GDPR compliance – where are we now?

Research commissioned by Egress
Independently conducted by OnePoll
Autumn 2019
Introduction

This research was conducted to understand the status of GDPR compliance among UK businesses more than a year since the regulation came into force. Its aim was to assess compliance levels, identify the primary approaches UK organisations have taken to meeting compliance obligations, understand their general sentiment towards compliance and to establish whether this has been affected by recent ICO actions.

Methodology

Egress commissioned a survey, undertaken by independent research organisation OnePoll, in July 2019. 250 UK GDPR decision-makers were surveyed. Respondents represented a range of vertical industries, including accounting, banking and finance, business consulting and management, engineering, IT, public sector, retail, and transport and logistics. One-third (33%) worked for companies that employ more than 1,000 people, 32% work for mid-size companies employing between 250-999 people, and 35% work for companies with 249 employees or fewer.
The GDPR compliance landscape in the UK: Heading towards a perfect storm

GDPR came into force on 25th May 2018 following one of the most high-profile public and business information campaigns seen in the modern era. Organisations seemed to be scrambling to get their houses in order in advance of the deadline as the threat of punitive fines and reputational damage loomed large.

More than a year on, is it working? Are businesses better at protecting customer data than they were before? Are they meeting compliance obligations and have they achieved the culture shift required to live by the mantra of ‘privacy by design and default’?

We conducted a survey of GDPR decision-makers across different sectors and business sizes to find out the compliance status of UK businesses, their attitude towards the regulation and the main areas they have invested in to support compliance. We also wanted to know what impact the announcements of the first intended fines from the Information Commissioner’s Office (ICO) have had.

The results were striking. We found that, despite 96% of respondents having invested in GDPR compliance in the past 12 months and 70% saying their organisations felt positively about protecting data, currently more than half (52%) of UK businesses are still not compliant with GDPR.

Of those respondents, 42% stated they are ‘almost compliant’, but the fact they are not yet over the line demonstrates a loss of focus on achieving the necessary standard. This is supported by the fact that more than one-third (35%) said GDPR compliance has become less of a priority in the past 12 months. Even the ICO’s announcement of its intention to issue multimillion pound fines to BA and Marriott Hotels has not reignited urgency; only 6% of respondents said it had shocked their business back into awareness.

Nevertheless, UK businesses are keeping the ICO busy. 37% of respondents said they have been obliged to report one or more data breaches to the ICO in the past year. Evidence suggests that, when the ICO investigates these incidents, a high percentage of organisations will be found wanting.

We also found that organisations were prioritising processes and auditing when it came to compliance investment, with deployment of new technology further down the list. This difference in emphasis is often observed when regulations are in their infancy – but, evidently, this approach is not doing enough to turn the tide on data breaches in the UK, and many organisations could benefit from robust technology programmes to support their compliance. When we analysed the data by looking at business size, we discovered that mid-market firms have a significant compliance gap. Fewer organisations claimed full compliance and they were more than twice as likely as enterprise businesses and one-third more likely than small businesses to have reported an incident to the ICO in the past year. For these organisations, the compliance clock is ticking ominously towards a perfect storm of regulatory risk and security weakness. Reported breach incidents will continue to rise, attracting the attention of regulatory authorities that are more than likely to find compliance has not been achieved. They will not be slow to issue fines and take remedial actions as a result.

We hope that you find our research and analysis of the UK GDPR compliance landscape valuable and informative. Our report concludes with some reflections and a look at how focus will change as the GDPR compliance environment matures.

Tony Pepper, CEO, Egress
Key research findings

Compliance is not comprehensive

Fewer than half (48%) of surveyed businesses reported that they are fully compliant with the GDPR.

42% of respondents said their business was mostly compliant, 8% rated themselves partway compliant and 2% were not compliant at all.

More than one-third have reported incidents to the ICO

The general increase in breach reporting was echoed in the research as 37% of the GDPR decision-makers surveyed said they had been obliged to report a data breach incident to the ICO in the past 12 months. 17% had reported more than one incident.

Most say their business is positive about GDPR

70% of GDPR decision-makers surveyed said that their organisation was positive about GDPR and proactively protects data. 62% said their organisation has made GDPR a priority over the past year.

But focus on GDPR has waned in more than one-third of businesses surveyed

The high-profile run-up to implementation may have had businesses rushing to prepare, but 35% of respondents said there had been a drop in focus once the deadline had passed, saying that GDPR had become less of a priority since implementation.

New processes are the primary area of compliance investment

28% of the GDPR decision-makers surveyed said that implementing new processes around the handling of sensitive data was the biggest area of investment for their organisation since GDPR was implemented.

“We received around 14,000 PDB reports from 25th May 2018 to 1st May 2019. For comparison, we received around 3,300 PDB reports in the year from 1st April 2017.”

The ICO

---

How has your organisation prioritised meeting GDPR since its implementation?

Almost two-thirds (62%) of GDPR decision-makers surveyed said that their company has made the regulation a top priority over the past 12 months. This figure rose to 71% in companies with more than 1,000 employees and reached 81% among companies from the accounting, banking and finance sector.*

29% of organisations said they had carried out initial activity for the May 2018 deadline but that GDPR had become (and remained) less of a priority since then.

