SPIRION

What are the Business Costs of Ignoring or Heeding GDPR?

GPDR Enforcement is “on Fire”: New Reporting on Penalties and Privacy Investments are Coming In

In the first year after the European Union’s General Data Protection Regulation (GDPR) launched, it seemed like it was not living up to its hype. Leading up to the launch in May 2018, pundits warned businesses about the regulations’ wider-reaching rules, stricter enforcement, and steeper fines. But one year later, non-compliance enforcement and penalties were low. However, today they are on fire.

What does the sudden uptick in GDPR enforcement and penalties mean for companies who are in compliance with the regulations versus those who are not in compliance? New reporting provides some valuable insights.

GDPR Had a Slow Start

One year after GDPR went into effect, the SD Times[1] reported that “The impact of the GDPR has been minimal to this point. Compliance has been slow, enforcement has been lax, and organizations are finding that learning about data origin, residence, and use can be hugely daunting and difficult.”

Fast-forward to today and everything has changed. In January 2020, DLA Piper reported that GDPR fines (not all related to data privacy) totaled 114 million Euros.[2]

€114M

in fines for violations of GDPR regulations, not just breaches

1 sdtimes.com/data/gdpr-one-year-later-slow-compliance-lax-enforcement
2 www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020

Higher Non-Compliance Penalties

Under GDPR, organizations that breach the rules can be fined up to 20 million Euros, or 4% of a company's annual global turnover, whichever is higher. For lesser infringements, the fines can be up to €10 million or 2%.

"Fines are determined based on a number of factors", according to Christian Wigand, a spokesman for the European Commission. Among them are how the company protected its data, how it reacted to a data breach, and whether it cooperated with the authorities.

3 Largest GDPR Fines by January 2020

Today there are both more GDPR-related non-compliance citations and increasingly higher penalties. The three largest penalties so far have grabbed the headlines.

$55M

In January 2019, an online advertising and tech company was fined for the improper disclosure to users on how their data is collected across its services, including its search engine, maps, and video channel, to use in personalized advertisements.

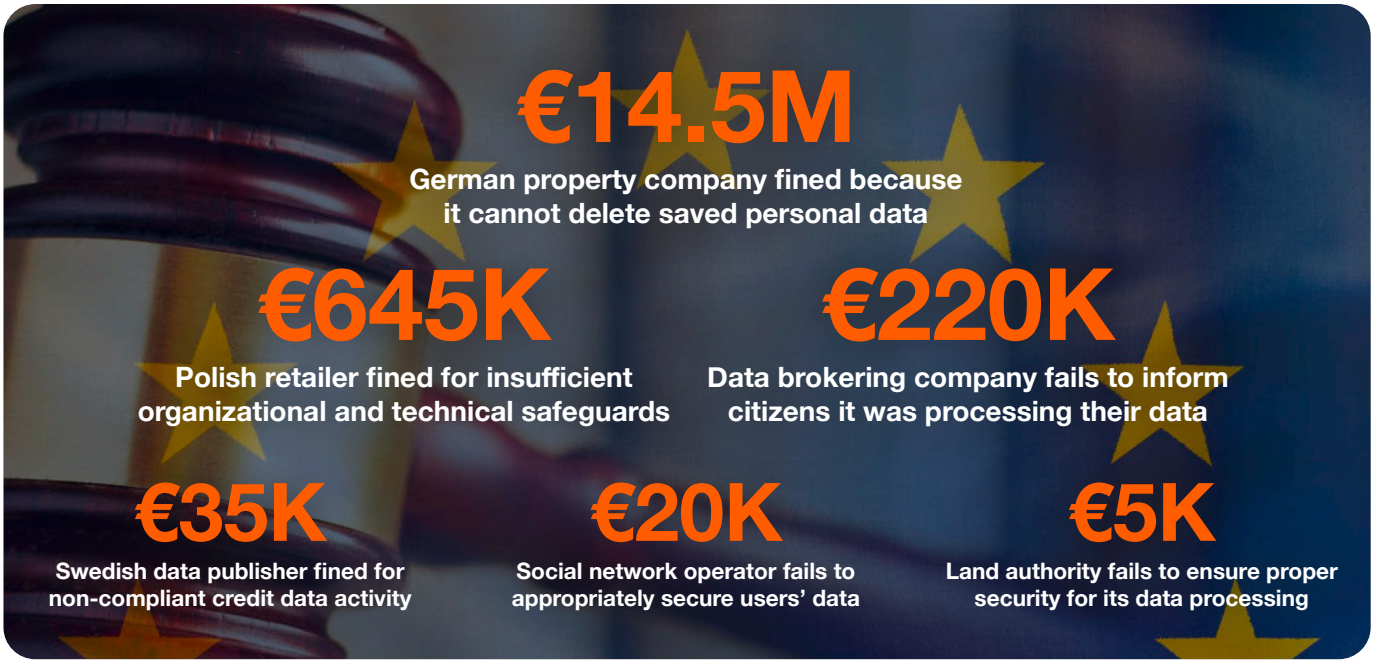
$123M

In July 2019, a hotel chain was fined for a breach that was thought to impact 500 million customers, including names, addresses, phone numbers, emails, payment card numbers, and passport numbers.

