
ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Brazil's GDPR-style DP law is a game-changer

Data Protection Laws are like waiting for a London bus – you wait ages for one and then they all come at once! **Felipe Palhares** and **Robert Bond** of Bristows analyse Brazil's new law.

The EU General Data Protection Regulation applied fully on 25 May 2018 and then there have been similar laws announced in California, Washington State, Kenya, Bahrain, Algeria, Panama, Lebanon, Barbados, Pakistan and many more. South Africa, Russia and Japan and some other countries have updated their laws and lean heavily on GDPR principles and those of Convention 108….and then there is Brazil.

On 14 August 2018, Brazil

*Continued on p.3*

# 'On again, off again' consultation for Canadian policy on data transfers

Canada's privacy protection regime faces pressures for modernisation in light of the GDPR. **Colin Bennett** from the University of Victoria, Canada reports.

It has been an interesting couple of months in the world of Canadian privacy protection policy, which signals some fundamental shifts in strategy and approach by the Office of the Privacy Commissioner of Canada (OPC) and the Canadian federal government.

*Continued on p.5*



Issue 159 **JUNE 2019**

INTERNATIONAL report

ISSUE NO 159 **JUNE 2019**

**PUBLISHER**
**Stewart H Dresner**
stewart.dresner@privacylaws.com

**EDITOR**
**Laura Linkomies**
laura.linkomies@privacylaws.com

**DEPUTY EDITOR**
**Tom Cooper**
tom.cooper@privacylaws.com

**ASIA-PACIFIC EDITOR**
**Professor Graham Greenleaf**
graham@austlii.edu.au

**REPORT SUBSCRIPTIONS**
**K'an Thomas**
kan@privacylaws.com

**CONTRIBUTORS**
**Colin Bennett**
University of Victoria, Canada

**Georgia Skouma**
Deloitte Consulting, Belgium

**Daniel J. Solove**
George Washington University Law School, US

**Robert Bond**
Bristows, UK

**Felipe Palhares**
Palhares Advogados, São Paulo, Brazil

**Elizabeth Coombs**
UN Right to Privacy Taskforce, Malta

**Petra Věžníková**
Squire Patton Boggs, Czech Republic

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
**Tel: +44 (0)20 8868 9200**
**Fax: +44 (0)20 8868 5215**
**Email: info@privacylaws.com**
**Website: www.privacylaws.com**
**Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X



# comment

## Happy Birthday, GDPR

Now, one year since the GDPR became applicable, can we move on to think about other issues, such as e-Privacy? Not quite – while GDPR compliance is an ongoing task, companies have not yet managed to fully adapt to some of its provisions. Read on p.7 which aspects have been the most troublesome for companies.

Individuals have woken up to use their rights – DPAs have received 144,000 queries and complaints since May 2018. Telemarketing, promotional e-mails and video surveillance are among the most complained about issues.

By early June, three EU Member States still had not brought the GDPR into national legislation (p.10). In this issue, we publish a table of the new EU laws, together with the European Economic Area, Jersey, Guernsey and the Isle of Man to help you keep track of the changes.

In Canada, a debate has started whether and how the current law could be amended in light of the GDPR (p.1). In Brazil, the new law, again affected by the GDPR, was adopted in 2018 but will not enter into force until 2020 giving organisations much needed time to put their house in order (p.1). But what will the US response be to the changing international data protection legislative framework? One option could be to expand the Federal Trade Commission's rulemaking powers, Professor Daniel J. Solove says (p.16).

On the international front, the OECD is revising its privacy principles. Read Professor Graham Greenleaf's analysis of whether the revisions are going in the right direction, and what their impact may be (p.18). At the United Nations, the Special Rapporteur on the Right to Privacy has reported to the UN Human Rights Council on 'Privacy and Personality' which includes an interesting analysis by Dr Elizabeth Coombs on whether privacy rights depend on gender (p.24).

