2019

GDPR Small Business Survey

Insights from European small business leaders one year into the General Data Protection Regulation

A report by GDPR.EU

May 2019

Summary

On May 25, 2018, a new data protection regime entered into force in the European Union. The General Data Protection Regulation (GDPR) consolidated disparate national legislation into a single union-wide law governing the way organizations must protect personal data and guarantee privacy rights to people in the territory.

GDPR.EU surveyed 716 small business leaders in Spain, the United Kingdom, France, and Ireland to understand how their businesses were coping with the new requirements. The results revealed a widespread eagerness to comply with the GDPR. Small businesses have spent tens of thousands of dollars on consultants and IT solutions. Most say the GDPR will not slow the growth of their company. "I would want my data protected, so I do the same for my clients," said one small business owner in London.

At the same time, many people are confused by the more technical aspects of data security, and a significant portion of business leaders admitted they did not comply with central requirements of the law. For instance, two-thirds of individuals claimed their organization uses an end-to-end encrypted email provider. But when asked to specify which provider, only about 9% named a service with this kind of encryption built in. Many named irrelevant companies and technologies, such as "Dropbox" or "the cloud" (the London business owner said "Mailchimp"). Meanwhile, nearly half of respondents said they did not always determine a lawful basis for processing user data before doing so, which is a key provision of the GDPR.

This report sheds light on GDPR compliance from the perspective of small businesses on the regulation's first anniversary. All of the people surveyed for this report are GDPR decision makers within their organizations: owners, managers, data protection officers, lawyers, and IT staff. Small businesses (in this case, defined as having fewer than 500 employees) face unique challenges concerning GDPR compliance. They represent the majority of firms but have the least capacity to conform to new regulations. They have smaller budgets than larger corporations, which also makes compliance more important. A small business can't afford to risk receiving a GDPR fine. The insights from this report can serve other business leaders as a benchmark by which to measure their own compliance efforts.

About GDPR.EU

GDPR.EU is an online resource dedicated to making GDPR compliance easier for small and medium-sized organizations. The website is filled with checklists, plain-language explainers, and news analysis, as well as the fully searchable text of the regulation itself. GDPR.EU is operated by Proton Technologies AG, which is co-funded by Project REP-791727-1 of the Horizon 2020 Framework Programme of the European Union. It is not an official EU Commission or Government resource. Nothing found in GDPR.EU or in this report constitutes legal advice.

Millions of small businesses still don't fully comply with the GDPR.

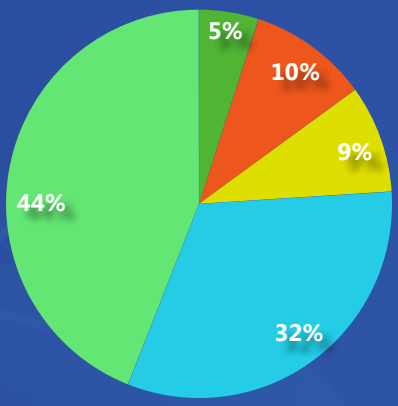
About half of GDPR decision makers believe their organizations are fully compliant with the GDPR, and 36% were mostly compliant. But when asked specific compliance questions, they weren't quite so confident.

Only 44% of organizations "completely agree" that their organization "describes its data processing activities in clear, plain language to data subjects" (Article 12). Most were either lukewarm about their performance (34% said they "somewhat agree" while 9% were "neutral") or believed they did not communicate data processing clearly.

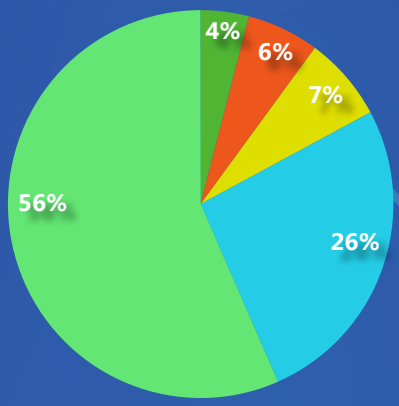
More surprisingly, a full 44% of respondents were not confident that they always obtain consent or determine a lawful basis before using personal data. Consent is a fundamental right of data subjects and Article 6 is the bedrock of the GDPR.

