



FEBRUARY 2022

# Privacy Law Pitfalls

## Lessons Learned from the European Union

In 2022, the Government of Canada is expected to introduce legislation to advance its Digital Charter and strengthen privacy protections for consumers.

This legislation will replace a made-in-Canada law (the Personal Information Protection and Electronic Documents Act, known as PIPEDA), which served for more than a decade as the international gold standard for the protection of personal information but now needs to be updated.

This report compiles critical analyses of the European Union (EU)'s experience with its privacy law, the General Data Protection Regulation (GDPR), since it took effect in 2018. While the GDPR improved data protection rights and awareness for consumers, it has proven over time to be much better in theory than in practice.

This report is a cautionary tale for Canadian legislators. The European Union's troubled experience with its data privacy law is one of the chief reasons that the Canadian Marketing Association is calling for another made-in-Canada balanced approach to privacy law reform.

## **Preface**

---

Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) served for more than a decade as the international gold standard for the protection of personal information.

PIPEDA's widely recognized strengths include its balanced purpose statement, which embraces the enormous social and economic benefits of data use for Canadians, while protecting individuals' right to privacy. Its principles-based framework, for the most part, has stood the test of time. It has provided considerable flexibility, allowing privacy protections to be applied to a range of fast-moving technologies and applications.

As the Canadian government prepares to replace PIPEDA with a law that provides more meaningful privacy protection in the digital age, it has the opportunity to once again create legislation that serves as a model for the world. Canadian policymakers must ensure that any new law is not simply imported from another jurisdiction, but rather, that it reflects and supports local conditions, practices and expectations, with the goal of achieving equivalent privacy protection as opposed to alignment to another jurisdiction's legislative approach.

Most notably, while the European Union (EU)'s privacy law—the General Data Protection Regulation (GDPR)—has significantly moved the dial on data protection issues and awareness, there has been growing acknowledgement since its inception in 2018 that the GDPR's shortcomings have led to some significant unintended consequences that are negatively impacting governments, consumers and organizations. These are pitfalls that policymakers in other jurisdictions would be wise to avoid.

This report documents the GDPR's main pitfalls. It is intended to be a cautionary tale to Canada as it pursues privacy law reform. In evaluating the suitability of GDPR provisions, Canadian policymakers must consider potential unintended negative impacts of the new law on the Canadian economy, particularly at a time when data innovation is critical to economic growth and competitiveness for the long-term.

Among those who would be most adversely impacted by having certain GDPR provisions imported to Canada would be small and medium-sized enterprises (SMEs)—the backbone of the Canadian economy. According to a recent survey of more than

1,000 Canadian SMEs<sup>1</sup>, having the ability to leverage consumer data to communicate regularly and in a personalized and relevant manner with customers was cited as the primary way SMEs gained and maintained consumer trust and loyalty to weather the pandemic. Privacy requirements that do not consider the impact on SMEs could prove debilitating in terms of the capital required and limitations on their ability to automate and optimize. SMEs lack ready access to legal advice and representation to navigate the complexities of overly prescriptive and unnecessarily restrictive legislation, making it more difficult for them to use data to innovate and compete.

Small business owners in Canada are extremely concerned with current costs relating to regulation, noting that this is one of their top concerns. In 2020, small businesses in Canada spent a total of C\$38.8 billion on the cost of compliance and red tape stemming from regulation from all three levels of government (municipal, provincial and federal).<sup>2</sup> Business owners believe this amount—which they have attributed to ‘red tape’—a euphemism for excessive regulation<sup>3</sup>—can be reduced by nearly one-third (C\$10.8 billion). In Canada, the smallest businesses are already paying the highest costs for overall regulatory compliance (including privacy and other types of business regulation, at a whopping cost per employee of C\$7,023 annually for businesses with less than five employees). This is significantly less than the C\$1,237 annually for businesses with 100-plus employees.<sup>4</sup>

In evaluating the suitability of including GDPR-derived provisions in Canadian legislation, Canada must consider the context of those provisions in the EU, their effectiveness as measured against the European experience, the demonstrated need for such provisions in Canada, and the impact of resulting unintended consequences on the Canadian economy and consumer expectations, particularly as the country prepares for economic recovery and expansion.

The GDPR’s pitfalls underscore the importance of ensuring that Canadian privacy law continues to be rooted in an administratively workable, principles-based legislative framework that promotes a technology- and sector-neutral approach to privacy, helping to ensure flexibility in the face of rapidly evolving technologies, business models and consumer expectations. In addition, they illustrate the importance of ensuring privacy law continues to be guided by a balanced purpose statement that enables organizations to use personal information to conduct essential aspects of business in a manner that improves the lives of individuals, while protecting their privacy rights.

<sup>1</sup> [The State of Small and Medium Businesses in 2021, Phase 5, 2021.](#)

<sup>2</sup> [Canada’s Red Tape Report – Sixth Edition: The Cost of Regulation to Small Business](#), Canadian Federation of Independent Businesses (CFIB), 2021. Results based on CFIB survey on Regulation and Paper burden, conducted in 2020, (n=4,603).

<sup>3</sup> *Ibid.*

<sup>4</sup> [Canada’s Red Tape Report – Sixth Edition: The Cost of Regulation to Small Business](#), CFIB, 2021. Calculations based on CFIB Survey on Regulation and Paper burden, conducted in 2020, (n=4,603) and data from Statistics Canada.

# Table of Contents

---

- Preface .....2
- Executive Summary.....5
- Introduction ..... 6
- Summary of Research in Key Areas ..... 8
  - 1. Creating a staggering regulatory burden ..... 8
  - 2. Hampering the ability of organizations to innovate and contribute to economic growth ..... 10
  - 3. Disproportionately impacting small and medium-sized enterprises..... 15
  - 4. Creating complexity for consumers ..... 18
  - 5. Triggering other inefficiencies and unintended consequences ..... 21
    - A. Lack of proportionality .....22
    - B. Complexity and rigidity.....23
    - C. Disproportionate use of a human rights framework.....23
  - 6. Suppressing emerging technologies .....25
    - A. Artificial intelligence .....25
    - B. Automated decision-making .....27
  - 7. Obstructing cross-border business .....27
- Sources.....31
- About the Canadian Marketing Association .....33

## **Executive Summary**

---

As Canada embarks on private sector privacy reform, it has much to learn from the pitfalls of the European Union (EU)'s privacy law—the General Data Protection Regulation (GDPR).

Although the GDPR framework represented a significant step forward in drawing awareness to privacy and data protection around the globe, introducing new privacy rights for consumers, and strengthening data protection requirements and penalties, after more than three years, it has proven to be much better in theory than in practice.

This report compiles a growing body of research and commentary on the GDPR's pitfalls—including from some of the law's original drafters—in the following seven areas. It is a cautionary tale for Canadian policymakers to avoid the negative consequences that have resulted—for governments, consumers and organizations alike—from the GDPR's overly complex, prescriptive or otherwise disproportionate provisions.

1. Creating a staggering regulatory burden
2. Hampering the ability of organizations to innovate and contribute to economic growth
3. Disproportionately impacting small and medium-sized enterprises
4. Creating complexity for consumers
5. Triggering other inefficiencies and unintended consequences
6. Suppressing emerging technologies
7. Obstructing cross-border business

These pitfalls underscore the importance of ensuring that Canadian privacy law continues to be rooted in an administratively workable, principles-based legislative framework that promotes a technology- and sector-neutral approach to privacy, helping to ensure flexibility in the face of rapidly evolving technologies, business models and consumer expectations. They also illustrate the importance of ensuring privacy law continues to be guided by a balanced purpose statement that enables organizations to use personal information to conduct essential aspects of business in a manner that improves the lives of individuals, while protecting their privacy rights.