We take pride in bringing you news from all over the world, regardless of the size of the jurisdiction. In this issue, we have an interview with the Data Protection Commissioner of Liechtenstein (p.28), and a report on the new law in the Czech Republic (p.26).

Take your last chance to meet 65+ speakers from 15+ countries at *PL&B's* 32nd Annual International Conference, 1-3 July www.privacylaws.com/ac

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

## Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

*Brazil... from p.1*

enacted a new data protection law, usually referred to by the acronym LGPD, which stands for *Lei Geral de Proteção de Dados*. Although the country already had prior legislations that encompassed privacy and data protection provisions such as the Consumer Defence Code, the Freedom of Information Act and the Civil Rights Framework for the Internet, this is the first comprehensive data protection law in Brazil and should be a game-changer, following the steps of the GDPR.

As happened with several pieces of legislation around the world in the wake of the GDPR, the Brazilian law is also very similar to its European counterpart and shares many of the same concepts and stances when it comes to protecting the privacy of individuals. For instance, the definitions of personal data, special categories of personal data, controller and processor are quite a clear match. This does not mean that they are exactly the same or that complying with the GDPR would result in compliance with the Brazilian law in all cases.

## GDPR principles in law

The LGPD carries the same principles as those under the GDPR, although they are divided into ten separate principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and accountability. Besides those that are mirrored from the European law, it also adds one of non-discrimination which prohibits processing of personal data for illicit or abusive discriminatory purposes.

Complying with the LGPD is mandatory in three different scenarios, regardless of where in the world the controller or processor is based or the nationality of the data subjects:

1. Where processing of personal data is carried out in the Brazilian territory.
2. Where processing of personal data is related to the offering of goods or services to data subjects located in the Brazilian territory.
3. Where the personal data being processed was collected in Brazil. This last case of the law's extraterritorial scope could mean an even wider reach than the GDPR.

There are four exceptions where the law does not need to be complied with:

1. Where processing is carried out by a natural person exclusively for personal and non-economic purposes.
2. Where processing is carried out exclusively for journalistic, artistic or academic purposes.
3. Where processing is performed exclusively for purposes of public safety, national defence, State safety or activities of investigation and persecution of criminal offences.
4. Where the personal data originated abroad and is not shared with Brazilian controllers or processors or is subject to international data transfers to a third country other than the one it originated from, and provided that the originating country has an adequate level of data protection.

The LGPD sets forth ten lawful bases for processing personal data:

1. Consent.
2. For compliance with a legal or regulatory obligation of the controller.
3. By the public administration, where necessary for the execution of public policies provided for in contracts or similar instruments.
4. For research, provided it is conducted by a research institution as defined by the law.
5. For the fulfilment of a contract or for preliminary procedures related to a contract, upon request of the data subject.
6. For exercising legal rights in judicial, administrative or arbitration procedures.
7. For the protection of life or physical safety of the data subject or a third party.
8. For health protection, in a procedure carried out by health professionals.
9. Legitimate interests.
10. For credit protection.

Some of these bases are also lawful for processing sensitive personal data, as it is the case with items 1, 2, 3, 4, 6, 7 and 8 above. The Brazilian law also gives emphasis to the processing of personal data of children and teenagers. In Brazil, someone under 12 years old is deemed as child while someone between 12 and 18 years old is deemed as a teenager.

Processing of data related to children and teenagers must always be carried out with their best interests in mind and when processing refers to a child, consent shall be obtained from at least one of the parents or legal guardians. Furthermore, controllers are forbidden from imposing as a condition for the participation of children and teenagers in games or Internet applications the supply of personal data beyond what is strictly necessary for that end. Controllers have an obligation of employing reasonable efforts, according to the technologies available, to confirm that consent was actually given by the parents or legal guardians.

