THOMSON REUTERS

GDPR REPORT

Business' struggle with data privacy

Regulatory environment continues to evolve rapidly

The intelligence, technology
and human expertise you need
to find trusted answers.

the answer company™
THOMSON REUTERS®

Contents

Executive summary

On 25 May 2018, the General Data Protection Regulation (GDPR) took effect, representing the most significant change in data privacy regulation in decades. As such, the global landscape for data privacy has changed significantly. The response by businesses to this fast-changing regulatory environment has also shifted dramatically. Over one year later, businesses are struggling to comply with GDPR and other data privacy regulations.

Thomson Reuters surveyed data privacy professionals at global organisations in nine countries. The surveys were conducted in 2017 and again in December 2018—both before and after GPDR took effect. The companies surveyed have average global revenues of US $282 million dollars and an average of 16,400 employees.

The surveys found that global companies' struggles with data privacy laws and regulations around the world have increased in several ways since GDPR took effect:

- More companies are failing to meet global data privacy regulations
- Many companies have found GDPR compliance more difficult than expected
- Half of companies are at risk of falling further behind
- An increasing number of companies have now been subject to enforcement actions
- Companies are becoming less open and pro-active with consumers
- Board and c-suite concern and engagement on data privacy issues is falling
- GDPR is now consuming a greater proportion of data privacy budgets

On the positive side:

- Nearly all global companies are aware of GDPR
- Most companies consider themselves knowledgeable on GDPR
- Data protection costs have decreased in most countries

Global data privacy regulatory environment rapidly evolves

When GDPR went into effect, it brought with it a great deal of uncertainty. While the 261 pages GDPR contained plentiful details, there was no way of knowing what impact it would have on organisations. Any organisation processing or holding data of European Union (EU) residents must follow GDPR and there were no precedents for evaluating what events would trigger enforcement or how sanctions would be levied.

With fines of up to €10 million or two percent of a company's global revenues for a first GDPR offense, and double that for a second offense—clearly the stakes are high.

The European Commission reported that as of January 2019, shortly after this latest survey was conducted, 95,180 complaints of alleged violations of GDPR had been filed with data privacy authorities in Europe. The most common complaints involved telemarketing, promotional emails, and use of closed-circuit television (CCTV) or video surveillance. In the first year of GDPR's application, 281,088 cases were logged by supervisory authorities. Of these cases, complaints accounted for 144,376 and there were 89,271 data breach notifications by data controllers.

France's data privacy enforcement agency, Commission nationale de l'informatique et des libertés (CNIL) has applied a €50 million fine on Google for GDPR violations, citing "lack of transparency, inadequate information and lack of valid consent regarding personalisation" of ads delivered to consumers. In addition, a €20,000 fine was assessed against a German social network operator for failing to secure users' data, as well as a €5,280 fine against an Austrian sports betting café for unlawful video surveillance. To date, the two most significant fines levied have been British Airways for £183m by the Information Commissioner's Office (ICO), in the UK, for not protecting customer data, and a £99m fine by the ICO on Marriott for not protecting guest data.

Despite a two-year grace period between passage in 2016 and implementation in 2018, which was intended to give organisations ample time to prepare, our survey has found after GDPR went into effect, companies are still struggling to meet its requirements.

With more data privacy laws and regulations coming into effect over the next few years in other countries, including the United States (U.S.), India, and China, the challenges facing businesses are mounting.

"With fines of up to €10 million or two percent of a company's global revenues for a first GDPR offense, and double that for a second offense—clearly the stakes are high."

Businesses struggle to meet GDPR and other data privacy regulations globally

More companies are either failing to meet regulatory requirements or having trouble keeping up. A massive 79 percent of companies surveyed post-GDPR say that they are either failing to meet regulatory requirements, having trouble keeping up to date, or both—compared with 72 percent prior to GDPR implementation.