A significant portion of organizations (22%) said they do not use technical measures to protect personal data (Article 32). Of those who said they did use technical measures, encryption was the measure mentioned most often. Pseudonymization, anonymization, and antivirus software were cited less frequently but also used. However, many respondents were vague, unaware, or said they outsourced this aspect of compliance to contractors.

My organization describes its data processing activities in clear, plain language to data subjects.



We always obtain consent or determine a lawful basis before using personal data.



Completely disagree | Somewhat disagree | Neutral | Somewhat agree | Completely agree

What technical measures does your organization use?

"We ensure that all data collected is encrypted using up-to-datecloud technology and ensure that this data is used by pre-authorized members within our organization."

"I don't know."

"Innovation"

"Computer man"

Note: Percentages may add up to more or less than 100% because of rounding.

Encryption technology is not widely understood.

Even though the GDPR requires the use of encryption technology wherever feasible, a large number of business leaders seem not to understand basic data security concepts.

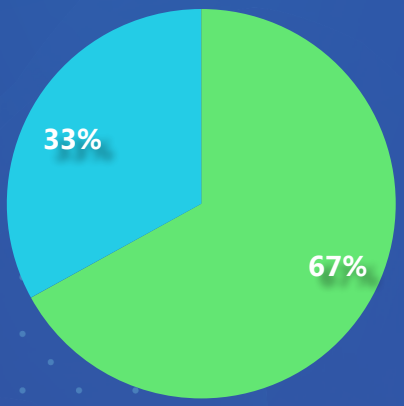
Two-thirds of respondents said their organization uses an end-to-end encrypted email provider to secure their communications against data breaches. (With end-to-end encryption, only the sender and recipient of a message can access it, preventing exposure even if there is a data breach of the email provider's servers.)

However, when asked which end-to-end encrypted email service they use, only about 9% of this group actually identified one[1]. The most popular responses were Gmail and Outlook. Many seemed not to understand the question at all. Of those who did identify an end-to-end encrypted email service, ProtonMail and Mailfence were the most common.

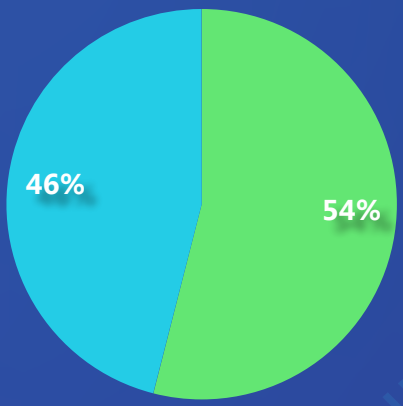
A little over half of the respondents said their organization uses an end-to-end encrypted cloud storage provider. But again, when asked to name their provider, they did not identify an end-to-end encrypted service. Google, Microsoft, Amazon, iCloud, and Dropbox were common answers. Seven respondents in Ireland said "Reddit," a social networking website. However, there were glimmers of hope. Six individuals in Spain named end-to-end cloud storage providers; four said Boxcryptor, and two said MEGA.

Among those who said they don't use end-to-end encrypted cloud storage, most said they don't use cloud storage at all.

Does your organization use an end-to-end encrypted email provider?



Does your organization use an end-to-end encrypted cloud storage provider?



Yes No

What end-to-end encrypted email provider does your organization use?

"HTML and other technologies are used to encrypt the messages."
"VPN"
"TLS"
"Mailchimp"
"WhatsApp"
"Dropbox"

1. It is possible to send end-to-end encrypted email using third-party software in conjunction with standard email services, such as Gmail or Outlook. However, only a handful of respondents mentioned using such software.

Small businesses want to comply and have invested heavily in GDPR compliance.

The vast majority (86%) of business leaders said it was essential to comply with the GDPR.

They gave four main reasons for prioritizing GDPR compliance:

1. Because it's the law
2. They don't want to get fined
3. It's good for business to protect data
4. They believe in the right to privacy

The minority who didn't believe it was important to comply with the GDPR often said they were too small for regulators to care much about.

"If we don't comply with GDPR we will have to pay an impossibly high penalty and we'll go bankrupt."

"Our reputation would be in the dirt if we didn't."

"I would want my data protected, so I do the same for my clients."

"We are a small organization, and I feel we have bigger fish to fry than GDPR."

