



**CONSUMERS  
INTERNATIONAL**

COMING TOGETHER  
FOR CHANGE

# **THE STATE OF DATA PROTECTION RULES AROUND THE WORLD**

## A BRIEFING FOR CONSUMER ORGANISATIONS

As the strongest data protection laws to date come into force for citizens in the European Union, Consumers International looks at the key components of the new EU General Data Protection Regulation and takes a snapshot of data protection regulations for consumers across the globe.

Consumers International is the membership organisation for consumer groups around the world. It is a charity (No.1122155) and a not-for-profit company limited by guarantee (No. 04337865) registered in England and Wales.

## WHAT IS THE EU GENERAL DATA PROTECTION REGULATION?

The EU's General Data Protection Regulation (or GDPR) came into effect on the 25 May 2018, replacing the previous minimum standards for processing data provided in the Data Protection Directive of 1995<sup>1</sup>. Though many of the main concepts and principles from the Directive underpin the GDPR, there are critical updates intended to address the implications of the digital age and the ways in which consumers' and citizens' data is collected, analysed and transmitted by new types of business practices and models, such as social networks, mobile applications and e-commerce.

- For the consumer, GDPR has strengthened rights. Individuals now have the power to demand companies reveal or delete the personal data they hold.
- For regulators, GDPR makes provisions which stipulate that data protection law will become identical throughout all EU member states. This should encourage partnership working and create a more harmonious environment for regulators, who previously worked independently and had to launch separate actions in each jurisdiction.
- GDPR requires businesses to be more accountable to the people whose data they collect and imposes much tougher punishments for those who fail to comply. All businesses handling EU citizens' data, whether based in the EU or outside, must comply with GDPR. Any business found not doing so could be charged fines of up to €20 million or 4% of the company's global annual turnover.

**GDPR will replace the EU's previous data law adopted in 1995 – before Google was even registered as a domain name.**

## THE MAIN CHANGES IN MORE DETAIL

The internet has made it easy to access information by visiting a website, or to buy goods and services at the touch of a button. But most consumers aren't always fully aware that in doing this, the organisations they deal with online are collecting vast amounts of personal data about them. This can be in the form of obvious things like your name and address, to tracking your browsing behaviour, location and inferring your preferences from this. This data is then used by companies in everything from sales to customer relationship management to marketing. The ease and sophistication of data collection means that thousands of companies not only collect personal details, but store it in often insecure locations, share it with third parties or move this data across borders to support their businesses. In addition, their business models rely on selling access to this data to advertisers who then target consumers with 'tailored' (or creepy) advertising.

With many security breaches now well publicised by the media, consumers are increasingly becoming aware about what happens to their data and have looming privacy concerns about what is being stored and processed, and by who. Policy makers and regulators have recognised the lack of protection offered by the former Directive in this area and have updated GDPR to rectify it. For example, a key component of GDPR is the requirement for consent, which must be an active agreement by the data subject, rather than the current models offered through pre-ticked boxes or opt-outs. It also puts obligations on businesses to carry out Privacy Impact Assessments for certain data use cases. This will have the effect of enabling businesses to consider more holistically what the organisation is doing with the data it collects and the impact it could have on people's privacy – giving them a chance to look across the piece at what they are collecting and why. Another key feature is privacy by design, which forces a company to design their data collection and processing methods in accordance with data protection law. In other words, they will need to ensure their data protection policies, structure and personnel are compliant.