$230M

In August 2019, a UK-based airline faced a potential fine of $230 million over a data breach that was found to have exposed customers' bankcard numbers, expiry dates, and CVV codes.

But it's not just big-name companies feeling the pain of non-compliance with GDPR. There is also a growing range of GDPR fines costing companies' significant dollars for not meeting GDPR requirements.



Multiple Companies Fined Under GDPR

The European Commission[3] reported some of the many penalties levied for non-compliance with GDPR rules, covering a wide range of amounts:

- A data brokering company fined €220,000 for failing to inform citizens it was processing their data
- A social network operator fined €20,000 for failing to appropriately secure users' data
- A land authority fined €5,000 for failing to ensure the necessary security for its data processing

In January 2020, Nathan Trust[4] published an updated list of GDPR non-compliance fines impacting organizations around the world. These are just a few of the global non-compliance fines from the list:

- German property company fined €14.5 million because it cannot delete saved personal data
- Polish retailer fined €645,000 for insufficient organizational and technical safeguards
- Swedish data publisher fined €35,000 for non-compliant credit information activity

The compliance management company stated, "The various European Supervisory Authorities are increasingly active with more and more enforcement actions every week."

3 ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf
4 nathantrust.com/gdpr-fines-penalties

The Rewards of Complying with Regulatory Laws

With GDPR now on fire, and so many other compliance regulations to contend with, what is the true cost and return of investing in data security and privacy solutions? Over 2,800 security professionals say there are many significant rewards, according to the Cisco *Data Privacy Benchmark Study 2020, From Privacy to Profit: Achieving Positive Returns on Privacy Benefits*.[5]

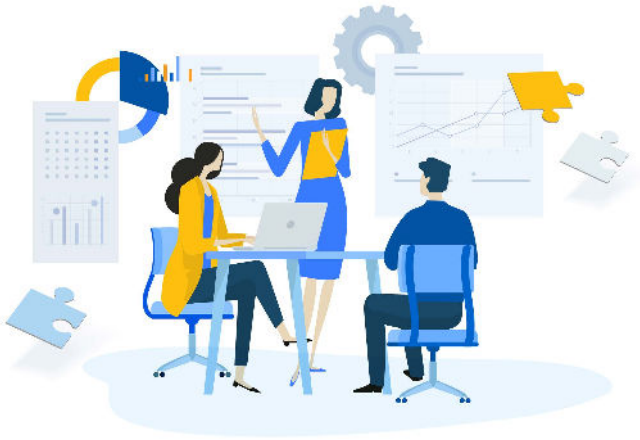
In this year's survey, Cisco quantified privacy spending and benefits to determine the ROI for privacy. Among the findings is that 70% of organizations are gaining "significant" or "very significant" business benefits from their efforts to maintain data privacy, including operational efficiency, agility, and innovation.

According to Cisco, "For some time, privacy regulation has been an important driver of companies' efforts to protect their personal data, and avoiding fines and penalties is certainly one motivator." The new report found that the benefits also impact the bottom line. "Most organizations are seeing very positive returns on their privacy investments, and more than 40% are seeing benefits at least twice that of their privacy spend."

Security professionals cited the following business impacts from privacy investments:

72%
achieve operational efficiency from data controls

74%
build customer trust and loyalty



73%
attract more investors

71%
enable agility and innovation

71%
mitigate losses from breaches

67%
reduce sales delays

5 cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf

Further, the study found strong correlations between organizations' privacy accountability and lower breach costs, shorter sales delays, and higher financial returns.

The average financial impact of these benefits is estimated at $2.7 million. The average ratio of benefits-to-spend was 2.7, meaning that for every dollar of investment the organizations received $2.70 worth of benefit. The breakdown of investment-versus-benefits for companies was:

- 47% are seeing a greater than a twofold return
- 33% are breaking even
- 8% appeared to spend more than they receive back

So, what is the bottom line on investing in GDPR compliance versus non-compliance? The answer could be summed up by an observation from the President of the Centre for Information Policy Leadership (CIPL), Bojana Bellamy: "It is a business imperative and competitive advantage for companies, their boards, and senior leaders to embrace accountability and transparency in how they manage personal data."

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion is the leader in data discovery, persistent classification, and protection of sensitive data on-premise and in the cloud. Since 2006, thousands of organizations worldwide to reduce their sensitive data footprint and proactively minimize the risks, costs and reputational damage of successful cyberattacks. Spirion provides greater command and control of sensitive data to leading firms across all industries from financial services to healthcare to the public sector. Visit us at **spirion.com**