A made-in-Canada approach to privacy reform—one that balances effective privacy protection with the enormous social and economic benefits of data to Canadians—will enable Canada to reclaim its reputation as a global leader in protecting citizens' privacy while fostering innovation by business.

## Introduction

---

When the EU's GDPR came into effect on May 25, 2018, it was hailed by many as the new global standard for privacy and data protection.

Spurred on by the EU's adequacy requirements for international data transfers, governments around the world faced growing pressure to replicate the GDPR's provisions, even aspects that were untested.

Although the framework represented a significant step forward in drawing awareness to privacy and data protection around the globe, introducing new privacy rights for consumers, and strengthening data protection requirements and penalties, after more than three years, the GDPR has proven to be much better in theory than in practice. The GDPR has only partially achieved its intended objectives. Many stakeholders—including some of the law's original drafters—have identified key aspects of the law that have proven to be costly, unmanageable, or prohibitively expensive without providing a commensurate privacy benefit.

Although the difficulty in enforcing the GDPR—with its prescriptive and complex provisions—originally resulted in calls for more funding and resourcing for the law's oversight, the focus has now shifted to calls for a fundamental re-think of the law, and its interpretation and application. Johannes Caspar, who served as the Data Protection Commissioner of Hamburg, Germany for approximately 12 years, stated in June 2021 that *"the basic model of the procedure set up by GDPR has massive flaws and it just can't work."*<sup>5</sup>

Other jurisdictions have already begun to take steps to avoid the GDPR's pitfalls. For example, the UK has seized a post-Brexit opportunity to backtrack on the GDPR by consulting on how it can implement: "a more pro-growth and pro-innovation data regime."<sup>6</sup> The UK is pursuing a principles-based approach that better supports the potential of its growing digital economy.

**"The basic model of the procedure set up by GDPR has massive flaws and it just can't work."**

Johannes Caspar, former Data Protection Commissioner, Hamburg, Germany.

---

<sup>5</sup> [Europe's Data Law Is Broken, Departing Privacy Chief Warns](#), Bloomberg, 2021.

<sup>6</sup> [Data: A new direction](#), Department for Digital, Culture, Media & Sport, GOV.UK, 2021.

This report is a literature review that compiles a growing body of research and commentary on the GDPR's pitfalls in the following areas:

1. Creating a staggering regulatory burden
2. Hampering the ability of organizations to innovate and contribute to economic growth
3. Disproportionately impacting small and medium-sized enterprises
4. Creating complexity for consumers
5. Triggering other inefficiencies and unintended consequences
6. Suppressing emerging technologies
7. Obstructing cross-border business



# Summary of Research in Key Areas

---

## 1. Creating a staggering regulatory burden

Governments and regulators across the EU have been struggling to keep up with the challenging demands of GDPR interpretation, oversight and enforcement. Although the law was intended to reduce the EU's administrative burden and improve regulatory coordination, it has led to an enormous increase in permanent unanticipated costs for governments across the EU, as well as regulatory complexity and backlog.

Data and privacy regulators—known in Europe as Data Protection Authorities (DPAs)—and governments across the EU have been struggling to keep up with the challenging demands of GDPR interpretation, oversight and enforcement. Although the GDPR was supposed to reduce the EU's administrative burden, it has instead led to an enormous increase in permanent unanticipated costs for governments across the EU.<sup>7</sup> The GDPR's prescriptive nature has resulted in regulatory complexity and backlog.

Although the GDPR was intended to harmonize data protection among EU member countries, the law is interpreted differently across member countries and the majority of EU DPAs have expressed "...that they are not properly equipped to contribute to cooperation and consistency mechanisms."<sup>8</sup>

Approximately two-thirds (21) of European countries surveyed by the European Data Protection Board (EDPB) stated that DPAs do not have enough human, financial and technical resources to effectively regulate the full set of requirements of the GDPR.<sup>9</sup>

---

<sup>7</sup> POSITION PAPER: GDPR-Evaluation 2020: DDV calls for the removal of obstacles to innovation and bureaucracy, Deutscher Dialogmarketing Verband (DDV), 2020.

<sup>8</sup> Contribution of the EDPB to the evaluation of the GDPR under Article 97, European Data Protection Board (EDPB), 2020, p.30.

<sup>9</sup> Contribution of the EDPB to the evaluation of the GDPR under Article 97, EDPB, 2020.

## Additional details

- Governments are struggling to afford to implement the GDPR. According to research from Brave in 2020, half of all national DPAs receive annual budgets of C\$7.1 million or less from their governments, significantly less than what is required to fully implement the GDPR.<sup>10</sup> In a pandemic environment, the situation has gotten worse; after annual increases to DPA budgets peaked at 24% in 2019 for the application of the GDPR, they have now dropped to 15%.<sup>11</sup> “Out of 30 DPAs from all 27 EU countries, the United Kingdom, Norway, and Iceland, only nine said they were happy with their level of resourcing.”<sup>12</sup>
- The UK’s Information Commissioner’s Office (ICO) expressed that the GDPR’s 72-hour reporting deadlines caused issues for staff and services, as they were overwhelmed by businesses “over-reporting” potential data breaches due to fear of high penalties if they failed to notify DPAs.<sup>13</sup>
- A representative from the Commission Nationale de l’informatique et des Libertés (CNIL), the French DPA, stated that “the resources of the CNIL are insufficient to enforce the GDPR.”<sup>14</sup>
- Before implementing the GDPR, the European Commission predicted substantial savings in their economic impact assessment. Germany’s leading marketing association, the Deutscher Dialogmarketing Verband (DDV), argues that the opposite has occurred: the regulatory bureaucracy introduced by the GDPR has led to enormous additional costs.<sup>15</sup>

**From a survey of 30 Data Protection Authorities in Europe, only nine agree that they had sufficient resourcing.**

From Access Now report.

<sup>10</sup> [Europe’s governments are failing the GDPR](#), Brave, 2020. Converted to Canadian dollars from euros, based on an exchange rate of €1 = C\$1.42 by Xe on January 21, 2022.

<sup>11</sup> [Europe’s governments are failing the GDPR](#), Brave, 2020.

<sup>12</sup> [Two Years Under the EU GDPR](#), Access Now, 2020, p.9.

<sup>13</sup> [ICO warns on over-reporting of data breaches](#), Pinsent Masons, 2018.

<sup>14</sup> [European Privacy Regulators Find Their Workload Expands Along With Authority](#), The Wall Street Journal, 2019.

<sup>15</sup> [POSITION PAPER: GDPR-Evaluation 2020: DDV calls for the removal of obstacles to innovation and bureaucracy](#), DDV, 2020.

## 2. Hampering the ability of organizations to innovate and contribute to economic growth

Organizations in the EU are diverting significant resources to understanding and interpreting the law's complex and prescriptive provisions—at the expense of more meaningful privacy protection and innovation-generating activities. Faced with the burden of compliance, some organizations outside of the EU have localized data flows or stopped servicing the European market entirely, further impacting economic growth, trade and investment.