Some other significant enhancements to GDPR that will empower the consumer include:

- Audit trail: Companies must have a record of when and how an individual has given consent.
- Right to be forgotten: In some circumstances, GDPR gives individuals the power to get their personal data erased ie where it is no longer necessary for the purpose it was collected, if consent is withdrawn, there's no legitimate interest, or if it was unlawfully processed. In this instance the controller and the people they have shared your information with will need to ensure it is permanently deleted.
- Automated decision-making: In some cases, individuals have the right not to be subject to decisions based on automated processing without any human intervention

---

1 [EU, Rules for the protection of personal data inside and outside the EU](#)

- Data portability: A new right under the GDPR, this enables individuals to request the transmission of their data to another controller to allow the data subject to make further use of the data. The further use could be to analyse bank transaction data for spending patterns and insights, or to move contacts from one network to another.
- Transparency of data collection and transmission: Companies must make clear how they collect people's information, what purposes they use it for, and the ways in which they process the data. This must be done in clear, easy to understand language.
- Accessing your data: People will a) no longer be charged to access their data and b) have the right to access any information a company holds on them within one month of asking. They can also ask for that data, if incorrect or incomplete, to be rectified.
- Mandatory breach notification: Companies' monitoring protocols must be able to recognise and act on breaches as soon as they happen. Companies must alert both their data protection authority and the people affected by the data breach within 72 hours of becoming aware of it, giving full details of the breach and an incident recovery plan proposal for mitigating its effects.
- Data Protection Officer: Companies over a certain size who regularly and systematically monitor or process data on a large scale must employ a data protection officer who will act as a point of contact for employees and customers with data protection queries.
- Children: Businesses will need to seek parental consent to process children's data.

## WHAT IS HAPPENING ACROSS THE WORLD?

Concern about how much data is collected, loss of privacy, security risks and other consequences is growing. In 2016, 57% of consumers worldwide reported that they were more concerned about their online privacy than they were in 2014<sup>2</sup>.

The GDPR is now the strongest data protection regime in the world, leading many to hope that it will set a 'gold standard' for other jurisdictions. The requirement on companies that process EU citizens' data to abide by the regulation regardless of location, adds weight to this and could be used as leverage by citizens of other countries, particularly where company activity crosses borders.

**A key component of GDPR is the requirement for consent, which must be an active agreement by the data subject.**

That is the hope for the future – but what is the current status of data protection laws across the world?

Globally, there is an increasing growth in data protection laws, many of which have been modelled on comprehensive guidelines or regulation such as the EU Directive mentioned above, or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data<sup>3</sup>. According to UNCTAD data protection tracker<sup>4</sup>, over 100 countries around the world now have data protection laws in place. Below is a summary of which countries across the globe have full or draft data protection legislation in place, based on this tracker.

### Africa

In Africa, 19 countries (Angola, Benin, Burkina Faso, Chad, Equatorial Guinea, Mali, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Malawi, Morocco, Niger, Senegal, South Africa, Tunisia, Zambia) have enacted data protection and privacy laws. 6 have laws in draft stages (including Kenya, Nigeria, Togo, Tanzania, Uganda and Zimbabwe). The remaining countries either have no legislation or have no data available.

As a continent, the African Union adopted the progressive [Convention on Cyber Security and Personal Data protection](#) in 2014. Only ten countries (Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia) are signatories and only two (Mauritius and Senegal) have [ratified](#) the convention.

Regionally, there is effort to ensure data protection within regional blocs. For example the Southern African Development Community (SADC) has developed a [model law](#) harmonising policies for the ICT Market in Sub Saharan Africa, which includes components on data protection. The Economic Community of West African States (ECOWAS) has created the [Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS](#). Finally

2 Centre for Internet Governance Innovation – Ipsos, '[2016 CIGI-Ipsos Global Survey on Internet Security and Trust](#)', 2016

3 OECD, [OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#)

4 UNCTAD, [Data Protection and Privacy Legislation Worldwide](#)

several Francophone countries (Benin, Burkina Faso, Ivory Coast, Gabon, Mali, Morocco, Senegal and Tunisia) are part of the French-Speaking Association of Personal Data Protection Authorities (AFAPDP) which promotes personal data protection principles and rules in French-speaking countries.

### Asia Pacific

Both Australia and New Zealand have legislation around data protection. In Australia the government has amended the Australia Privacy Act 1988<sup>5</sup> to include mandatory breach notification requirements that will require organizations to report an 'eligible data breach' to the data protection authority and notify affected customers immediately. In New Zealand the country's Privacy Act<sup>6</sup> controls how 'agencies' collect, use, disclose, store and give access to 'personal information'.

