggest very many firms are affected. How large the “average” effect is, though, is less clear. Where studies quantify effects, these are mostly small. However, these estimates are generally based on data for ~2018–~2021. We do not have estimates for the years since. If the full effect of the GDPR accumulates over time – as surveys indicate – later data could show greater effects.

While online tracking and personalized advertising has attracted intense public concern (“surveillance capitalism”), it appears to have been impacted relatively little, likely due to a mix of techno-economic flexibility facilitating adjustment (e.g. consent tech) and de-facto regulatory forbearance. It is also the best-studied sector, perhaps because high-quality data could be obtained comparatively easily. Conversely, university and especially medical research may be among the most affected, due to a mix of high regulatory burden (Art. 9), extremely risk-averse public-sector compliance cultures and limited resources. This would be a deeply ironic, even perverse outcome. Given their societal and strategic economic significance, it is unfortunate that not more empirical research has been done on the GDPR’s effects on medical and “deep tech” sectors (e.g. autonomous systems).

Extant research has not systematically tested which of the different mechanisms discussed are most responsible for the GDPR’s innovation-obstructing effects. Most likely it is some combination of reduced ability

<sup>18</sup> Own, ongoing research.

to access and use data, and complicated, burdensome compliance. In practice, at least with the GDPR, the principles-based approach seems to have delivered paralysis more than flexibility. Sometimes, this may be due to bizarre readings of the GDPR by compliance staff. Fundamentally though, a regulation and regulatory culture that apparently invites such responses even from highly sophisticated institutions, and which the broad mass of firms struggle to fully implement even years later, must be assessed as unworkable.

A further question in this regard is the GDPR's interactions with other legislation, such as the 2002 ePrivacy Directive, which regulates processing of personal data from end-user devices (including cookie setting). The ePrivacy Directive is more specific and rigid than the GDPR (e.g. no "legitimate interests"-clause, no purpose compatibility tests). The sharp changes after ~2018 discussed above suggest that, by itself, the Directive likely had only limited influence on data-processing practices. It is however possible that the "shock" of the GDPR, which sets the overall legal framework, prompted stricter adherence to the ePrivacy Directive also, and that some of the effects discussed above are more properly attributed to the interaction of ePrivacy and GDPR, than to the GDPR alone.<sup>19</sup>

These findings imply a need for significant reform if Europe is not to fall further behind technologically and economically. Fundamentally, a better balance needs to be struck between individual interest in privacy and data protection, and the collective interest in technology development and growth. The question is how this can be achieved. On this, the essay's authors differ.

Among the two authors, the political scientist and innovation-studies scholar (Martin) believes legislators should bite the bullet and significantly lower the substantive requirements of data protection law. The focus should be on reducing rules and restrictions governing the collection, use and sharing of data. Automatically, this will also reduce compliance burdens. Conversely, a focus on easing compliance – rather than on easing data use as such – is liable to achieve neither. With the clarification on the nature of personal data and the provisions under Article 9, in particular, the Digital Omnibus Law takes important steps in the right direction. Further levers to consider are clarifying and if necessary expanding research exemptions to make clear that they apply in full to industry research also, that research can per se mostly be conducted under legitimate-interest grounds, and that compatibility of purpose and thus an exemption from purpose limitation is presumed. More generally, and beyond research exemptions, it is worth considering whether the principles of purpose limitation and data minimisation need not be substantially rethought for the present technological era, to make them less restrictive. It could also be worth debating whether opt-out rather than opt-in consent might not be acceptable in some circumstances. Negative externalities from digital technology are real, and demand regulatory action. But tools other than data-protection law may often be better suited to address these. For instance, social-media addiction, polarisation and mental (il-)health is likely *not* best addressed through the GDPR.

In contrast, the legal scholar among the two authors (von Grafenstein), trained in regulating innovation, is convinced, based on research findings that focus on the interaction of law and innovation [85], that stronger focus on reducing legal uncertainty, and increasing effectiveness and above all, efficiency in the implementation of the GDPR is the most relevant entry point for improving regulation [86]. As discussed, the principle-based approach of the GDPR leaves a great deal of leeway in its implementation. National implementation and certain national compliance cultures – in particular, the highly rule-oriented and extraordinarily risk-averse German compliance culture – arguably carry much of the blame for the difficulties with the GDPR.