Since the introduction of the GDPR, privacy budgets for organizations across a variety of sectors, including the health, finance, and education sectors and within government itself, have been increasing at a startling pace. Privacy professionals from across the EU and five other countries, including Canada and the United States, reported an average 29% increase in their privacy budgets between 2020 and 2021 due to increased costs related to GDPR implementation, with 60% believing their companies' privacy budget was still insufficient.<sup>16</sup>

During this period, organizations allocated extensive human resources to GDPR implementation: more than half of privacy budgets (57%) are spent on employee salaries and travel, with a further 17% on legal and other consulting services.<sup>17</sup>

These expenses continue to be incurred, long after the law came into effect. A recent report by DataGrail indicated that the average organization in North America spent approximately 2,000 to 4,000 hours in meetings preparing for the GDPR, with some companies spending more than 9,000 hours in meetings prior to the GDPR's implementation.<sup>18</sup> Three-quarters (67%) of organizations had at least 25 employees involved in preparing for the GDPR, while 44% had at least 50 employees working on preparations.<sup>19</sup>

---

<sup>16</sup> IAPP-EY Annual Privacy Governance Report 2021, The International Association of Privacy Professionals (IAPP), 2021.

<sup>17</sup> *Ibid.*

<sup>18</sup> *The Cost of Continuous Compliance*, DataGrail, 2020.

<sup>19</sup> *The Cost of Continuous Compliance*, DataGrail, 2020. DataGrail partnered with Marketcube, a third-party research company, and surveyed 301 professionals in April 2019. All respondents work at companies with 50+ employees and are affected by GDPR, CCPA, or both.

The significant resources allocated to lawyers, consultants and compliance staff in order to understand and interpret the law's prescriptive provisions diverts spending from other organizational priorities. Initiatives not pursued due to this resource allocation might more directly improve privacy protection for consumers (e.g., investments in security improvements, or in consumer education and awareness) or support innovation and growth.

Faced with the burden of compliance, some organizations outside the EU have opted to localize their data flows, stop servicing the EU market, or otherwise adjust their operations. This has impacted trade and investment in the EU. Privacy professionals reported that the GDPR's requirements around cross-border data transfers are their most challenging task; 10% indicated these challenges led their firms to opt to localize data, discontinue a service, or stop data transfers to and from the EU altogether.<sup>20</sup>

For US companies, this challenge has been exacerbated by a decision by the Court of Justice of the European Union (CJEU), known as the "Schrems II" decision, which invalidated the EU-US Privacy Shield (a framework for regulating transatlantic exchanges of personal data for commercial purposes between the EU and the US), and suggested that the GDPR's standard contractual clauses may, on their own, be insufficient to ensure an adequate level of data protection for foreign data transfers.<sup>21</sup>

Organizations expect to allocate appropriate resources to comply with a reformed privacy law. At the same time, it behooves policymakers to establish and maintain the most efficient and effective model to achieve the desired outcomes. In the case of privacy protection, it is essential to have a law that is built on solid principles that provide flexibility and tailoring for specific applications, and that is understandable and achievable for non-specialists. For example, the framework underlying Canada's PIPEDA resulted in a high level of voluntary compliance from organizations over more than two decades.

**In a survey of 500+ German businesses, three-quarters said that innovative projects have failed due to GDPR requirements, and 86% reported stopping projects due to ambiguities with the GDPR.**

From Bitkom report.

<sup>20</sup> IAPP-EY Annual Privacy Governance Report 2021, IAPP, 2021. Results based on an IAPP-EY survey conducted on 473 privacy professionals.

<sup>21</sup> *Ibid.*

## Additional details

- The Information Technology and Innovation Foundation (ITIF) estimated that the cost to the American economy to implement a framework similar to the GDPR would be the equivalent of approximately C\$156 billion per year, or about C\$619 per adult.<sup>22</sup> Although the United States and Canada differ in many ways, and Canada already has a federal law, if we applied the ITIF's analysis to Canada, the cost to the Canadian economy would be approximately C\$19 billion.<sup>23</sup>
- In addition to implementation costs, the cost of violating the GDPR is exceptionally high. Canadian companies could face fines of up to C\$30 million or 4% of their worldwide revenue, whichever is higher.<sup>24</sup> In some cases, fines are extremely high, even for what many would consider to be more of a "procedural" violation, with no clear impact on the protection of the personal data of European residents. For example, LocateFamily.com, a Canadian company, was fined the equivalent of more than C\$750,000 for failing to designate a representative located in the EU, as required by Article 27 of the GDPR.<sup>25</sup>
- Investing in GDPR compliance has led to budget cutbacks elsewhere.<sup>26</sup> A survey of more than 400 European business leaders in 2019 discovered that "...a concerning number of businesses are cutting back in other areas including plans to create innovative new products (23%) or to fuel growth through international expansion (22%)."
- GDPR implementation has cost FTSE 350 and Fortune 500 companies in the United States and United Kingdom approximately C\$11.6 billion, including C\$20.6 million for the average Fortune 500 company.<sup>27</sup>

<sup>22</sup> The Costs of an Unnecessarily Stringent Federal Data Privacy Law, Information Technology and Innovation Foundation (ITIF), 2019. US\$122 billion was converted based on an exchange rate of US\$1 = C\$1.28 by Xe on December 10, 2021.

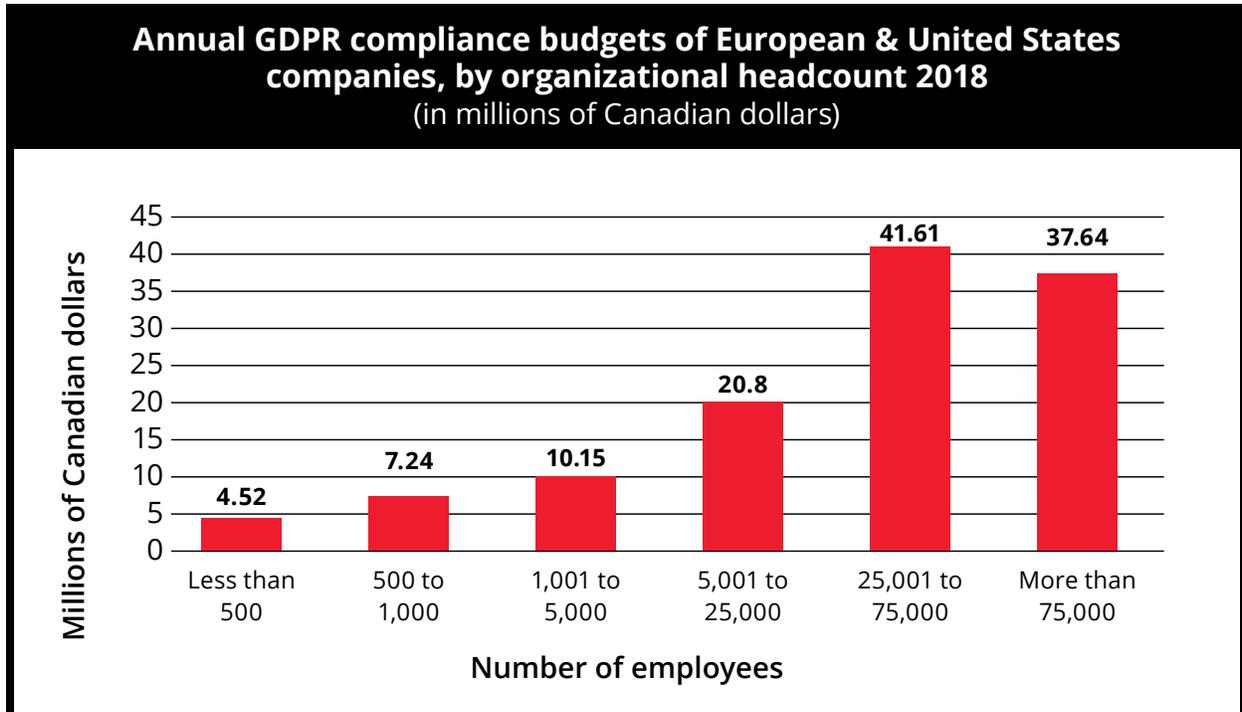
<sup>23</sup> The Costs of an Unnecessarily Stringent Federal Data Privacy Law, ITIF, 2019. Population estimate of 31,010,000 excludes 0-17-year-olds. US\$483 was converted to C\$619.05, based on an exchange rate of US\$1 = C\$1.28, by Xe on December 10, 2021.

