

Since 2018, data protection laws have reduced security breaches but affected firms' value

July 17 2024



Credit: CC0 Public Domain

The introduction of new data protection rules significantly reduced breaches by firms but negatively impacted their market value, according to new research by the University of East Anglia (UEA) and University of Texas.

Researchers looked at what happened when the European Union's General Data Protection Regulation (GDPR) started to be enforced in 2018. Using its extraterritorial reach, the authors explore variation in US firms' exposure to the EU GDPR to see how stricter data privacy laws affected their value, investment choices and data breaches.

They found companies that had to comply with GDPR saw their market value drop by 0.6-1.1%—or from \$42 to \$76 billion in total—in the week it became enforceable. This was partly related to stricter data privacy and security laws slowing firms' sales growth.

However, these companies invested more money in [data protection](#) than those not affected by GDPR and were less likely to experience data breaches. This reduction was significant, preventing up to 34 million records from being leaked each year, which would have cost firms between \$205 million and \$561 million annually to deal with.

The findings are published in the *Journal of Business Finance and Accounting*. Co-author Dr. Fabio Motoki, Lecturer in Accounting at UEA's Norwich Business School, said, "Overall, this study shows key costs and benefits of stricter data privacy laws, providing useful information for businesses and regulators around the world.

"These results suggest that the GDPR may have achieved one of its intended goals of enhancing consumer data protection and privacy. This is thought to be the first study to document the potential benefits associated with recent efforts to regulate these areas.

"Specifically, we find that US firms subject to the GDPR are less likely to report a data breach after enforcement of the regulation. The decrease in data breach likelihood appears to be driven by a reduction in [data breaches](#) associated with hacking and malware, which might be attributed to greater investment in cybersecurity. This greater investment

could be due to the increased attention of a more specialized board to oversee cybersecurity risks in US firms due to the GDPR."

The EU approved the GDPR to address growing concerns around data privacy and security. It came into force on May 25, 2018, and requires [greater transparency](#) in how firms collect consumer data by establishing clear opt-in consent for collection, imposing stricter data management and control, and assigning substantial penalties and liability risks for data processing or data flow violations. As a result, the regulation was thought likely to impose high compliance costs on firms.

The GDPR requires any enterprise that controls or processes EU residents' data to abide by the rules, regardless of its location. Therefore, firms across the world, including those in the US, might be subject to the GDPR if they process EU residents' personal data.

Many states in the US and other countries, such as Brazil, China, and Canada, have since either enacted or are also debating laws such as the GDPR, highlighting the importance of assessing the consequences of it outside the EU.

Dr. Motoki and co-author Jedson Pinto, Assistant Professor of Accounting at the University of Texas, analyzed how GDPR affected a sample of 1,013 US firms' stock prices around the week the rules came into force, comparing those companies exposed to them with those that were not.

The control group of firms not exposed to GDPR-associated risks operate in the [health care](#), banking or insurance industries, as they already work under stricter data protection laws. The industries most affected by GDPR were found to be in areas ranging from business services and utilities to pharmaceutical products and shipping containers.

The researchers say the drop in firm value is consistent with investors anticipating a substantial negative effect of stricter data privacy laws on firms' future cash flow.

They also find that firms exposed to the GDPR exhibit statistically slower sales growth than those not exposed to GDPR—those affected saw their sales grow 5.8-6.6 percentage points slower than control firms after the law came into effect.

The decrease in data breach likelihood represented 10 fewer breaches in a year. In 2023, the cost per record for a medium-sized breach (up to 101,200 records) was estimated to be approximately \$165 per record, with large breaches having lower per-record estimates but elevated total economic costs.

Dr. Pinto said, "Our findings add to the growing body of literature documenting the costs of GDPR, such as a decrease in EU venture capital investment, especially when ventures and lead investors are not in the same state or union.

"They indicate that GDPR may have changed how the market perceives these breaches, potentially changing executives' incentives to protect customer data. These results are consistent with regulations being an alternative way to address the recent concerns of data privacy and security and should be of interest to regulators worldwide that have enacted or are looking to enact laws similar to the EU GDPR."

Dr. Motoki and Dr. Pinto also examined whether the GDPR affected how investors reacted to the announcement of a data breach using information from 62 breaches in the sample period. They find that post-GDPR, investors may react more negatively to a data breach for firms with stricter data protection requirements.

The effect is economically significant, with a data breach being associated with up to a 5.3% drop in [stock prices](#) in the five days around the announcement of the breach compared to firms not under the regulations. They say these results are consistent with investors anticipating significant litigation costs associated with the fines in the case of a [breach](#).

More information: Regulating Data: Evidence from Corporate America, *Journal of Business Finance & Accounting* (2024). [DOI: 10.1111/jbfa.12820](#)

Provided by University of East Anglia

Citation: Since 2018, data protection laws have reduced security breaches but affected firms' value (2024, July 17) retrieved 18 July 2024 from <https://techxplore.com/news/2024-07-laws-breaches-affected-firms.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.