Some of the examples cited earlier by the co-author of this paper are

<sup>19</sup> We are indebted to an anonymous reviewer for drawing our attention to this matter.

perfect illustrations of this: In practice, there is considerable legal uncertainty regarding the aspects mentioned. However, the wording of the law already provides significant relief for research projects, especially for statistical analyses: in particular (and not only), statistical analyses can already be based in the vast majority of cases on legitimate interests and thus on an opt-in procedure (Art. 6(1)(f); compatibility of purpose is presumed for research purposes (Art. 5(1)(b)), and the rights of data subjects in Art. 15 ff. can be waived (Art. 89(2)). This also applies to private research projects (recital 159 GDPR).

The interpretation of the explicit wording of the law also gives rise to considerable legal uncertainty in practice: The principle of purpose limitation is often discussed as being hostile to innovation, without clarifying what it actually prescribes in concrete terms; and when its regulatory content is examined more closely, it turns out to be surprisingly open to innovation [86]. Similarly, the principle of data minimisation is often interpreted as meaning that as little data as possible should be processed, although it actually only says that the personal reference of the information contained in the data should be reduced, and only to the extent possible (and not necessarily further) [87]. If these simplifications are not applied in practice, this is not due to the substantial requirements, but to legal uncertainties in practice. Legislative changes should therefore focus on reducing these uncertainties and on ensuring efficient procedures to apply the law effectively.<sup>20</sup>

For certain cases, indeed, there is a need for more substantial flexibility. For example, with regard to the rigid regulation of the ePrivacy Directive. As the current Digital Omnibus proposal does, this should therefore be incorporated into the more flexible GDPR, with its purpose compatibility test, the legitimate interests-clause and the risk-dependent application of opt-in and (!) opt-out mechanisms. The particular potential for abuse that the ePrivacy Directive actually sought to control should instead be addressed through an obligatory certification requirement (which is currently optional in the GDPR) [88].

Whichever approach the legislators takes, the new law should in time be subject to rigorous empirical evaluation, focusing not only on its economic but also its wider societal effects. Should liberalization lead to significant harms, it is important to uncover and amend this. Conversely, should reform *not* produce such harms, this too would be an important data point. More evidence-based regulation and a regulatory culture that systematically assesses real outcomes and where necessary initiates evidence-based reform would contribute significantly to the rationality of the legal system itself, and restore confidence in the efficiency of our European constitutional systems.

## Funding

This paper was partially supported by German Federal Ministry of Research, Technology and Space as part of the research project "DatenTRAFO" (16KIS1882K)

## Declaration of generative AI and AI-assisted technologies in the writing process

No generative AI or AI-assisted technologies were used in the writing process

## Declaration of competing interest

The authors – Nicholas Martin and Max von Grafenstein – declare that there are no conflicting interests related to this paper

<sup>20</sup> See also the recommendations the article by v. Grafenstein, M., Resolving the value for risk-dilemma by (data) governance laws and other mechanisms, in this special issue.

## Acknowledgements

We would like to thank Knut Blind and Christian Rammer for helpful comments on an earlier draft, and the anonymous reviewers for their very useful suggestions for improvement. All remaining errors are our own.

## Data availability

No data was used for the research described in the article.