<sup>24</sup> GDPR is here – And your Canadian business is likely impacted, National Public Relations, 2018.

<sup>25</sup> €525,000 Fine Under the GDPR: A Strong Signal for Businesses with No Establishment in Europe, Fasken, 2021. Converted to Canadian dollars from euros, based on an exchange rate of €1 = C\$1.45, by Xe on December 10, 2021.

<sup>26</sup> Ninety-two percent of European businesses are unprepared for GDPR, RSM, 2017.

<sup>27</sup> The GDPR Racket: Who's Making Money From This \$9bn Business Shakedown, Forbes, 2018.



- The following chart displays companies' annual GDPR compliance budgets in the United States and the EU by organizational headcount in 2018. Companies with 25,001 to 75,000 employees report having the highest budgets, at approximately C\$41.6 million.<sup>28</sup> The respondents were from privacy, data protection, compliance, legal, IT, and IT security offices of companies with a presence in the EU.
- Half of German businesses surveyed by Bitkom, Germany's digital association, believe that Germany is overdoing it with its current level of data protection. Two-thirds (66%) of these businesses believe that the current implementation of data protection laws makes digitization more difficult due to inconsistent interpretation of the regulation.<sup>29</sup>

<sup>28</sup> *The Race to GDPR: A Study of Companies in the United States & Europe*, IAPP, 2018. Study independently conducted by Ponemon Institute LLC and sponsored by McDermott Will & Emery LLP. Converted to Canadian dollars from US dollars, based on an exchange rate of US\$1 = C\$1.25 by Xe on January 14, 2022.

<sup>29</sup> *Datenschutz setzt Unternehmen unter Dauerdruck*, Bitkom, 2021. These results are based on a survey of 502 companies with 20 or more employees in Germany on behalf of the Bitkom digital association.

- Innovation is being impacted in Germany due to the GDPR. Three-quarters of businesses believe that innovative projects have failed due to requirements set out by the GDPR. A shocking nine out of 10 (86%) companies have stopped projects due to ambiguities with the GDPR.<sup>30</sup>
- German businesses indicated their main difficulties with GDPR compliance during the COVID-19 pandemic. Table 1 outlines those key issues.<sup>31</sup>

Three-quarters (76%) of businesses in Germany reported that at least one project related to innovation has failed due to the requirements of the GDPR.<sup>32</sup>

Table 1

<b>Top compliance issues in Germany during the COVID-19 pandemic that prevented full GDPR implementation</b>	
<b>Internal reasons</b>	<b>External reasons</b>
<ul style="list-style-type: none"> <li>• Other priorities due to COVID-19 taking precedence (82%)</li> <li>• Lack of human resources (61%)</li> <li>• Lack of financial resources (27%)</li> <li>• We cannot only focus solely on data protection (23%)</li> <li>• Lack of know-how (20%)</li> <li>• The necessary system changes take time (14%)</li> </ul>	<ul style="list-style-type: none"> <li>• Not possible to completely implement the GDPR (77%)</li> <li>• Continuous adjustment due to new judgements and recommendations of the supervisory authority (47%)</li> <li>• Data transfers to countries outside the EU must be re-examined (45%)</li> </ul>

<sup>30</sup> *Ibid.*

<sup>31</sup> Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers, Bitkom, 2021. Results gathered from companies with more than 20 employees in Germany, n=389.

<sup>32</sup> Datenschutz setzt Unternehmen unter Dauerdruck, Bitkom, 2021. Results gathered from companies with more than 20 employees in Germany, n=502.

### 3. Disproportionately impacting small and medium-sized enterprises

Small and medium-sized enterprises (SMEs) have been the hardest hit, experiencing challenges in interpreting and understanding the law's complexity, despite significant investments in GDPR compliance. With their survival heavily reliant on consumer data, it is critical that SMEs are given the tools and means to fully integrate privacy knowledge and practices, rather than engaging in box-checking exercises.

The compliance costs outlined in the previous section disproportionately impact small and medium-sized enterprises (SMEs). Research shows that small businesses in Europe are struggling to implement the GDPR despite their best efforts.

In 2019, GDPR.EU surveyed<sup>33</sup> 716 small business leaders in Spain, the United Kingdom, France and Ireland to understand how their businesses were coping with the new requirements. The survey found that there was widespread eagerness to comply with the GDPR among those surveyed, and that these small businesses had spent tens of thousands of dollars on consultants and IT solutions. It also showed that despite these efforts, the SMEs still uncovered challenges in understanding and interpreting the law's complexity.

#### Additional details

- More than 50% of EU small businesses surveyed in 2019 had spent the equivalent of between C\$1,450 and C\$72,500 on GDPR compliance.<sup>34</sup> According to the survey, "the most common expense was for employee training and consultants, followed by software and equipment. Yet 67% said these expenses were unlikely to affect the growth of their companies."

<sup>33</sup> *GDPR Small Business Survey*, GDPR.EU, 2019. France; Ireland; Spain; United Kingdom; January 17 to April 18, 2019; 716 respondents; 18 years and older; Spain (n=250); UK (n=242); France (n=134); Ireland (n=90).

<sup>34</sup> *GDPR Small Business Survey*, GDPR.EU, 2019, p.5. France; Ireland; Spain; United Kingdom; January 17 to April 18, 2019; 716 respondents; 18 years and older; Spain (n=250); UK (n=242); France (n=134); Ireland (n=90). Currency converted based on an exchange rate of €1 = C\$1.45 by Xe on December 10, 2021. Original figure was €1,000 - €50,000.

- Research shows that SMEs are slower to adapt to the GDPR compared to larger companies. The key issue for SMEs is that they lack data protection knowledge and need more support from authorities.<sup>35</sup> It is critical that SMEs are given the tools and means to fully integrate privacy knowledge and practices, rather than engaging in box-checking exercises.
- The GDPR has had unintended impacts on competition in the digital economy. Since the implementation of the GDPR, large online companies with significant resources to dedicate to privacy compliance, and the ability to create new and differentiating privacy solutions, have increased their already dominant market share in the EU, to the detriment of smaller players.<sup>36</sup>
- In the online advertising world, businesses have opted to advertise or partner with larger technology firms as they have the means to fulfil the regulatory requirements of the GDPR more effectively.<sup>37</sup> A week after GDPR implementation, a study found that market concentration increased by 17% with websites deciding to no longer work with smaller vendors. In general, smaller online vendors face additional hurdles due to their reliance on data from various sources.<sup>38</sup>
- With the introduction of the GDPR's right to deletion, there has been an emergence of services that automate consumer requests for organizations to delete their information, without consideration for whether there is a valid consumer concern in each case, and to the detriment of legitimate business and social needs to retain information. This is particularly unfortunate for SMEs that may face undue requests for data deletion when access to data is critical for their continued growth.