## Data subject rights are present

Data subjects' rights under the Brazilian law follow those set by the GDPR. Individuals have the right to confirm the existence of processing, a right of access, rectification, blockage, deletion, portability, of knowing with which companies and public entities their data was shared, and of revoking consent at any time. Those rights might be exercised in certain circumstances (especially blocking and deletion rights) and should be respected and the data subjects informed. Data subjects also have a right to lodge a complaint both with the Data Protection Authority and with the courts, which means they could be able to recover actual damages or claim moral (non-material) damages related to any non-compliance with the law. This should be treated carefully considering the high levels of litigation that in Brazil and the existence of special courts where individuals can file claims without the need to pay court fees or attorney fees, even in case of defeat.

There is an additional right available to data subjects to request that any decisions taken solely based on the automated processing of their personal data, including profiling, are reviewed by the controller. This have to be done by a natural person, which will certainly increase the resources needed by the controller to respond to such requests. The Data Protection Authority may issue further guidance specifying in which cases the review needs to be carried out by a natural

person and the scenarios where it could be performed by a second run of the same algorithm, according to the size of the controller, the nature and volume of its processing activities.

Fulfilling data subjects' access requests is harder under the LGPD when compared to the GDPR. After receiving a request for access, controllers must respond within 15 days and provide data subjects with a full report on their data which will demonstrate the source of the data, the non-existence of records (if applicable), the purposes of processing and the criteria used for processing. There is no provision in the law that allows an extension to that deadline not even when this could represent a complex request and if the data subject only wants a simple confirmation of whether his personal data is being processed. A response to an access request should be given immediately if possible, through a simplified means.

### Mandatory DPO for all

In order to comply with the accountability requirements, both controllers and processors must keep records of the processing activities. There is no thresholds or exceptions to these requirements, regardless of the number of employees or size of any given company and this could be a heavy burden to small companies with little resources to keep track of everything. The Brazilian law also puts an extra burden on controllers as it makes mandatory for every controller to appoint a data protection officer. It does not matter if you are a massive tech company that processes huge amounts of data or a small bakery that only sells bread to the local neighborhood – right now if you are a controller you need to nominate a DPO in all cases. The law also states that processors might be required to appoint a DPO as well, according to some criteria that will be defined by the Data Protection Authority.

Another aspect that distinguishes the LGPD from the GDPR is the lack of mandatory requirements for conducting data protection impact assessments (DPIA). The Brazilian law states that the Data Protection Authority may request a controller to conduct a DPIA, especially in cases involving the processing of sensitive personal data or processing based on legitimate interests. But it does not make a DPIA mandatory in any case, at least not to private entities. With regard to public entities, the law sets forth that the supervisory authority may request that a DPIA is published. This could be viewed as an obligation to public entities to conduct DPIAs, although there is no explicit indication making this mandatory.

### International data transfers

International transfers of personal data are allowed under almost the same bases as prescribed by the GDPR, which means that they are permitted to jurisdictions considered as adequate or when the controller offers appropriate safeguards such as standard contractual clauses, Binding Corporate Rules, specific contractual clauses, seals, certifications or codes of conduct. All of those instruments must be prior approved by the Data Protection Authority.

Moreover, the LGPD has provided for further situations where international data transfers are also permitted, such as where:

1. A transfer is necessary for international legal cooperation between public entities devoted to intelligence, investigation and prosecution.
2. A transfer is necessary for protecting the life or physical safety of the data subject or third parties.
3. The Data Protection Authority authorizes it.
4. A transfer is a result of a commitment made under international treaties or agreements.
5. A transfer is necessary for the execution of public policies.
6. A transfer is necessary for compliance with legal or regulatory obligations, for the fulfilment of a contract or for the exercise of legal rights in judicial, administrative and arbitration procedures.
7. The data subject explicitly consented after being informed of the international nature of the processing.

> The sanctions established by the Brazilian law are considerably lower than those available under the GDPR.

### Notification

Data breach notification requirements are set at a lower level. Where there is a security incident which might result in either relevant damage to the affected data subjects or a risk to them, both the Data Protection Authority and the affected data subjects must be notified within a reasonable period of time. Considering that a risk will almost always arise out of a data breach, this could be viewed as a requirement for notification in all scenarios.