## References

- OECD/Eurostat. Oslo manual 2018: guidelines for collecting, reporting and using data on innovation. 4th Edition. Paris: The Measurement of Scientific, Technological and Innovation Activities, OECD Publishing; 2018. <https://doi.org/10.1787/9789264304604-en>.
- Metzger F, Krauß K. Clarifying new urban mobility services based on a threefold business model framework. *Transp Res Interdiscip Perspect* 2024;27. <https://doi.org/10.1016/j.trip.2024.101207>.
- Grafenstein Mv. Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I. *Eur Data Prot Law Rev* 2020;6(4):509–21. <https://doi.org/10.21552/edpl/2020/4/7>.
- Grafenstein Mv. Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II. *Eur Data Prot Law Rev* 2021;7(2):190–205. <https://doi.org/10.21552/edpl/2021/2/8>.
- Grafenstein Mv. Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III. *Eur Data Prot Law Rev* 2021;7(3):373–87. <https://doi.org/10.21552/edpl/2021/3/6>.
- Nissenbaum H. *Privacy in context technology, policy, and the integrity of social life*. 1st ed. Stanford: Stanford University Press; 2009.
- Lerner J, Nanda R. Venture capital's role in financing innovation: what we know and how much we still need to learn. *J Econ Perspect* 2020;34(3):237–61. <https://doi.org/10.1257/jep.34.3.237>.
- Martin N, Matt C, C.Niebel KBlind. How data protection regulation affects startup innovation. *Inf Syst Front* 2019;21(6):1307–24. <https://doi.org/10.1007/s10796-019-09974-2>.
- Grafenstein Mv. Co-regulation and the competitive advantage in gdpr: data protection certification mechanisms, codes of conduct and the “state of the art” of data protection-by-design. In: González-Fuster G, Brakel Rv, De Hert P, editors. *Research handbook on privacy and data protection law. values, norms and global politics*. Cheltenham: Edward Elgar Publishing; 2019. p. 402–32.
- Johnson G. *Economic research on privacy regulation: Lessons from the GDPR and beyond*. In: Goldfarb A, Tucker C, editors. *The Economics of Privacy*. University of Chicago Press; 2022.
- Bitkom. DS-GVO, ePrivacy, brexit – datenschutz und die wirtschaft. 2019. <https://www.bitkom.org/sites/main/files/2019-09/bitkom-charts-pk-privacy-17-09-2019.pdf>. accessed 27 November 2025.
- BitKom. DS-GVO und corona – Datenschutzherausforderungen für die wirtschaft. 2020. <https://www.bitkom.org/sites/main/files/2020-09/bitkom-charts-pk-privacy-29-09-2020.pdf>. accessed 27 November 2025.
- BitKom. Datenschutz als Daueraufgabe für die wirtschaft: ds-gvo & internationale datentransfers. 2021. <https://www.bitkom.org/sites/main/files/2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf>. accessed 27 November 2025.
- BitKom. Datenschutz in der deutschen wirtschaft: ds-gvo & internationale datentransfers. 2022. [https://www.bitkom.org/sites/main/files/2022-09/Bitkom-Charts%20Datenschutz%2027%2009%202022\\_final.pdf](https://www.bitkom.org/sites/main/files/2022-09/Bitkom-Charts%20Datenschutz%2027%2009%202022_final.pdf). accessed 27 November 2025.
- BitKom. Wo steht die deutsche wirtschaft beim datenschutz?. 2023. <https://www.bitkom.org/sites/main/files/2023-10/231005Bitkom-ChartsDatenschutzfinal.pdf>. accessed 27 November 2025.
- BitKom. Wo steht die deutsche wirtschaft beim datenschutz?. 2024. <https://www.bitkom.org/sites/main/files/2024-09/241001-Bitkom-Charts-Datenschutz-final.pdf>. accessed 27 November 2025.