**A week after GDPR implementation, market concentration increased by 17%, with websites deciding to seek out large web technology providers over smaller vendors.**

From Regulatory Studies Centre (The George Washington University).

<sup>35</sup> GDPR still a mystery to SMEs: the risks of non-compliance, Hiscox, 2019.

<sup>36</sup> Six months in, Europe's privacy revolution favors Google, Facebook, POLITICO, 2018.

<sup>37</sup> *Ibid.*

<sup>38</sup> Two Years Later: A look at the Unintended Consequences of GDPR, Regulatory Studies Centre, The George Washington University, 2020.

- The GDPR has strongly affected business models and investor confidence, resulting in entrepreneurial discouragement and the abandonment of products. It has also had an impact on the start-up ecosystem. The Data Catalyst Institute (DCI) discovered a 26.1% drop in the number of EU venture deals following GDPR implementation. Their analysis found that the decline was due to the chilling impact on newer ventures and ventures that were more reliant on personal data.<sup>39</sup> Additionally, the average amount of money that companies raised from foreign investors within the same timeframe (May 2018 to April 2019) dropped by 33.8%, while domestic investments continued at the same rate of financing.<sup>40</sup>



<sup>39</sup> The One-Year Impact of the General Data Protection Regulation (GDPR) on European Ventures, The Data Catalyst Institute (DCI), 2020.

<sup>40</sup> Two Years Later: A look at the Unintended Consequences of GDPR, Regulatory Studies Centre, The George Washington University, 2020.

## 4. Creating complexity for consumers

In addition to a reduction in the availability of goods and services available to them, EU consumers are suffering from increased “consent fatigue”, being less likely to carefully review notices and make informed decisions. They also face a slow and overly complex complaint resolution process.

The introduction of the GDPR has indirectly reduced the availability of goods and services for EU consumers. As noted above, some global companies have adjusted their operations and denied service to EU citizens, rather than make the substantial investments required to comply with the GDPR.

An additional impact—one that is just beginning to take shape in the online world—is that if consumers provide less personal information, companies are considering whether to introduce new charges or increase current prices to offset lost revenues. Many of the online services and content consumers have come to rely on are paid for, at least to some extent, by online advertising fueled by data collection techniques. According to Vox, a completely ad free internet would cost users C\$44 per month.<sup>41</sup>

Besides these knock-on effects, consumers have been directly impacted by a slow and overly complex complaint resolution process, particularly as it relates to privacy complaints involving large multinationals. Although the GDPR has mechanisms for coordination and consistency in the application of the law that should support the resolution of cross-border investigations (among other things), the majority of DPAs are experiencing substantial issues in applying the promised “one-stop-shop” mechanism, resulting in massive delays in the enforcement of cross-border cases.<sup>42</sup>

Consumers continue to suffer from “consent fatigue”. Years before the GDPR, a study showed that it would take the average person roughly 244 hours per year, or about 40 minutes per day, to read through all of the privacy policies that applied to them, costing C\$463 billion in lost leisure and

**Some global companies have stopped servicing individuals located in the EU rather than making substantial investments to comply with the GDPR.**

<sup>41</sup> [The cost of an ad-free internet: \\$35 more per month](#), Vox, 2019. Converted using Xe, based on an exchange rate of US\$1 = C\$1.27, on February 2, 2022.

<sup>42</sup> [Three Years Under the EU GDPR](#), Access Now, 2021.

productivity time and amounting to a national opportunity cost of C\$991 billion.<sup>43</sup> It is no surprise, then, that most consumers do not read privacy notices provided by websites.<sup>44</sup>

With the introduction of the GDPR, notices to consumers have become even more frequent and complex. The GDPR's stringent consent and transparency requirements have resulted in consumers being less likely to carefully review notices and make informed decisions.

Despite the legal requirements for explicit, informed consent, intended to increase consumer understanding, research shows that many consumers may not know what they are consenting to. Researchers have discovered that: "...the more information individuals have access to about what happens to their (personal) data, the less information they are able to filter, process, and weigh to make decisions that are in line with their own privacy preferences."<sup>45</sup> It may also deter them from using a certain website or service altogether.<sup>46</sup>

**With too much information, consumers are less likely to absorb notices and make decisions in line with their preferences.**

From an analysis in the *Brooklyn Law Review*.

### **Additional details**

- Only 40% of consumers recognize companies' efforts to be more transparent with their data use policies since the implementation of the GDPR.<sup>47</sup> In fact, consumers seem to be experiencing increased consent fatigue and confusion, unable to focus their attention on what matters most.<sup>48</sup>

<sup>43</sup> ["Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation](#), *Brooklyn Law Review*, 2019. Numerical figures converted using Xe, based on an exchange rate of US\$1 = C\$1.27, on February 2, 2022.

<sup>44</sup> ["Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation](#), *Brooklyn Law Review*, 2019.

<sup>45</sup> [Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective](#), *Journal of Consumer Policy*, 2018, p.95.

<sup>46</sup> ["Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation](#), *Brooklyn Law Review*, 2019.

<sup>47</sup> [GDPR One Year On](#), Ipsos, 2019.

<sup>48</sup> [Most EU cookie 'consent' notices are meaningless or manipulative, study finds](#), TechCrunch, 2019.

- Despite a requirement for transparency around cookies that was intended to improve consumer understanding, research shows that consumers have not gained much clarity around why and how companies use cookies to provide them with a more personalized and intuitive web and advertising experience. They experience some confusion as to how cookies function, and they do not know why they don't trust the term *cookie*.<sup>49</sup>
- Researchers from Germany and Copenhagen discovered that consumers in Germany are annoyed with cookie notices. By comparing the results of two studies—done in December 2017 and December 2018—they were able to determine whether there were significant differences in attitudes towards cookies once the GDPR was introduced. The research showed that GDPR has not improved consumers' attitudes towards cookies. Researchers found that: "a large number of the participants claimed to be annoyed by the cookie disclaimer, as they considered it a disturbance in their surfing." One survey respondent summed it up (in the 2017 survey but still typical of the 2018 results) as follows: "As these messages appear constantly, I find them to be disruptive and annoying."<sup>50</sup>
- Axel Voss, a Member of the EU Parliament (MEP) involved in the original drafting of the GDPR, launched a public consultation in 2021 on how the GDPR has impacted the daily lives of individuals and organizations. He received more than 180 replies detailing the negative impact of the GDPR on everyday life. What surprised him was that two-thirds of the responses came not from business but from "citizens, researchers, scientists, nurses, data protection officers, lawyers, non-profit associations, sport clubs and many more." In contrast, only one-third came from businesses and business associations.<sup>51</sup>
- Despite the GDPR having several legal grounds for processing, an overreliance on express consent remains. "Giving the user the illusion of control, the controller is thereby able to pass the responsibility on to the user in complex and page-long data protection declarations. Being on the edge after another privacy banner pops up, many users excessively consent to everything in order to finally get the service they were looking for, often without knowing what they actually agreed to."<sup>52</sup>

<sup>49</sup> *Ibid.*

<sup>50</sup> Has the GDPR hype affected users' reaction to cookie disclaimers?, Journal of Cybersecurity, Oxford University Press, 2020, p.3.

<sup>51</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.2.

<sup>52</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.7.