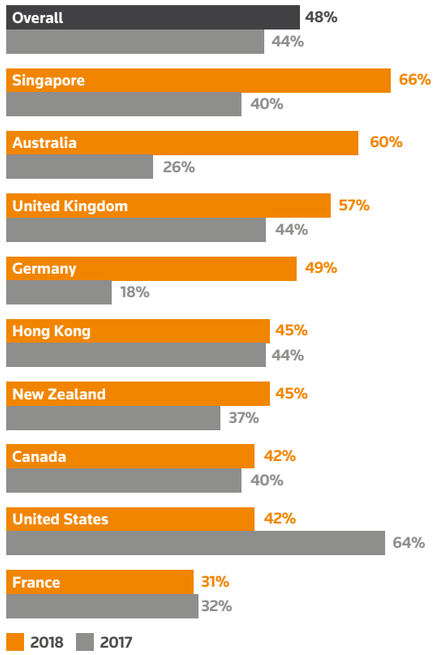
Meeting Current Requirements

Nearly half of companies (48 percent) say they are failing to meet the requirements of GDPR and other data privacy regulations around the world. That is up from the 44 percent in 2017.

U.S. companies have seen major improvements. In 2017, U.S. businesses were the most likely by a significant margin to report that they were failing to meet data privacy requirements. Nearly two-thirds of U.S. organisations (64 percent) said at that time that they were unable to meet requirements. In 2018, that percentage fell to 42 percent and is now among the lowest among the countries surveyed. Only France is currently reporting better numbers.

Meanwhile, reports of difficulties have increased across some EU counties as well as Australia and Singapore, since GDPR implementation. For example, in 2017, only 18 percent of companies in Germany and 44 percent in the UK were failing to meet requirements. Now, those percentages have risen to 49 percent in Germany and 57 percent in the UK.

Failing To Meet Data Privacy Requirements



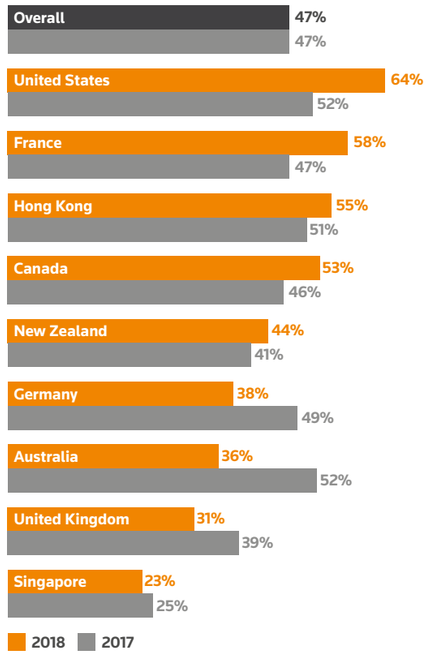
Keeping Up or Falling Behind

Moreover, nearly half (47 percent) of companies surveyed globally say they are struggling to keep up to date or falling further behind. That figure is unchanged from prior to GDPR implementation.

However, within each country, the numbers have changed considerably. Since GDPR took effect, more companies in the U.S., France, Hong Kong, Canada, and New Zealand are having troubling keeping up compared with a year earlier. Nearly two-thirds (64 percent) of U.S. companies now say they are having difficulty keeping up, up from 52 percent a year earlier.

Meanwhile, fewer companies in Singapore, UK, Australia and Germany are saying that they are unable to keep up compared with a year earlier, and those four countries are currently reporting the lowest levels of difficulty keeping up to date on regulatory requirements.

Struggling To Keep Up To Date Or Falling Further Behind

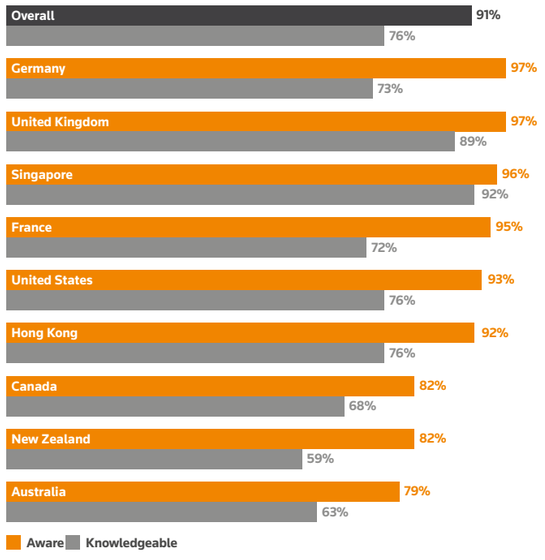


Aware and knowledgeable about GDPR

Businesses are now almost universally aware of GDPR. Ninety-one percent of companies surveyed are aware of GDPR, up from 86 percent prior to GDPR implementation. Not surprisingly, the EU countries in the survey are all above the global average, with Germany and the UK reporting 97 percent awareness. Companies in Canada, New Zealand and Australia currently have the lowest levels of awareness of GDPR, but even so, eight in ten businesses in those countries are aware.