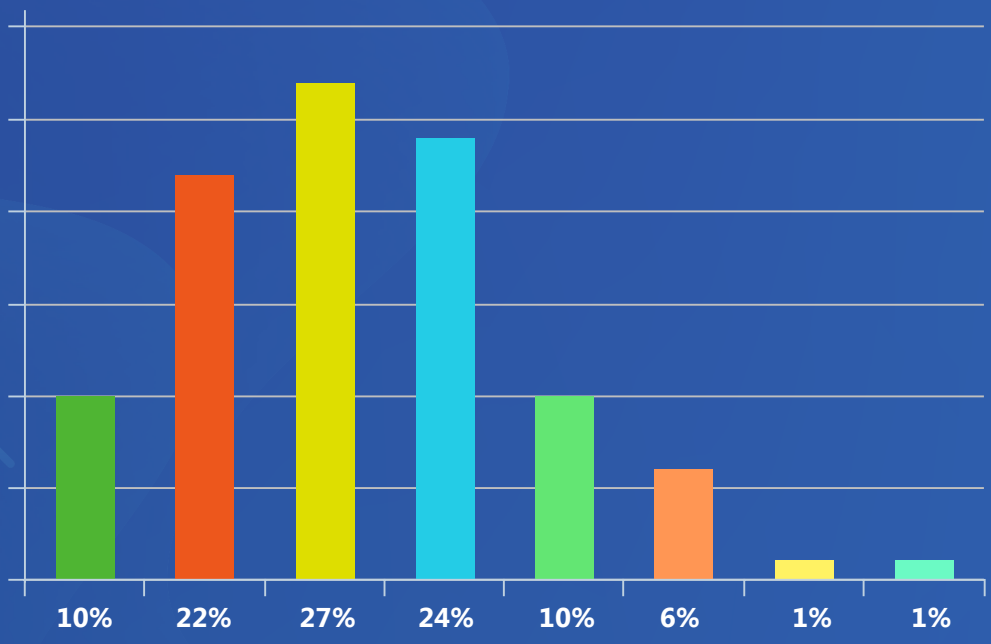
Over half of small businesses have spent between €1,000 and €50,000 on compliance. The most common expense was for employee training and consultants, followed by software and equipment. Yet 67% said these expenses were unlikely to affect the growth of their companies.

Despite their fear of penalties, respondents were uncertain about whether regulators were likely to impose fines against small businesses. Forty percent said it was "somewhat likely" to happen.

"When you consider the misuse of data by the likes of Facebook, say, why would the regulator spend time levying fines on sole traders?"

"Any GDPR breach, especially serious ones, will have grave consequences."

"We are the easy hits. Big companies can afford lawyers to fight in their corner. We can't so are seen as easy targets."



How much have you spent so far on compliance?

- €0
- €1-999
- €1,000-9,999
- €10,000-49,999
- €50,000-99,999
- €100,000-499,999
- €500,000-999,999
- >€1,000,000

Methodology

A total of 716 individuals in Spain, the United Kingdom, France, and Ireland completed surveys between January 17, 2019, and April 18, 2019, via Pollfish, an online survey fielding platform. The surveys were conducted in writing in the local language: English in the UK and Ireland, Spanish in Spain, and French in France. The number of completed surveys for each country is 250 in Spain, 242 in the UK, 134 in France, and 90 in Ireland.

Respondents were selected based on multiple screening criteria. They must be older than 18 and self-employed or employed for wages. Respondents then were asked whether their small business (fewer than 500 employees) was required to comply with the GDPR. Only those who stated their business is required to comply could advance to the second screening question. Here, respondents were asked whether they were a "GDPR decision maker," defined as someone who "oversees GDPR compliance as an owner or manager." Those "involved in GDPR compliance but not directly responsible" were disqualified from the survey. Only those who passed both screening questions were able to complete the survey.

According to the Eurostat, there are about 23 million small and medium-sized businesses in the European Union. Therefore, at a 95% confidence level, the margin of error for this survey is +/-4%.

GDPR.EU is co-funded by Proton Technologies AG and by a grant from the Horizon 2020 Framework Programme of the EU. However, the EU was in no way involved in the creation of this report. For more information about this survey, please write to media@gdpr.eu.