- Another survey indicates that the GDPR does not appear to have increased trust among consumers. Six months after the law came into effect, consumer confidence on the Internet was at the lowest it had been in a decade. Four out of five (81%) Europeans who give out their information online believe that they only had partial control or no control of the data.<sup>53</sup>

## **5. Triggering other inefficiencies and unintended consequences**

Pitfalls outlined in this section include:

- The GDPR does not effectively differentiate between issues of private sector and public sector privacy, and between low and high-risk applications and activities. This reduces regulatory efficiency.
- The GDPR was drafted with outdated assumptions about the nature of data processing and is overly complex, making it challenging for privacy lawyers, let alone the average organization, to interpret and apply correctly.
- Using a single human rights-focused approach to regulate all uses of personal information, by all parties, in all contexts, is flawed, and potentially detrimental to a number of other societal objectives.

The GDPR was intended to protect the rights of the individual by acting as a defence against data breaches, undue surveillance, and malicious misuses of personal information—a worthwhile objective. Unfortunately, the broad scope and level of prescriptiveness of the GDPR framework has resulted in fundamental flaws that lead to inefficiencies, unintended consequences, or both.

Key concerns identified by MEP Axel Voss in his in-depth examination of the GDPR in May 2021 include:

---

<sup>53</sup> [What the Evidence Shows About the Impact of the GDPR After One Year](#), Centre for Data Innovation, 2019.

## A. Lack of proportionality

The GDPR aims to be a one-size-fits-all solution to privacy issues across the private **and** public sectors. It does not effectively differentiate between the processing of personal information by governments and by private individuals and organizations.<sup>54</sup>

MEP Voss notes that the GDPR **lacks a risk-based approach and fails to account for context**, and the varying scope and scale of data processing activities by organizations. Although this concept is alluded to in the GDPR, it is not consistently executed in the legal text. As MEP Voss points out, “the GDPR does not differentiate enough between low-risk and high-risk applications, determining—with a few exceptions such as prior consultation of the DPA for high-risk applications—largely the same obligations for each type of data processing.”<sup>55</sup>

Furthermore, there is an unwillingness among European regulators to designate low-risk classes of data processing with separate bases for processing, which would reduce compliance burdens for organizations and regulators alike.<sup>56</sup>



<sup>54</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021.

<sup>55</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.4.

<sup>56</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021.

## **B. Complexity and rigidity**

Privacy law should be built on solid principles that provide flexibility for specific applications so that organizations and regulators can adapt to address changing technologies and circumstances. Any privacy framework must also be understandable and achievable for non-specialists.

In contrast, at 88 pages, the GDPR is overly complex, making it challenging for privacy lawyers, let alone the average organization, to interpret and apply correctly.

The GDPR was drafted with outdated assumptions about the nature of data processing. For example, it is based on the notion that data is generally processed at a specific location at a specific time. This is an outdated and unworkable conception in an age of clouds and blockchain technology, where data is constantly in flux, moving across global networks.

According to MEP Voss, the GDPR, like its predecessor legislation from the 1980s, “is based on the processing of individual data (thus ignoring Big Data), as well as on the processing by a single controller, thereby, ignoring cloud computing, the Internet of Things, platforms or other complex actors.”<sup>57</sup>

## **C. Disproportionate use of a human rights framework**

MEP Voss stresses that the GDPR fails to adequately recognize that data protection needs to be: “...balanced with other fundamental rights or interest such as the right to life, to liberty and security, the freedom to conduct a business or the freedom of the press.”<sup>58</sup>

At the core of the GDPR framework is the assumption that, regardless of the context or potential outcome, any collection, use or disclosure of personal information erodes an individual’s right to privacy; personal information may only be processed where one of the legal grounds recognized by the law exists. This fundamental conception of data use as an incursion on a human right is flawed, and potentially detrimental to a number of other societal objectives.

While it is clear in our digital world that some uses of personal data may be cause for concern, it is equally clear that many other uses of data can be extremely beneficial to both individuals and to society large, such as helping to address public health concerns and climate change. The COVID-19 pandemic (which saw corporate data reserves deployed

---

<sup>57</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.4.

<sup>58</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.5.

for the common good through contact tracing and the like) is just one example of the processing of personal data for a socially beneficial purpose. Indeed, the ability to collect, assemble and analyze appropriately protected personal information is critical to the economic and social fabric of modern economies.

Privacy laws were initially conceived to protect the rights of individuals against the state. Given the near absolute power of the state over the lives of individuals and the severity of the potential consequences to individuals that can result from abuse of that power, it makes sense for democratic societies to enact laws to protect individuals against the unjustified use of personal information by government institutions, and to view privacy-invasive interactions with the state as implicating fundamental human rights. The nature of the relationships between an individual and the state, and between an individual and a private business, are fundamentally different, as are the potential consequences to an individual flowing from these relationships.

These different contexts demand different legislative and regulatory approaches—whereas the GDPR applies equally to public and private sector organizations. In the case of state surveillance and other privacy-intrusive activity by the state, privacy should be regulated through a human rights lens. However, the nature of the relationship between an individual and a commercial organization, and the potential consequences to an individual stemming from mishandling of personal information by a business is fundamentally different, and therefore requires a different legislative approach and lens.

Indeed, modern economies are predicated on the exchange of personal information. Where individuals provide personal information to an organization in connection with the purchase of goods or services, it is reasonable to expect the organization to use the information to serve their customers better, and to use it for everyday business activities, such as managing inventory, identifying areas of expansion, improving products and services, fundraising (in the case of charities), and targeted advertising.

Using a single human rights-focused approach to regulate all uses of personal information, by all parties, in all contexts, would be akin to equating egregious privacy infringement—and real threats to human rights—with a myriad of legitimate and beneficial commercial activities, as well as with many inconsequential uses of data.

**“The GDPR fails to clarify that data protection is not an absolute fundamental right, but should... be balanced with other fundamental rights or interest such as the right to life, to liberty and security, the freedom to conduct a business or the freedom of the press.”**

Axel Voss, Member of the EU Parliament involved in the original drafting of the GDPR.

## 6. Suppressing emerging technologies

The GDPR continues to have a chilling impact on the growth of emerging technologies, with many EU companies choosing to innovate less with personal data or pursue their ideas in less restrictive jurisdictions. Although the GDPR is meant to be technology-neutral, the law and its concepts are incompatible with many new technological developments, including artificial intelligence and automated decision-making.

Although the GDPR is meant to be technology-neutral, the law and its concepts are incompatible with many new technological developments. The GDPR continues to have a chilling impact on the growth of emerging technologies, with many EU companies choosing to innovate less with personal data or pursue their ideas in less restrictive jurisdictions. According to the DDV, the GDPR hinders the emergence of innovative technologies, and there is no evidence of positive economic growth or increased competitiveness of the EU economy since the implementation of the GDPR.<sup>59</sup>

MEP Voss stresses that GDPR requirements are incompatible with several vital technologies and processes. This includes “principles of data minimisation as well as the purpose and storage limitation (in Article 5), the GDPR’s focus on the processing of individual data by a single controller (in Article 4) or the restrictions of the secondary use of data are no longer problem adequate.” MEP Voss finds that these concepts “in fact prevent emerging technologies from exploiting their full potential.”<sup>60</sup>

**GDPR requirements are incompatible with several vital technologies and processes.**

From *Fixing the GDPR: Towards Version 2.0*, Axel Voss.

### A. Artificial intelligence

Research indicates that AI has the transformative potential to improve social outcomes, along with the potential to double annual economic growth rates in developed countries over the next 15 years. Consumers are demanding much greater speed and quality of information in order to use services provided by companies, and to make informed purchase decisions. AI is critical to delivering on that promise.