However, there are sizeable gaps between the percentage of companies that are aware of GDPR and those that say they are knowledgeable about GDPR and its 11 chapters and 99 articles. While 91 percent of companies surveyed globally are aware of GDPR, only 76 percent say they are knowledgeable about it. Even in Germany, where 97 percent of companies are aware of GDPR, the percentage that are knowledgeable about GDPR is at a much lower 73 percent, representing a significant gap between levels of awareness and knowledgeability.

Companies Aware Of & Knowledgeable About GDPR

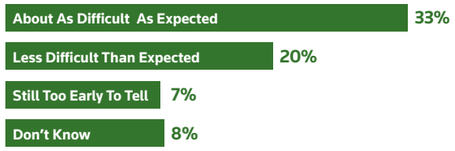


GDPR compliance challenges

Companies are split on whether GDPR compliance has been more or less difficult than they expected. A third say it has been more difficult than expected. Another third has found GDPR to be about as difficult as expected. Only 20 percent said it has been less difficult than expected. Fifteen percent don't know or say it's still too early to tell.

Hong Kong, UK and U.S. companies were most likely to say that GDPR has been more difficult than expected.

A Third Of Companies Say GDPR More Difficult Than Expected



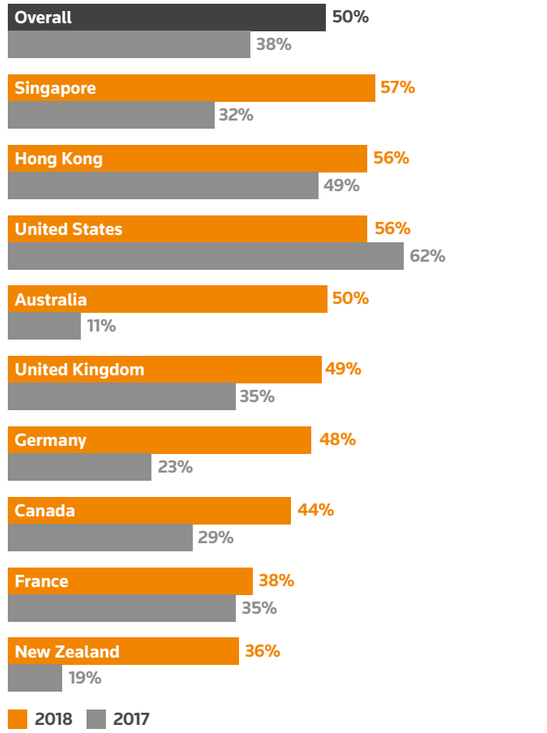
Enforcement actions

Many of these struggles may be because since GDPR went into effect, more companies are dealing with enforcement actions for non-compliance with a data privacy regulation, whether involving GDPR or any other regulations globally.

Half of companies surveyed say they have been the subject of an enforcement action, up from 38 percent the year before. The percentages were up in every country except for the U.S., Singapore has the highest rate at 57 percent. Even in New Zealand—the country with the lowest rate—more than a third of companies reported receiving enforcement actions.

Australia saw the largest jump, with half of companies surveyed saying they have experienced an enforcement action, compared with only 11 percent a year earlier.

Have Been The Subject Of Enforcement Action



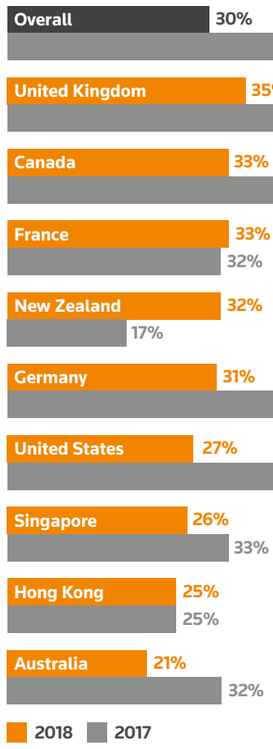
Engagement with consumers

Businesses have become less engaged with consumers on data privacy issues since GDPR implementation. Less than one-third (30 percent) of companies surveyed say they are being open and pro-active with consumers on data privacy, down sharply from 42 percent before GDPR took effect.