6% said there was less of a focus after the implementation deadline passed, but that the recent ICO announcement of its intention to fine British Airways and Marriott had shocked their business back into awareness.

The ICO signals serious intent

In July 2019, the UK’s Information Commissioner’s Office (ICO) announced its intention to issue the first fines levied as a result of breaches to GDPR. British Airways (BA) was ordered to pay the sum of £183.39m for a data breach it reported in September 2018, which saw the personal data of around 500,000 customers compromised, including log-in, payment card, home addresses and travel booking details. The ICO’s investigation into the breach found evidence of poor security arrangements by BA.

A second intention to fine was announced just over a week later in relation to Marriott Hotels, whose Starwood subsidiary was the subject of a long-term breach that exposed personally identifiable information (PII) in around 339 million guest records, including 30 million belonging to European Economic Area residents and seven million belonging to UK residents. The proposed fine is £99.2m.

While, these fines are not yet confirmed, as they will be subject to representations from legal teams of all the parties, their scale signals clear intent by the ICO to seek maximum and punitive recompense from organisations that fail in their duty to protect consumer privacy.

To add perspective, these fines are on the same scale as those issued against businesses that breach international business regulations, such as the Foreign Corrupt Practices Act (FCPA) and anti-money laundering (AML) legislation. The ICO has clearly signalled that failure to protect privacy will be viewed as a criminal transgression and punished in the severest terms.

* Small data sample
How does your organisation feel about GDPR?

70% of respondents were confident that their organisation is ‘very positive about GDPR and proactively protects data’, indicating that they are succeeding in driving the necessary culture change. More than one-quarter (27%), however, recognised their organisation in the description ‘it initially took GDPR seriously, but this has lessened as time passed’. This rose to 32% in companies from the IT sector and 35% among retail companies.*

Just 2% of respondents admitted that their organisation had ‘never really taken GDPR seriously’, showing that there is strong overall awareness of the importance of the data privacy regulation.

Since GDPR was implemented, what has been the single biggest area for compliance investment in your organisation?

28% of the GDPR decision-makers surveyed said that their biggest area of investment had been in implementing new processes around the handling of sensitive data. This figure rose to 30% in mid-size companies and 32% in large enterprises.

However, smaller companies had slightly different priorities; 26% had invested most in better auditing around what data they collect and for what reasons, outranking new process implementation, which was chosen by only 22%. One-in-five (20%) smaller companies said their biggest investment had been employing a Data Protection Officer (DPO) or additional compliance staff.

In the engineering and manufacturing sector,* respondents said they had invested most in better auditing around data collection (29%).

Deploying new technology was the biggest investment area for 17% of respondents overall, although this figure rose to 33% in the accounting, banking and finance sector. 21% of large and 19% of mid-size companies invested in new technology tools, while only 13% of smaller companies had made this their main focus.

End user education and training was the primary area of compliance investment for 8% of respondents overall. Larger organisations were less likely to have opted for this tactic, with just 5% saying it was the main focus of investment, while 10% of mid-size companies had invested in training.

Surprisingly, given the GDPR’s breach reporting requirement, implementing new procedures for incident reporting was also low on the ranking of key investments; just 8% said this had been their main area of activity.

In the period immediately pre and post-GDPR implementation, the initial focus on establishing processes is logical. The challenge going forward will be ensuring that employees comply with those processes.

It is notable that historically regulated sectors, where there is typically a more mature approach to compliance, such as accounting, banking and finance, have proved more likely to invest in technology to assist compliance efforts.
With the new regulation in place, have you had to report an incident to the ICO in the past 12 months?

37% of GDPR decision-makers surveyed said that they had been obliged to report a data breach incident to the ICO in the past 12 months. Of these, 17% had reported more than one incident.

Human error remains the leading cause of data breaches

According to figures obtained from the ICO, 60% of the 4,856 personal data breach incidents reported between 1st January and 20th June 2019 were the result of human error.

Analysis of the different sectors reporting breaches to the ICO reveals that the public sector is the worst performer when it comes to insider data breaches: healthcare suffered 18% of reported breaches; 16% were reported in central and local government; and 12% in education. Crossing the border between public and private sector, 11% were reported in the justice and legal sector. 9% originated from Financial Services organisations.

Causes of human error data breaches

- 43% occurred due to incorrect disclosure
- 20% were caused by employees posting or faxing data to the wrong recipient
- 18% resulted from email mistakes, such as sending to the wrong recipient or not using BCC
- 5% resulted from phishing attacks
- 14% Other

There was considerable variation in incident reporting frequency between the different company sizes. Almost three-quarters (73%) of large enterprises had not needed to report any breaches; 10% had reported a single breach and 13% more than one. Among mid-size companies, the number with no breaches to report was just 44%. 30% of mid-size companies had reported a single breach and 23% of them had reported more than one.

Small businesses had fared better than their mid-size counterparts. 21% had reported a single breach and 10% reported more than one.