<sup>59</sup> POSITION PAPER: GDPR-Evaluation 2020: DDV calls for the removal of obstacles to innovation and bureaucracy, DDV, 2020.

<sup>60</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.9.

User data-driven systems, including recommendation engines, customer service chatbots and marketing geared towards consumer preferences, are important and beneficial tools and services for consumers, and for organizations looking to better serve them.

The GDPR's provisions are generally ill-suited to the reality of AI; its requirements around "explainability" (i.e., to explain an organization's use of AI to consumers), purpose limitation, data minimization and restrictions on secondary use can be seen as the major obstacles for the technology.

The GDPR's requirement for organizations to explain how an AI system makes decisions (that have significant impacts on them) needs some realistic parameters as it penalizes beneficial AI processes that may be difficult to explain. The fact is that many AI systems are not easily explained, and the goal should be transparency with respect to the range of factors taken into account, rather than transparency with respect to the precise calculation giving rise to a particular decision.

Purpose limitation demands that researchers and companies obtain each individual's consent before utilizing their data for a new purpose. This obstacle makes maintaining consent more challenging and restricts organizations from experimenting with their algorithms, even when there is no negative impact on the consumer. The fact that the training of algorithms is not clearly recognized as a scientific or statistical purpose is problematic and limiting.<sup>61</sup> MEP Voss points out that in Europe, as a consequence of the GDPR, it is difficult to obtain sufficient levels of personal data to train algorithms with beneficial purposes, such as to help with medical diagnoses or drug development.<sup>62</sup>

Although the GDPR includes certain exceptions for data processing for the purpose of scientific or statistical research, there's no clear definition of scientific research and it's unclear when AI development can fit within it, or whether these exceptions are available to private companies.

Finally, the GDPR's data minimization requirements mean engineers must determine what data and what quantity is necessary for a project. Sometimes, this can be a challenge. It's not always possible to predict how and what a model will learn from data.

---

<sup>61</sup> *Ibid.*

<sup>62</sup> *Ibid.*

## B. Automated decision-making

As outlined by Axel Voss, there is: "...a lack of distinction between automated processing, including profiling, which is expected by individuals and which contributes to more effective services to individuals and more relevant content, and profiling which creates harm, such as political manipulation, or a commercial lock up effect for which specific safeguards should be put in place."<sup>63</sup> With the more serious cases being addressed under the Digital Services Act, legislative overlap with existing GDPR provisions should be avoided.

Automated decision-making includes a broad range of routine, micro decisions, the majority of which will have no significant impact on an individual or potential to harm them (such as a call centre using automated decisions to support call routing, or a website declining to serve copyright-protected content to a user resident in a jurisdiction for which the website provider does not hold the rights to make that content available).

Restrictions on the use of automated decision systems should only be in relation to those that could have a significant impact on an individual, permitting individuals to engage if they feel they have been harmed.

## 7. Obstructing cross-border business

Although the GDPR theoretically has several mechanisms to permit international data flows in and out of the EU, only three are effectively used. As a result, international data flows are under threat, which risks separating the European Union from the rest of the world. There is some question as to whether the EU's complicated adequacy scheme provides meaningful additional privacy protection above the standard in other jurisdictions.

The GDPR adequacy scheme for international data flows has had a chilling impact on cross-border business. For years, cross-border data flows have generated more economic value than the traditional flows of traded goods.<sup>64</sup> The marginal costs of digital communications are so low (nearly zero) that the possibilities for firms conducting businesses on a global scale opens them up to endless opportunities.<sup>65</sup> Moreover, keeping

<sup>63</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.11.

<sup>64</sup> Digital Globalization: The New Era Of Global Flows, McKinsey & Company, 2016.

<sup>65</sup> *Ibid.*

duplicate copies of data on two or more storage systems, in multiple countries, is an effective tool to ensure business continuity in the case of data corruption, server failure and other incidents of data loss.

Although the GDPR theoretically has several mechanisms to permit international data flows in and out of the EU, only three are effectively used.<sup>66</sup> As a result, according to MEP Voss, “international data flows are currently under threat, which risks isolating the European Union from the rest of the world.”<sup>67</sup>

Although some EU companies have tried to restrict their data flows outside the EU, the global nature of their businesses, customer bases and data traffic is oriented in such a way that data still passes through other countries or is saved in international cloud services. Understanding and monitoring these processes is highly complicated and expensive, especially for SMEs.<sup>68</sup>

There is some question as to whether the EU’s complicated adequacy scheme provides meaningful additional privacy protection above the standard in other jurisdictions, and through the use of contractual commitments. For example, the third-party transfer requirements in Canada’s PIPEDA are founded on the accountability of the primary organization, and include providing notice and using contractual or other means to provide a comparable level of privacy protection when data is transferred. These requirements collectively are considered by many to be sufficiently strong in the context of transfers for processing.

The vast majority (94%) of firms that transfer data from the EU to a third country (outside the EU) end up relying on standard contractual clauses as the primary legal means for data transfer, rather than relying on the adequacy status of the recipient firm or destination country, suggesting that the time and resource-consuming adequacy framework results in little practical benefit.

**94% of firms that transfer data out of the EU rely on standard contractual clauses, suggesting that the GDPR’s intensive adequacy framework provides little practical benefit.**

The figure of 94% is taken from an IAPP-EY Report.

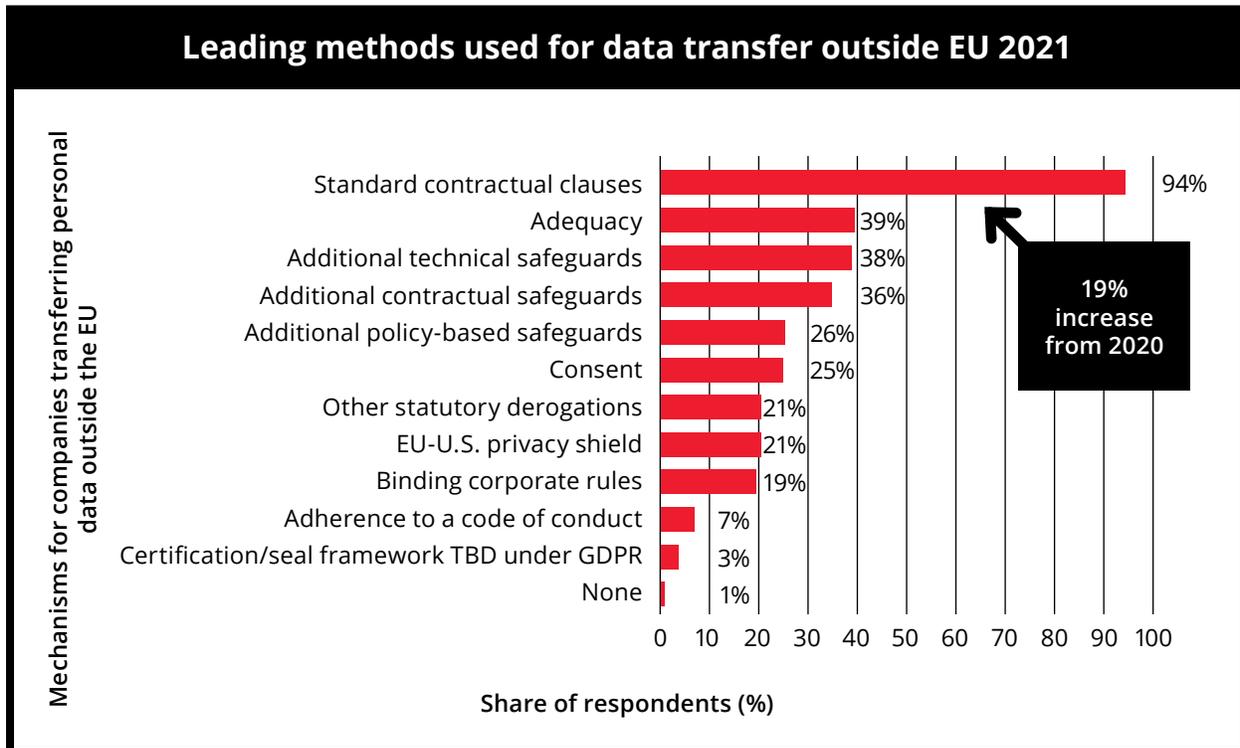
<sup>66</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021.