Consumer engagement levels have plummeted in the U.S. Before GDPR took effect, U.S. companies were the leaders, with 60 percent saying they were open and pro-active with consumers. In the year since GDPR, that percentage has fallen by more than half to 27 percent. And the U.S. has gone from leading the world—to just being average on being pro-active and the least likely to be open with consumers.

New Zealand is the only country where more companies say they are open and pro-active in engaging consumers since GDPR. France and Hong Kong have stayed about the same both before and after GDPR.

Open And Pro-active Engaging Consumers On Data Privacy



Corporate board and c-suite—concern and engagement

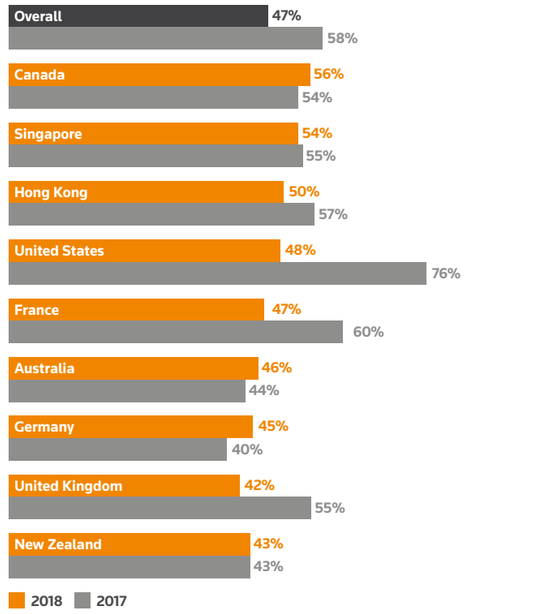
Concern and engagement on data privacy at the board and c-suite level has fallen sharply in several countries in the last year, most notably in the U.S.

Prior to GDPR implementation, the U.S. had the highest level of executive concern and engagement. In 2017, 76 percent of U.S. companies said their board or c-suite was concerned about data privacy. In just one year, that percentage has fallen to less than half (48 percent).

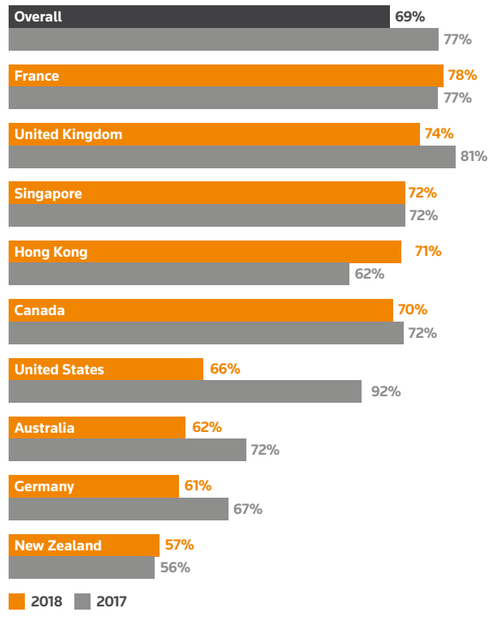
An even larger drop was seen in U.S. engagement levels. A year earlier, an overwhelming 92 percent of U.S. companies surveyed reported that their board or c-suite was engaged on data privacy issues. That percentage of engagement has now fallen to 66 percent, dropping the U.S. from the top spot to below the average of countries surveyed.

Every country surveyed saw drops in either concern or engagement levels, although none of the declines was as dramatic as the U.S.

Board/C-suite Concerned



Board/C-suite Engaged



Company spend on data protection

Companies report spending an average of US $1.32 million in 2018 on data protection issues, including employees, software, and third-party resources. This represents a slight decrease from the US $1.36 million reported in 2017.

Spending increased in Canada, Australia, New Zealand and France. Data protection costs decreased dramatically in the U.S., going from an average of US $2.1 million to US $1.5 million. Costs also decreased in Singapore, Hong Kong, Germany, and the UK.