### Fines

The sanctions established by the Brazilian law are considerably lower than those available under the GDPR. Controllers and processor may receive a fine of up to 2% of the turnover of the company, group or conglomerate in Brazil in its last financial year, excluding taxes, limited to a maximum amount of 50 million Brazilian reais per infraction (around €10 million). This monetary penalty is fairly low, especially taking into account that to receive the maximum fine of 50 million reais a company would need to have an annual turnover of at least 2.5 billion reais, which is large by Brazil's standards and should limit this large penalty to a few companies, mainly banks that do business in the country. Other sanctions include a warning with a deadline to make corrective measures, making the infringement public, and blocking or deleting the personal data related to an infraction.

### Status of DPA still unclear

To a large extent, the Brazilian legislative framework still needs further regulations. There are several provisions of the LGPD that expressly make reference to a regulation or

 

guidance to be issued by the Brazilian Data Protection Authority or that state that the DPA could alter some requirements of the law, such as when a DPO really needs to be appointed and the cases where one would not need to be nominated. This could be a problematic issue considering that Brazil still does not have a functioning Data Protection Authority.

At the end of last year, the country's president at the time, Michel Temer, issued Executive Order n. 869/2018 that created the Brazilian Data Protection Authority and altered some provisions of the LGPD. Right now, though, the Authority is an empty shell – it has not been staffed or structured yet, mainly because there was no clear indication if the Executive Order that created it would actually stand. According to Brazil's legislative process, an Executive Order is deemed to have the same effects as a valid law since its issuance date but it needs to be approved by Congress and converted into law within 120 days or it becomes null and void. On 29 May 2019, the Brazilian Congress approved an amended version of the Executive Order. This final text of the law still needs to be sanctioned by the President, who is entitled to veto all or parts of the amended Executive Order, and only after that Brazil's DPA should be actually structured and start functioning.

There is one thing, however, that is most likely certain now: the LGPD will probably come into effect on 16 August 2020. There were some doubts about the effective date of the law because of the Executive Order n. 869/2018. Although the LGPD was enacted on 14 August 2018, it had a grace period of 18 months, which means it should come into effect on 16 February 2020. However, the Executive Order n. 869/2018 extended the grace period of the law to 24 months, resulting in transferring its effective date to 16 August 2020. As the Executive Order has been approved by Congress and now only awaits the President's sanction – and considering that the provision that extended the grace period of the law is not expected to be vetoed by President Bolsonaro – companies have another six months to enhance their internal policies and procedures and to get ready for compliance with the LGPD.

**AUTHORS**

Felipe Palhares is a Brazilian attorney and Robert Bond is a Partner at Bristows, UK.
Emails: robert.bond@bristows.com
felipe@palharesadvogados.com

# Join the Privacy Laws & Business community

## Six issues published annually

### PL&B's International Report will help you to:

**Stay informed of data protection legislative developments in 125+ countries.**

**Learn from others' experience through case studies and analysis.**

**Incorporate compliance solutions into your business strategy.**

**Find out about future regulatory plans.**

**Understand laws, regulations, court and tribunal decisions and what they will mean to you.**

**Be alert to future privacy and data protection law issues that will affect your organisation's compliance.**

## Included in your subscription:

**1. Online search functionality**
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

**2. Electronic Access**
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

**3. E-Mail Updates**
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

**4. Back Issues**
Access all the *PL&B International Report* back issues since 1987.

**5. Special Reports**
Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

**6. Events Documentation**
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

**7. Helpline Enquiry Service**
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

## To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**"

## Subscription Fees

**Single User Access**

*International Reports* **£560 + VAT***
*UK Reports* **£450 + VAT***
*UK & International Reports* **£900 + VAT***
* VAT only applies to UK based subscribers

**Multi User Access**

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

**Subscription Discounts**

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

**International Postage (outside UK):**

Individual International or UK Edition
Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions
Rest of Europe = £50, Outside Europe = £70

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

*Privacy Laws & Business* also publishes the United Kingdom Report.
**www.privacylaws.com/UK**