In the engineering and manufacturing sector,* 29% had reported breaches in the past 12 months while 47% of information technology companies said they had been obliged to report one or more breaches.

---

* Small data sample

2 This information was obtained by Egress following a freedom of information request to the Information Commissioner’s Office. The office was asked to provide details of data breach incidents or losses (data protection cases) submitted to it with natures that reflect a Principle 7 or ‘security’ angle under the Data Protection Act or principle (f) under the General Data Protection Regulation, as well as details of the sectors reporting those incidents and the types of breach reported.
Analysis: Mid-size organisations face a compliance squeeze

Our analysis indicated that mid-size companies are struggling to cope with the scale of GDPR and its obligations in relation to their business.

While larger organisations have more budget and resources to devote to compliance and smaller businesses generally have lower compliance exposure, the mid-market is being squeezed, resulting in data breaches and compliance risks.

Our survey found that mid-size organisations are less likely to report full compliance and more likely to have reported a data breach to the ICO in the past year. 53% have reported incidents to the ICO, while only 39.5% say they are fully GDPR compliant.

Interestingly, a higher percentage of mid-market businesses (11%) said that the ICO’s intention to fine had reignited awareness. Combined with lower levels of compliance and higher incidence of breach reporting, this seems to indicate that they may have been adopting a high-risk ‘wait and see’ strategy before committing their full attention to meeting the regulation. The ICO’s announcements should be acting as a wake-up call that the regulator has real power and is prepared to use it.

“Mid-market companies… may have been adopting a high-risk ‘wait and see’ strategy before committing their full attention to compliance”

At this point in time, how would you rate the status of your own compliance with GDPR?

48% of GDPR decision-makers rated their organisations as fully compliant with the GDPR. 42% said they were mostly compliant, a further 8% said they were partway compliant and a remaining 2% said they were not at all compliant, meaning that for a significant proportion of UK organisations, GDPR compliance is still a work in progress.

Again, there was variation in compliance status related to organisation size. Large enterprises performed strongest, with 56% stating they were fully compliant. Next came small companies, where 51% were fully compliant. Mid-size companies were worst off, with only 39.5% saying they were fully compliant, although 53% said they were mostly compliant.

The accounting, banking and finance sector reported higher than average compliance levels, with 58% stating full compliance.
Reflections

‘Almost compliant’ is not good enough

We appear to be seeing an attitude that ‘almost compliant is good enough’. This is an increasingly high-risk strategy as ICO enforcement decisions start to come down the line. Worryingly, however, even these may not be enough to prompt businesses back into action – only 6% of GDPR decision-makers said their company had been moved to respond following the announcements regarding BA and Marriott.

Is this lack of impact down to the long wait between the implementation of the regulation and the first action? Or are businesses betting that the ICO will aim to make examples of large organisations and overlook the transgressions of less well-known companies?

However, the time to ‘wait and see’ has come and gone. The ICO has shown it has teeth, and will be aiming for consistent and fair application and interpretation of the regulation across all sectors and business sizes. Businesses that are not yet compliant must now make this a priority.

A shift from processes to people and technology

Most businesses focused compliance investment on establishing processes to manage sensitive data, better auditing and the employment of a Data Protection Officer. This is understandable in the early stages of compliance as organisations establish structures and frameworks. However, as time goes on, businesses will find that people and processes can be uneasy partners. It is one thing to have a process and another to ensure that employees follow it without making the errors to which busy workers are all too prone.

As data from the ICO highlights, this insider threat remains a major risk. People are always going to make mistakes or behave unexpectedly, so more must be done to provide a safety net that protects sensitive information. As organisations evolve from the adoption to the maintenance phase of GDPR compliance, I expect to see a shift towards greater investment in technology to support processes.

Beyond compliance: GDPR 2.0

For the 48% of organisations that have achieved full compliance with GDPR, the next priority is to maintain it. Data privacy will always be a continuous challenge that demands intelligent investment in people, processes and technology to ensure that it stays fit for purpose.

We are entering the era of GDPR 2.0, where businesses that have succeeded in instilling a privacy culture will cascade it through procurement strategies, seeking technologies and services that can help them make their privacy performance into a competitive differentiator.

The financial cost of maintaining compliance will also become a key focus as organisations’ approaches mature. As businesses look to drive efficiency, we will see growing interest in the power of artificial intelligence and business process automation to protect users, help them to work in a safe, effective, compliant way and reduce risk.

For the 52% of organisations that are still to reach compliance, the clock is running out. GDPR is here to stay and it is only a matter of time before we start to see the regulator exercising its power across a broad spectrum of businesses who are failing to protect customer data.
Egress Software Technologies Ltd

Egress takes a people-centric approach to data security – helping users receive, manage and share sensitive data securely to meet compliance requirements and drive business productivity. Using machine learning, Egress ensures information is protected relative to the risk of a data breach and reduces user friction to ensure smooth adoption.

Trusted by enterprise organisations and governments around the globe, Egress’ award-winning platform provides email encryption, secure file transfer and online collaboration services, as well as risk management, accidental send prevention, and compliance auditing and reporting.

Egress is headquartered in London, with regional offices in the UK, the US, Canada and the Netherlands.