<sup>67</sup> Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021, p.8.

<sup>68</sup> IAPP-EY Annual Privacy Governance Report 2021, IAPP, 2021.

## Detailed findings

- The following chart provides a snapshot of other leading mechanisms for the transfer of personal data out of the EU in 2021:<sup>69</sup>



The survey results show that businesses that transfer data out of the EU have continued to rely on or switched to using standard contractual clauses, which the European Commission updated in June 2021.<sup>70</sup> However, 10% of these firms have made significant changes to their data transfer policies. This includes localizing data or stopping their data transfers because of the CJEU’s “Schrems II” decision.<sup>71</sup>

<sup>69</sup> IAPP-EY Annual Privacy Governance Report 2021, IAPP, 2021, p.4.

<sup>70</sup> IAPP-EY Annual Privacy Governance Report 2021, IAPP, 2021.

<sup>71</sup> *Ibid.*

## Conclusion

The GDPR's pitfalls, outlined in this paper, have led to some significant unintended negative consequences for governments, consumers and organizations. As the Canadian government looks to reform its own private sector privacy law, there is much to learn from this cautionary tale.

A made-in-Canada approach to privacy reform—one that balances effective privacy protection with the enormous social and economic benefits of data to Canadians—will enable Canada to reclaim its reputation as a global leader in protecting citizens' privacy while fostering innovation by business.



## Sources

Sources are listed here in the order in which they appear in the report.

- [The State of Small and Medium Businesses in 2021](#), Phase 5, 2021.
- Marvin Cruz, Keyli Kosiorek, Laura Jones, and Taylor Matchett, [Canada's Red Tape Report – Sixth Edition: The Cost of Regulation to Small Business](#), Canadian Federation of Independent Business (CFIB), 2021.
- Stephanie Bodoni, [Europe's Data Law Is Broken, Departing Privacy Chief Warns](#), Bloomberg, 2021.
- [Data: A new direction](#), Department for Digital, Culture, Media & Sport, GOV.UK, 2021.
- [POSITION PAPER: GDPR-Evaluation 2020: DDV calls for the removal of obstacles to innovation and bureaucracy](#), Deutscher Dialogmarketing Verband (DDV), 2020.
- [Contribution of the EDPB to the evaluation of the GDPR under Article 97](#), European Data Protection Board (EDPB), 2020.
- Johnny Ryan and Alan Toner, [Europe's governments are failing the GDPR](#), Brave, 2020.
- Estelle Massé, [Two Years Under the EU GDPR](#), Access Now, 2020.
- [ICO warns on over-reporting of data breaches](#), Pinsent Masons, 2018.
- Catherine Stupp, [European Privacy Regulators Find Their Workload Expands Along With Authority](#), The Wall Street Journal, 2019.
- Müge Fazlioglu, [IAPP-EY Annual Privacy Governance Report 2021](#), The International Association of Privacy Professionals (IAPP), 2021.
- [The Cost of Continuous Compliance](#), DataGrail, 2020.
- Alan McQuinn and Daniel Castro, [The Costs of an Unnecessarily Stringent Federal Data Privacy Law](#), Information Technology and Innovation Foundation (ITIF), 2019.
- Diana McLachlan, [GDPR is here – And your Canadian business is likely impacted](#), National Public Relations, 2018.
- [€525,000 Fine Under the GDPR: A Strong Signal for Businesses with No Establishment in Europe](#), Fasken, 2021.
- [Ninety-two percent of European businesses are unprepared for GDPR](#), RSM, 2017.
- Oliver Smith, [The GDPR Racket: Who's Making Money From This \\$9bn Business Shakedown](#), Forbes, 2018.
- [The Race to GDPR: A Study of Companies in the United States & Europe](#), IAPP,

2018. Study independently conducted by Ponemon Institute LLC and sponsored by McDermott Will & Emery LLP.

- [Datenschutz setzt Unternehmen unter Dauerdruck](#), Bitkom, 2021.
- Susanne Dehmel, [Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers](#), Bitkom, 2021.
- [GDPR Small Business Survey](#), GDPR.EU, 2019.
- [GDPR still a mystery to SMEs: the risks of non-compliance](#), Hiscox, 2019.
- Mark Scott, Laurens Cerulus, Laura Kayali, [Six months in, Europe's privacy revolution favors Google, Facebook](#), POLITICO, 2018.
- Aryamala Prasad, [Two Years Later: A look at the Unintended Consequences of GDPR](#), Regulatory Studies Centre, The George Washington University, 2020.
- Jian Jia and Liad Wagman, [The One-Year Impact of the General Data Protection Regulation \(GDPR\) on European Ventures](#), The Data Catalyst Institute (DCI), 2020.
- Rani Molla, [The cost of an ad-free internet: \\$35 more per month](#), Vox, 2019.
- Estelle Massé, [Three Years Under the EU GDPR](#), Access Now, 2021.
- Katherine M. Wilcox, ["Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation](#), Brooklyn Law Review, 2019.
- [Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective](#), Journal of Consumer Policy, 2018.
- [GDPR One Year On](#), Ipsos, 2019.
- Natasha Lomas, [Most EU cookie 'consent' notices are meaningless or manipulative, study finds](#), TechCrunch, 2019.
- Oksana Kulyk, Nina Gerber, Annika Hilt, Melanie Volkamer, [Has the GDPR hype affected users' reaction to cookie disclaimers?](#), Journal of Cybersecurity, Oxford University Press, 2020.
- Axel Voss, [Fixing the GDPR: Towards Version 2.0](#), Axel Voss, 2021.
- Eline Chivot and Daniel Castro, [What the Evidence Shows About the Impact of the GDPR After One Year](#), Centre for Data Innovation, 2019.
- James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, Dhruv Dhingra, [Digital Globalization: The New Era Of Global Flows](#), McKinsey & Company, 2016.

## About the Canadian Marketing Association

---

The CMA's purpose is to embolden Canadian marketers to make a powerful impact on business in Canada. We provide opportunities for our members from coast to coast to develop professionally, to contribute to marketing thought leadership, to build strong networks, and to strengthen the regulatory climate for business success. Our Chartered Marketer (CM) designation signifies that recipients are highly qualified and up to date with best practices, as reflected in the Canadian Marketing Code of Ethics and Standards. We represent virtually all of Canada's major business sectors, and all marketing disciplines, channels and technologies. Our Consumer Centre helps Canadians better understand their rights and obligations.

[thecma.ca](http://thecma.ca)

A French synopsis of this document is available on our website or by request.  
E-mail: [advocacy@thecma.ca](mailto:advocacy@thecma.ca)