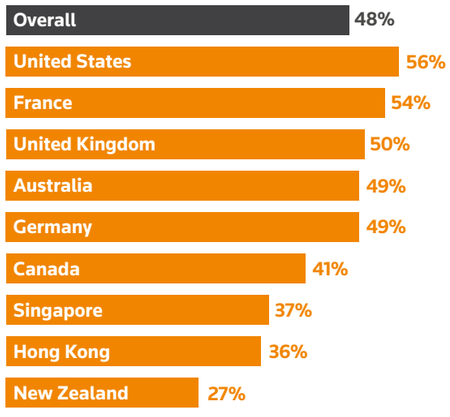
*all figures in USD.

Data Protection Costs	2018	2017
France	$1.7m	$1.2m
UK	$1.1m	$1.2m
Singapore	$0.9m	$1.6m
Hong Kong	$1.2m	$1.5m
Canada	$1.5m	$1.1m
United States	$1.5m	$2.1m
Australia	$1.8m	$0.7m
Germany	$1.1m	$1.1m
New Zealand	$0.6m	$0.4m

Costs expected to increase

Nearly half (48 percent) of companies surveyed expect their global cost of data protection to increase this year. Expectations for higher costs are greatest in the U.S. (56 percent) and France (54 percent), and lowest in New Zealand (27 percent).

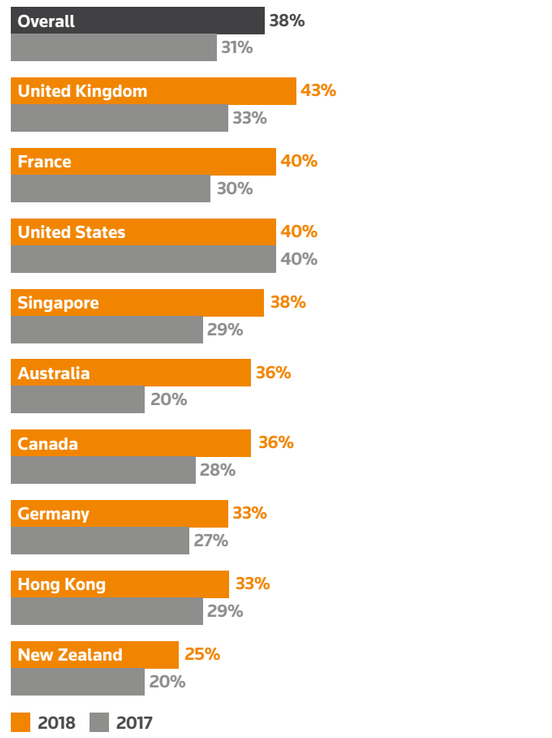
Half Of Companies Expect Costs To Increase



GDPR—data privacy budgets

GDPR is claiming an increasing proportion of data protection budgets, rising from an average of 31 percent in 2017 to 38 percent in 2018. UK companies reported the highest proportion of their budgets being consumed by GDPR at 43 percent.

GDPR Compliance As % Of Total Data Privacy Budget'

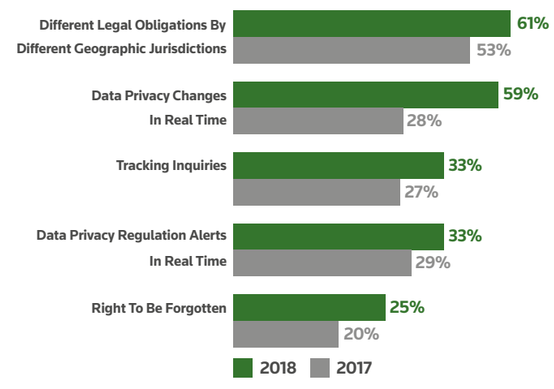


Tools for tracking legal obligations

Many companies say that they lack adequate tools for tracking their regulation and consumer engagement obligations. However, the encouraging news is that more companies reported having at least some tools in place.

Possess Adequate Tools For Tracking

Different legal obligations by different geographic jurisdictions



The future of privacy regulation

GDPR has been described as the most significant change in data privacy regulation in more than two decades. However, it is proving to be only the first step in a sweeping global transformation of such regulations.