- Blind K, Niebel C, Rammer C. The Impact of the EU General Data Protection Regulation on Innovation in Firms. *ZEW - Cent Eur Econ Res Discuss* 2022;22–047. <https://doi.org/10.2139/ssrn.4257740>.
- Blind K, Niebel C, Rammer C. The impact of the EU General Data Protection Regulation on product innovation. *Ind Innov* 2022;31(3):311–51. <https://doi.org/10.1080/13662716.2023.2271858>.
- Ambec S, Cohen MA, Elgie S, Lanoie P. The porter hypothesis at 20: can environmental regulation enhance innovation and competitiveness? *Rev Environ Econ Policy* 2013;7(1):2–22. <https://doi.org/10.1093/reep/res016>.
- R. Cao, T. Kretschmer, Regulation as opportunity: proactive GDPR compliance in the US financial services industry, *Indus Corp Change*, (2025). DOI: <https://doi.org/10.1093/icc/dtaf031>.
- Frey CB, Presidente G. Privacy regulation and firm performance: estimating the GDPR effect globally. *Econ Inq* 2024;62(3):1074–89. <https://doi.org/10.1111/eicn.13213>.
- Dewitte P. AI Meets the GDPR: navigating the Impact of Data Protection on AI Systems. In: Smuha NA, editor. *The cambridge handbook of the law, ethics and policy of artificial intelligence*. cambridge law handbooks. Cambridge University Press; 2020. p. 133–57.
- Hallinan D, Leenes R, de Hert P. *Data protection and privacy: data protection and artificial intelligence*. Oxford: Hart Publishing; 2021. <https://doi.org/10.1111/1468-2230.12655>.
- Sartor G, Lagioia F. The impact of general data protection regulation (GDPR) on artificial intelligence. Brussels: European Parliament; 2020. <https://doi.org/10.2861/293>. 2020.
- Erdsiek D, Rost V. Branchenreport Informationswirtschaft, ZEW Leibnitz Zentrum für Europäische Wirtschaftsforschung. 2024. <https://www.zew.de/fileadmin/FTP/brepikt/202401BrepIKT.pdf>. accessed 27 November 2025.
- Bradford A. The brussels effect: how the european union rules the world. New York, NY: Oxford University Press; 2020. <https://doi.org/10.1093/oso/9780190088583.001.0001>.
- Canayaz M, Kantorovitch I, Mihet R. Consumer privacy and value of consumer data swiss finance institute research paper series. Swiss Finance Institute; 2022. p. 22–68. <https://doi.org/10.2139/ssrn.3986562>.
- Frey CB, Presidente G, G. Data-Biased innovation: directed technological change and the future of artificial intelligence. Oxford Martin School working paper series; 2024. <https://www.oxfordmartin.ox.ac.uk/publications/data-biased-innovation-directed-technological-change-and-the-future-of-artificial-intelligence>. accessed 26 November 2025.
- Lalova-Spinks T, Sutter ED, Valcke P. Challenges related to data protection in clinical research before and during the COVID-19 pandemic: an exploratory study. *Front Med (Lausanne)* 2022;9:995689. <https://doi.org/10.3389/fmed.2022.995689>.
- Clarke N, Vale G, Reeves EP. GDPR: an impediment to research? *Ir J Med Sci* 2019;188(4):1129–35. <https://doi.org/10.1007/s11845-019-01980-2>.
- Lawlor RT. The impact of GDPR on data sharing for European cancer research. *Lancet Oncol* 2023;24(1):6–8. [https://doi.org/10.1016/S1470-2045\(22\)00653](https://doi.org/10.1016/S1470-2045(22)00653).
- Hallinan D. Broad consent under the GDPR: an optimistic perspective on a bright future. *Life Sci Soc Policy* 2020;16(1). <https://doi.org/10.1186/s40504-019-0096-3>.
- Chico V. The impact of the General Data Protection Regulation on health research. *Br Med Bull* 2018;128(1):109–18. <https://doi.org/10.1093/bmb/ldy038>.