In Asia, 15 countries (Bhutan, China, Hong Kong, India, Indonesia, Iran, Israel, Japan, South Korea, Malaysia, Nepal, Oman, Philippines, Taiwan, UAE, Vietnam, Yemen) have legislation. Four are in the process of drafting (Iraq, Jordan, Pakistan, Thailand), while the others either have none or have provided no data.

Regionally, the continent has the Asia-Pacific Economic Cooperation<sup>7</sup> (APEC) Privacy Framework which aims to develop uniform standard of data protection law across the region. Only China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Philippines, Singapore and Vietnam are a part of this regional bloc. The APEC Cross-Border Privacy Rules (CBPR) system has been forged out of this framework. Unlike GDPR the CBPR system does not displace or change a country's domestic laws and regulations.

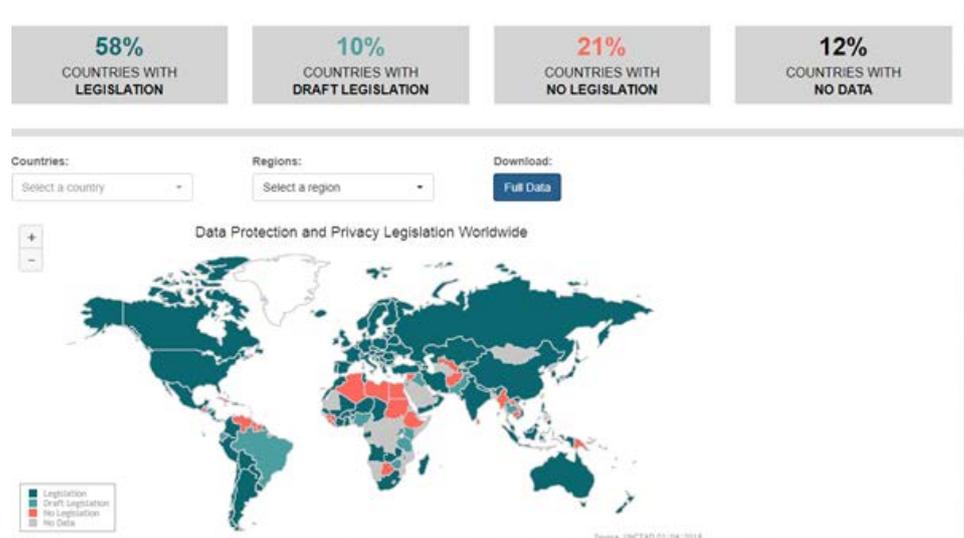
### The Americas and the Caribbean

Across North America and Latin America 17 countries (Canada, US, Mexico, Nicaragua, Jamaica, Trinidad and Tobago, Nicaragua, Costa Rica, Colombia, Peru, Bolivia, Chile, Argentina, Paraguay, Uruguay, Bahamas, Dominican Republic) have legislation. 4 are drafting (Ecuador, Honduras, Panama, Brazil, Jamaica) while the others either had none or had no data available to determine whether one was in place.

Outside of its own country specific legislation, the US and the EU have adopted the EU-US Privacy Shield Framework.<sup>8</sup> This Framework was designed by the US Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

Latin American countries are also part of the Ibero-American Data Protection Network (RIPD), which consists of 22 Data Protection Authorities from Andorra, Argentina, Chile, Colombia, Costa Rica, Mexico, Peru and Uruguay. Over the last decade, the organisation has promoted the development of comprehensive data protection legislation and the introduction of data protection authorities throughout Latin America.

A 2016 Consumers International member survey found that in Latin America concern over how individuals' data is collected and fears over loss of privacy are relatively high compared to all other regions. 70% of respondents from Latin America and the Caribbean stated that consumers very rarely understand and have control over how their data is collected, stored and used.