With over a year of experience dealing with GDPR under their belts, companies are now having to turn their attention to a growing number of new data privacy regulations taking effect worldwide. According to Thomson Reuters Data Privacy Advisor, several countries passed new data privacy laws in 2018—many modeled after GDPR—including Brazil, Bahrain, and Israel. Other countries are in process of implementing new data privacy regulations, such as China and India. Recently, several other Latin American countries have announced a series of legislative proposals to update their respective data protection regulations—to include: Argentina, Chile and Columbia. One Latin American country, Uruguay, has data privacy laws that already account for some aspects of GDPR requirements.

Even within the EU, nearly all member states have now adopted national data protection laws that in many cases supplement GDPR, resulting in non-uniformity across the EU on data privacy requirements. For example, specific data processing activities—such as matters relating to freedom of information, freedom of expression, or public access to official documents—member states can provide exemptions or derogations..

U.S. national data privacy law in the works?

While the U.S. still lacks a national data privacy law, numerous recent high-profile data breaches have raised calls for Congress to pass such legislation. Several bills have been introduced that would establish national privacy requirements, including the American Data Dissemination Act (Section 142) and the Social Media Privacy Protection and Consumer Rights Act (Section 189).

Even in the absence of a national data privacy law, enforcement of existing data privacy regulations may be stepping up. Facebook recently revealed in a regulatory filing that it is setting aside US $3 billion for an anticipated settlement with the Federal Trade Commission (FTC) over an investigation into its data privacy practices, which would be the largest such fine ever by the FTC.

FTC Commissioner Joseph Simons has suggested that in the future, company executives could potentially face financial and other penalties for their personal responsibilities in data breaches and data privacy violations..

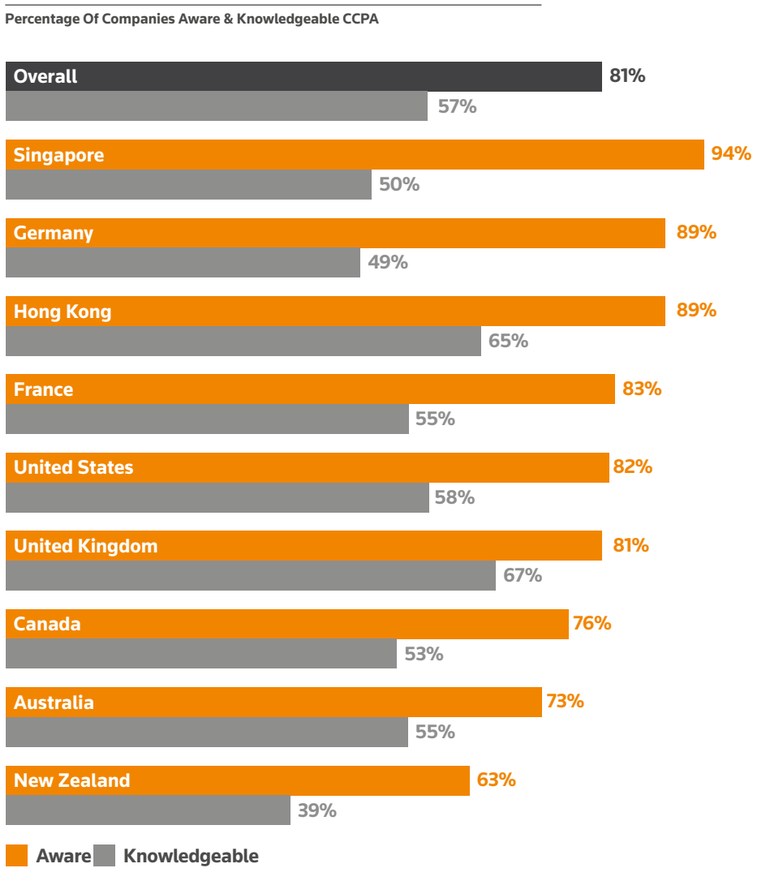
California Consumer Protection Act

One of the important recent developments has been in California, where the California Consumer Protection Act (CCPA) was passed in June 2018. The provisions apply to any organisation conducting business within the state. CCPA takes effect on January 1, 2020 and in the wake of its passage, at least 11 other states are also considering similar legislation this year.

Somewhat surprisingly, companies in Singapore, Germany, Hong Kong and France are more likely to be aware of CCPA than companies in the U.S., where awareness is only about at the global average of just over 80 percent. However, in 2018, California was the world's fifth largest economy—which is ahead of India and behind the UK and Germany—and trades globally.