- Bobrov E, Habermehl C, Strech D, Weissgerber T, Bernard R. Six solutions for clinical data sharing in Germany. *BMC Med Res Methodol* 2025;25(1):140. <https://doi.org/10.1186/s12874-025-02560-y>.
- Cagnazzo C. The thin border between individual and collective ethics: the downside of GDPR. *Lancet Oncol* 2021;22(11):1494–6.
- Glintborg B, Hansson M, Hammer HB. Legal obstacles jeopardise research in personalised medicine – experiences from a Nordic collaboration within rheumatology. *Scand J Public Health* 2024;52(8):1019–25. <https://doi.org/10.1177/14034948231212711>.
- Bentzen HB, Olav HK, Ursin G. Maximizing the GDPR potential for data transfers: first in Europe. *Lancet Reg Health Eur* 2023;27. <https://doi.org/10.1016/j.lanepe.2023.100600>.
- ALLEA, EASAC & FEAM. International sharing of personal health data for research. ALLEA, EASAC and FEAM joint initiative on resolving the barriers of transferring public sector data outside the EU/EEA; 2021. [https://allea.org/wp-content/uploads/2021/03/International-Health-Data-Transfer\\_2021\\_web.pdf](https://allea.org/wp-content/uploads/2021/03/International-Health-Data-Transfer_2021_web.pdf). accessed 26 November 2025.
- Yom-Tov E, Ofra Y. Implementation of data protection laws in the European union and in California is associated with a move of clinical trials to countries with fewer data protections. *Front Med (Lausanne)* 2022;9. <https://doi.org/10.3389/fmed.2022.1051025>.
- Brück O, Sanmark E, Ponkilainen V. European Health Regulations Reduce Registry-Based Research. *Health Res Policy Syst* 2024;22(1):135. <https://doi.org/10.1186/s12961-024-01228-1>.
- Miller AR, Tucker C. Privacy protection and technology diffusion: the case of electronic medical records. *Manage Sci* 2009;55(7):1077–93. <https://doi.org/10.1287/mnsc.1090.1014>.
- Miller AR, Tucker C. Can health care information technology save babies? *J Polit Econ* 2011;119(2):289–324. <https://doi.org/10.1086/660083>.
- Miller AR, Tucker C. Privacy protection, personalized medicine and genetic testing. *Manage Sci* 2018;64(10):4648–68. <https://doi.org/10.1287/mnsc.2017.2858>.
- Janssen R, Kesler R, Kummer ME, Waldfogel J. GDPR and the lost generation of innovative apps (No. w30028). National Bureau of Economic Research; 2022.
- Kollnig K, Binns R. The cost of the gdpr for apps? nearly impossible to study without platform data. 2022. <https://arxiv.org/abs/2206.09734>. accessed 26 November 2025.
- Demirer M, Jiménez Hernández DJ, Li D, Peng S. Data, privacy laws and firm production: evidence from the GDPR. *Natl Bur econ res* 2024. <https://doi.org/10.3386/w32146>. accessed 26 November 2025.
- Marti AP. The birth of a geopolitical eu cloud industry – reclaiming open source as a tool for europe's technological sovereignty. 2022. <https://sovereignedge.eu/bl og/the-birth-of-a-geopolitical-eu-cloud-industry/>. accessed 26 November 2025.
- Bitkom. Data economy and data act: wo steht die deutsche wirtschaft 2025?. 2025. <https://www.bitkom.org/sites/main/files/2025-09/bitkom-studienbericht-dat-a-economy.pdf>. accessed 26 November 2025.
- S.Kreutzer THeimer, Bauer B, Rabe L, Blind K, Martin N, Grafenstein Mv, Streblov R, Du J, Joel D. Datentreuhänder als schlüssel zum datenteilen: ansätze, herausforderungen und empfehlungen für die umsetzung. 2., korrigierte Auflage. - Aachen: E.ON Energieforschungszentrum, RWTH Aachen University Bericht (White Paper); 2025.