Source: UNCTAD, 01/04/2018

5 Australian Government, [Privacy Act 1988](#)  
6 New Zealand Government, [The Privacy Act](#)  
7 APEC, [Cross-Border Privacy Rules \(CBPR\) System](#)  
8 EU-U.S. Privacy Shield

## MOVING FORWARD TO A COHERENT GLOBAL POSITION?

The sheer increase in data protection laws across the world is testament to data protection's rising importance on the global agenda. In spite of this, there is still more that needs to be done. In an ideal world data protection would be harmonised across continents to ensure a more comprehensive and coherent global policy on the fundamental right to personal data protection, especially in the extraterritorial application of data. This would reduce the degree of flexibility with which countries can implement data protection requirements, and reduces confusion when data protection issues arise between countries.

Some countries have already started to do this by aligning with robust data privacy frameworks like the OECD guidelines or GDPR, but these are not widespread. The only non-EU countries that have data protection laws considered adequate by the EU are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US. Australia, New Zealand, Hong Kong, and Japan have modelled their data protection laws off the OECD Guidelines.

So, while the GDPR may be held up as a new gold standard, it could be ambitious to assume that others will reach it any time soon, considering that many countries across the globe are yet to put data protection laws in place or finalise existing draft legislation.

The selection of components of strong online privacy and data protection rights below shows the scale of the challenge for middle and low income countries, particularly where obligations on service providers were complicated by the issue of data control across borders.

- Establishment of state and regional mechanisms that strengthen data protection frameworks such as oversight from independent bodies
- A move away from a patchwork of sector-based regulation towards single legislative dataprotection mandate to protect individuals' privacy
- Mandatory breach notification requirement
- Mandatory fines for non-compliance
- A consent-based model for data protection regulation where data is regulated on the basis of general data protection principles across industry sectors without distinction.
- Data portability which will take into consideration the extraterritorial nature of data collection and transmission
- Data subject rights such as right to be forgotten etc

Consumers International research found that capacity of policy makers, resources for monitoring and enforcement systems and the political climate around national security all made developing frameworks coherent with GDPR or OECD difficult. Additionally, where data is included in trade negotiations, there will be pressure to harmonise down as protection is often seen as a barrier to trade. 9

There was also concern that taking 'legislative shortcuts' such as copying data protection clauses from other countries, may not work as they have different enforcement or market surveillance infrastructure or could even be affected by different cultural norms.<sup>10</sup>

**In 2016, 57% of consumers worldwide reported that they were more concerned about their online privacy than they were in 2014.**

**Outside the EU, very few countries have data privacy frameworks that are aligned with OECD guidelines or GDPR.**

9 Consumers International blog, [Why global e-commerce talks will have wide implications for consumer rights and privacy](#), 2018

10 Consumers International, [Connecting Voices: a role for consumer rights in developing digital society](#), 2017

## KEY FACTS AND FURTHER READING ON GDPR

### What is personal data?

'Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data'. Examples include name and surname, a home address, an email address, etc <sup>11</sup>

### What is data protection?

"Data protection is about protecting any information relating to an identified or identifiable natural (living) person, including names, dates of birth, photographs, video footage, email addresses and telephone numbers. Other information such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered personal data".<sup>12</sup>

Data privacy, or data protection, laws regulate the use of 'personal data' by organisations to protect certain rights of individuals – organisations are not free to use personal data at will.

### Who needs to abide by GDPR?

'A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.'<sup>13</sup>

### References

European Commission: [What is personal data?](#)

UNCTAD: [Data Protection and Privacy Legislation Worldwide](#)

ICO: [Key Definitions](#)

European Data Protection Supervisor: [History of the GDPR](#)

Privacy International: [General Data Protection Regulation \(GDPR\) CI other blog on GDPR](#)

Consumers International: [GDPR: will it be the global standard for data protection?](#)

Consumers International, [Connecting Voices: a role for consumer rights in developing digital society](#), 2017

---

11 EU, [What is personal data?](#)

12 European Data Protection Supervisor, [Data Protection](#)

13 ISO, [Who does the GDPR apply to?](#)