UK (67 percent) and Hong Kong (65 percent) businesses are most likely to say that they are knowledgeable about CCPA, followed by the U.S. (58 percent).

For the countries surveyed, awareness and knowledgeability levels around CCPA, as its implementation date approaches are mostly lower than similar readings taken for awareness and knowledgeability of GDPR prior to its implementation.



China

Though China has the most internet users in the world, at present they do not have a single comprehensive data protection law. There are various laws and regulations pertaining to personal data protection, however, the system is complex and has been viewed as ineffective due to rapid technological advancements. The country's top legislative body, the 13th National People's Congress (NPC) of the People's Republic of China, has put on its agenda to legislate on personal information protection. The aim is to implement standards relating to the data protection requirements imposed by their cybersecurity law, which came into effect in June of 2017.

India

India is the world's second largest internet population with over 500 internet users. India also ranks second to China in the e-commerce market. As a country offering extraordinary business opportunities, the years of free reign over personal information needed to change. In 2017, India's Constitution, Article 21 'Right to Life & Liberty' was amended to include that privacy is a fundamental right. This Constitutional change prompted a move towards a national privacy law. The result was a draft of the comprehensive 'Personal Data Protection Bill (PDPB) 2018'. The Bill proposes a detailed legal framework and draws heavily upon GDPR. However, there are significant differences—

such as the PDPB doesn't include the 'right to be forgotten'. Another difference is the requirement of localisation for processing of data. A citizen's data must say in the country for collection, processing and storage. The PDPB is likely to be enacted in 2019.

The Kingdom of Bahrain

The Constitution in the Kingdom of Bahrain (Bahrain) guarantees an individual right to privacy. This is applicable for postal, telegraphic, telephone and electronic communications. In Bahrain, the all-encompassing data protection law is Law No. 30 of 2018 on the Personal Data Protection Law (PDPL). The PDPL went into effect on 1 August 2019. The PDPL provides rights to the individual in relation to how their personal data can be collected, process and stored. Businesses now have an obligation to ensure personal data is held securely. A new authority, the Personal Data Protection Authority, has the power to investigate potential violations of the PDPL and can issue orders and fines, both criminally and administratively. The PDPL is somewhat comparable to the GDPR, however, there are differences such as the role of 'Data Protection Supervisor' (DPS) in Bahrain. Unlike a Data Protection Officer under the GDPR, the DPS must exercise their role in an "independent and neutral manner".

Israel

In May of 2018, Israel's new data protection regulations came into force. The Privacy Protection Regulations (Data Security), 5777-2017, implements the data security requirements put forth by the Privacy Protection Act, (PPA, 5741-1981). In accordance with the Privacy Protection Law, the Privacy Protection Authority (PPA) is the regulatory and enforcing agency. The PPA has the responsibility to protect all personal information held in digital form; has the power to levy administrative and criminal fines for breaches; and, is applicable to all entities holding personal digital information—private, business and public. The PPA, 5741-1981, has some similar principles to that of the GDPR, although, the new privacy regulations impose requirements beyond that of the GDPR. For example, the GDPR only requires 'appropriate technical and organisational measures' are taken to ensure an appropriate level of security as compared to risk. The data security requirements in Israel are significantly more specific and include detailed requirements for collection and storing of personal data. Before in addition to data security measures, data export restrictions and outsourcing are governed by more stringent guidelines that the GDPR.

Argentina

In October 2000, Argentina passed one of the first data protection laws in the Latin American region. Today, the Law on Protection of Personal Data (PDPL) (Ley de Protección de los Datos Personales), Law 25.326 remains largely unchanged. However, in 2018 a bill was proposed: MEN-2018-147-APN-PTE—which is closely aligned with GDPR including similar rights and principles. As stated in the preamble, the Bill aims to provide Argentina with a more modern data protection laws that address new circumstances created by new technologies—as well as the global developments in data protection legislation. If the Bill is adopted, it will replace Law 25.326 in its entirety. If the Bill becomes law, it is anticipated to improve the processing of personal data by better definition of the scope and concepts, reach, security obligations, and accountability mechanisms.