- [50] Giattino C, Mathieu E, Samborska V, Roser M. Annual private investment in artificial intelligence. 2025. <https://archive.ourworldindata.org/20250909-093708/grapher/private-investment-in-artificial-intelligence.html>. accessed 27 November 2025.
- [51] Johnson GA, Shriver SK, Goldberg SG. Privacy and market concentration: intended and unintended consequences of the GDPR. *Manage Sci* 2023;69(10):5695–721. <https://doi.org/10.1287/mnsc.2023.4709>.
- [52] Lefrere V, Warberg L, Cheyre C, Marotta V, Acquisti A. Does Privacy Regulation Harm Content Providers? A Longitudinal Analysis of the Impact of the GDPR. *Manage Sci* 2025. <https://doi.org/10.1287/mnsc.2022.03186>.
- [53] T. Libert, L. Graves, R. Kleis Nielsen, Changes in Third-Party Content on European News Websites after GDPR, Oxford Reuters Institute for the Study of Journalism, <https://doi.org/10.60625/risj-r2ex-7248>, 2018 (accessed 27 November 2025).
- [54] Aridor G, Yeon-Koo C, Salz T. The effect of privacy regulation on the data industry: empirical evidence from GDPR. *Rand J Econ* 2023;54(4):695–730. <https://doi.org/10.1111/1756-2171.12455>.
- [55] Miller KM, Lukic K, Skiera B. The impact of the General Data Protection Regulation (GDPR) on online tracking. *Int J Res Mark* 2025. <https://doi.org/10.1016/j.ijresmar.2025.03.002>.
- [56] Kollnig K, Binns R, Van Kleek M, Lyngs U, Zhao J, Tinsman C, Shadbolt N. Before and after GDPR: tracking in mobile apps. *Internet Policy Rev* 2021;10(4).
- [57] Goldberg S, Johnson GA, Garrett A, Shriver SK. Regulating Privacy Online: an Economic Evaluation of the GDPR. *Am Econ J: Econ Policy* 2024;16(1):325–58. <https://doi.org/10.1257/pol.20210309>.
- [58] Quantcast. Quantcast choice powers one billion consumer consent choices in two months since gdpr. 2018. <https://marcommnews.com/quantcast-choice-powers-one-billion-consumer-consent-choices-in-two-months-since-gdpr/>. Accessed 25 November 2025.
- [59] Aridor G, Yeon-Koo C, Salz T. The economic consequences of data privacy regulation: empirical evidence from GDPR. *Rand J Econ* 2023;54(4):695–730. <https://doi.org/10.1111/1756-2171.12455>.
- [60] Godinho de Matos M, Adjrid I. Consumer consent and firm targeting after the GDPR: the case of large telecom provider. *Manage Sci* 2022;68(5):325–58. <https://doi.org/10.1287/mnsc.2021.4054>.
- [61] Peukert C, Bechtold S, Batikas M, Kretschmer T. Regulatory Spillovers and Data Governance: evidence from the GDPR. *Mark Sci* 2022;41(4):746–68. <https://doi.org/10.1287/mksc.2021.1339>.
- [62] Schmitt J, Miller K, Skiera B. The impact of the General Data Protection Regulation (GDPR) on Online Usage Behavior. *HEC Paris Res Pap No MKG-2021-1437* 2024. <https://doi.org/10.2139/ssrn.3774110>.
- [63] Congiu R, Sabatino L, Sapi G. The Impact of Privacy Regulation on Web Traffic: evidence From the GDPR. *Inf Econ Policy* 2022;61. <https://doi.org/10.1016/j.infoecopol.2022.101003>.
- [64] Glinborg B, Hansson M, H.B Hammer. Legal obstacles jeopardise research in personalised medicine – experiences from a Nordic collaboration within rheumatology. *Scand J Public Health* 2024;52(8):1019–25. <https://doi.org/10.1177/14034948231212711>.
- [65] Draghi M. The future of european competitiveness. Luxembourg: Publications Office of the European Union; 2024. [https://commission.europa.eu/topics/competitiveness/draghi-report\\_en](https://commission.europa.eu/topics/competitiveness/draghi-report_en). accessed 27 November 2025.
- [66] European Commission. Commission staff working document accompanying the eu startup and scaleup strategy: choose europe to start and scale. SWD; 2025. p. 138. [https://research-and-innovation.ec.europa.eu/document/download/8f899486-6e4e-48df-8633-9582375f41eb\\_en](https://research-and-innovation.ec.europa.eu/document/download/8f899486-6e4e-48df-8633-9582375f41eb_en). 2025 (Accessed 25 November 2025).
- [67] Jia J, G Z Jin, Wagman L. The short-run effects of the General Data Protection Regulation on technology venture investment. *Mark Sci* 2021;40(4):661–84. <https://doi.org/10.1287/mksc.2020.1271>.
- [68] Jian J. The persisting effects of the EU general data protection regulation on technology venture investment. *Antitrust Source* 2021.
- [69] J. Jian, G.Z. Jin, M. Lecess, L. Wagman, How does privacy regulation affect transatlantic venture investment? Evidence from GDPR. NBER Working Paper No. W33909. (2025). DOI: <https://ssrn.com/abstract=5296541>.