Brazil

In Brazil, the new data protection law 'Lei Geral de Proteção de Dados Pessoais (Law No. 13.709/2018) (LGPD) enters into force in Feburary 2020. The LGPD introduces some important revisions to the previous sector-based approach, comprised of over 40 different regulations, which was regulated by the countries' civil rights framework. A new agency will be created—the National Data Protection Authority (Autoridade Nacional de Proteção de Dados) (ANPD)—to oversee and enforce the LGPD. The new legislation imposes detailed rules for the collection, use, processing, and storage of personal data—and was inspired by the GDPR—with similar requirements for data protection impact assessments; data exports limited by adequacy requirements of the destination; data protection officers; limits on automated processing; and, data breach notifications to the ANPD and the data subject.

Chile

Chile was the first South American country to pass a comprehensive data protection law in 1999. The aim of Derecho a la Privacidad (Right to Privacy), Law No. 19.628 was to establish general provisions regarding third-parties processing personal information. However, Law No. 19.628 fails to establish compliance and enforcement mechanisms. The National Congress of Chile is considering a new data protection bill which will amend Law No. 19.628 and takes into account aspects of GDPR's standards and provisions. Moreover, in 2018 Chile modified its constitution, Article 19, to include protection of the right to protection of personal data.

Columbia

Columbia recognizes the right to privacy and the right to data rectification in its Constitution. Processing of personal data is further regulated by two laws. The first, Ley hábeas data y manejo de la información contenida en bases de datos personales, which is Law 1266 of 2008 (known as the Law of Habeas Data or the financial habeas data) and covers data law and management of personal information. The main purpose of Law 1266 is for regulating use of financial and commercial use of personal data. The other, Ley protección de datos personales (Personal Data Protection Law), which is Law 1581 of 2012. The purpose of Law 1581 was to establish a more comprehensive legal framework that is applicable to government and nearly all commercial and non-commercial activities.

Despite the legislation in place, which is relatively recent, the GDPR includes obligations that the existing Columbian laws do not account for such as the appointment of a data protection officer and the right to be forgotten. There is a Bill in Congress that will supplement Law 1581 to remedy those issues as well as enable the local data protection authority to impose fines on data controllers and processors.

Uruguay

Uruguay was one of the first Latin American countries to adopt a comprehensive data protection law. On 11 August 2008, 'Ley De Proteccion De Datos Personales' (Data Protection Act) Law No. 18.331 entered into force. It operates a framework of laws that apply to personal data. Working in conjunction with Law No. 18331 are 'Ley de Acceso a la Información Pública', (Law on Access to Personal Information / the Habeas Data Action), Law No. 18.381, and Decree 414/009 (31 August 2009). The later, Decree 414/009, was adopted specifically to bring its regime into alignment with Europe's data protection regime. The legislation strengthens the scope, data breach notification requirements, accountability, and includes the requirement of data protection officers. Despite the age of the existing laws, the updated legislation already includes aspects of GDPR. Uruguay has received 'adequacy' status by the EU, but still closely monitors for other changes to be implemented. The data protection 'authority' or 'body' of control is the 'Unidad Reguladora y de Control de Datos Personale's (URCDP) was established by Article 31 of Law No. 18.331. Overall, with the increased awareness of an individual's right to privacy, the URCDP has seen a rise in the number of complaints of data privacy breaches.

Conclusion

GDPR clearly had a major impact on global organisations' ability to meet their data privacy regulatory requirements. Many companies are having difficulty meeting those requirements and are in danger of falling even further behind. While the cost of compliance generally did not rise following GDPR taking effect, further cost increases are expected, and many companies still lack vital tools for tracking and meeting the increasingly expanding global regulatory framework they are facing. Data privacy regulations around the world continue to proliferate at a rapid pace. And if the GDPR implementation provides any lessons, it appears to be that organisations are finding themselves increasingly challenged to meet these growing requirements.

"GDPR has been described as the most significant in data privacy regulation in more than two decades. However, it is proving to be only the first step in a sweeping global transformation of such regulations."

Contact Us

Thomson Reuters

If you'd like to receive more reports and exclusive content about legal industry trends from Thomson Reuters visit us at: **legalsolutions.thomsonreuters.co.uk** or **tr.com/legalinsights**

Follow us on Twitter: **@TRLegalEurope**

Follow us on LinkedIn, search:
Thomson Reuters Legal Europe