- [70] Campbell J, Goldfarb A, Tucker C. Privacy regulation and market structure. *J Econ Manag Strategy* 2015;24:47–73. <https://doi.org/10.1111/jems.12079>.
- [71] IAPP International Association of Privacy Professionals. 2022 Privacy Tech Vendors Report V6.1.03. 2022. [https://iapp.org/media/pdf/resource\\_center/2022TechVendorReport.pdf](https://iapp.org/media/pdf/resource_center/2022TechVendorReport.pdf). Accessed 27 November 2025.
- [72] Martin N, Ebberts F. When Regulatory Power and Industrial Ambitions Collide: the “Brussels Effect,” Lead Markets, and the GDPR. In: Schiffner S, Ziegler S, Rodriguez A Quesada, editors. *Privacy symposium*. Cham: Springer; 2022. p. 129–51. [https://doi.org/10.1007/978-3-031-09901-4\\_8](https://doi.org/10.1007/978-3-031-09901-4_8).
- [73] The Royal Society. Protecting privacy in practice: the current use, development and limits of privacy enhancing technologies in data analysis. London: The Royal Society; 2019. <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/protecting-privacy-in-practice.pdf>. Accessed 27 November 2025.
- [74] Macgillivray A. Advancing a vision for privacy-enhancing technologies. *The White House*; 2022. <https://bidenwhitehouse.archives.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/>. 2022 Accessed 27 November 2025.
- [75] Bauer PC, Gerdon F, Keusch F, Kreuter F, Vannette D. Did the GDPR increase trust in data collectors? Evidence from observational and experimental data. *Inf Commun Soc* 2022;25(14):2101–21. <https://doi.org/10.1080/1369118X.2021.1927138>.
- [76] N. Kalkkreuth, M. Kopka, C. Schmid, C. Kratzer, A. Reptuschenko, M.A. Feufel, Trustworthiness of the electronic health record in Germany: an exploratory, user centered analysis. *Front Digit Health*. 7 (2025). DOI: <https://doi.org/10.3389/fgdth.2025.1473326>.
- [77] Rousi R, Piispanen JR, Boutellier J. I trust you Dr. Researcher, but not the company that handles my data - trust in the data economy. In: Presentation at the 57th Hawaii International Conference on System Sciences (HICCS), Waikiki Beach Resort, January 3-6. University of Hawaii at Manoa; 2024. p. 4632–41. <https://doi.org/10.24251/HICCS.2024.556>.
- [78] Engels B. Data portability among online platforms. *Internet Policy Rev* 2016;5(2). <https://doi.org/10.14763/2016.2.408>.
- [79] Krämer J, Stüdle N. Data portability, data disclosure and data-induced switching costs: some unintended consequences of the General Data Protection Regulation. *Econ Lett* 2019;181:99–103. <https://doi.org/10.1016/j.econlet.2019.05.015>.
- [80] Wohlfahrt M. Data Portability on the Internet. *Bus Inf Syst Eng* 2019;61:551–74. <https://doi.org/10.1007/s12599-019-00580-9>.
- [81] Lam WMW, Liu X. Does Data Portability Facilitate Entry? *Int J Ind Organ* 2020;69(3). <https://doi.org/10.1016/j.ijindorg.2019.102564>.
- [82] Ramos EF, Blind K. Data portability effects on data-driven innovation of online platforms: analyzing Spotify. *Telecomm Policy* 2020;44(9):102026. <https://doi.org/10.1016/j.telpol.2020.102026>.
- [83] Syrmodis E, Grossklags SAJ. A longitudinal analysis of corporate data portability practices across industries. In: *Proceedings - Annual Computer Security Applications Conference, ACSAC*; 2024. p. 207–23. <https://doi.org/10.2209/ACSAC63791.2021.00032>.
- [84] Presthus W, Sørum H. A Three-year study of the GDPR and the consumer. In: *14th IADIS International Conference Information Systems*; 2021.
- [85] Eifer M, Hoffmann-Riem W. *Innovation und rechtliche regulierung*. Baden-Baden: Nomos; 2018.
- [86] Grafenstein MV. The principle of purpose limitation in data protection laws. the risk-based approach, principles, and private standards as elements for regulating innovation. *Baden-Baden: Nomos*; 2018.
- [87] Rupp V, Grafenstein Mv. Clarifying “personal data” and the role of anonymisation in data protection law: including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection. *Comput Law Secur Rev* 2024;52. <https://doi.org/10.1016/j.clsr.2023.105932>.
- [88] v M, Heumüller J, Belgacom E, Jakobi T, Smieskol P, Wunderlich L. Effective regulation through design – Aligning the ePrivacy regulation with the EU general data protection regulation (GDPR): tracking technologies in personalised internet content and the data protection by design approach. *OpenAIRE* 2021. <https://doi.org/10.5281/zenodo.5575447>.