ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EU DP Regulation now faces the challenge of consistency

Nearly half way between the adoption of the EU Data Protection Regulation and May 2018 when it applies, concerns include national variations and international data transfers. **Laura Linkomies** reports.

The EU Commission is now actively engaging with EU Member States to ensure that national exemptions will not be too severe in the areas where flexibility is possible. One of the most advanced countries in terms of implementation is Germany, and there are several variations from the GDPR in the draft Bill (see p.35 in this issue). *Karolina Mojzesowicz*, Deputy Head, Data Protection Unit, EU DG

Continued on p.3

Indonesia enacts Personal Data Regulation

The Regulation is the first comprehensive privacy law in Indonesia, but lacks effective enforcement mechanisms. By **Andin Aditya Rahman**.

At the twilight of 2016, there were considerable developments in Indonesia's privacy law framework. Firstly, Indonesia's parliament enacted Law No. 19 of 2016 (EIT Law Amendment) on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law), introducing the right to be forgotten to the Indonesian legal framework. This is a concept pioneered in Europe which

Continued on p.6

Issue 145 **February 2017**

Indonesia... from p.1

is essentially the right to request personal information be removed from the Internet. Secondly, Minister of Communication and Information Technology issued Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (PDP Regulation), the first comprehensive regulation that governs provisions related to personal data protection in Indonesia, albeit limited to those that are in electronic form. It is worth noting that the PDP Regulation is a ministerial-level regulation that implements a mandate from Government Regulation No. 82 of 2012 on Implementation of Electronic Transactions and Systems (Electronic Transactions Regulation).

Applicability of the EIT Law Amendment and PDP

In order to understand the applicability of both the EIT Law Amendment and PDP Regulation, it is important to first elaborate what is meant by an "electronic system provider", the main subject of the EIT Law Amendment and PDP Regulation.

An "electronic system provider" is defined the same under the EIT Law Amendment and PDP Regulation, namely "any person, state administrator, business entity, and public entity that provides, manages, and/or operates an electronic system, either individually or collectively to the users of the electronic system for their own interests and/or for the interests of others".[1]

Although the following understanding is untested, because of the generality of the definition of electronic system providers, the applicability of the EIT Law Amendment and PDP Regulation also includes those that provide, manage, or operate electronic systems for external and internal users. As an example, an office that operates an internal network for employees will be considered as an electronic system provider pursuant to the EIT Law Amendment and PDP Regulation.

Most Indonesian government institutions use electronic systems to manage personal data, while the majority of business entities in Indonesia still use traditional methods (manual) in managing personal data. However, the major players have mostly migrated to use electronic systems.

The nature of the requirements and obligations in relation to personal data protection under the EIT Law Amendment and PDP Regulation are characteristically only appropriate to electronic system providers that manage the personal data of clients and customers. This is because of the broad definition of what is considered as an electronic system provider under the EIT Law Amendment and PDP Regulation. People who manage personal data only for internal purposes (for example, the personal data of employees), are forced to comply with the EIT Law Amendment and PDP Regulation, which is in some cases overly burdensome.

In addition to that, the EIT Law along with the EIT Law Amendment has cross-border applicability, meaning that offshore parties conducting activities in Indonesia are subject to the EIT Law as amended by the EIT Law Amendment.

As a derivative regulation of the EIT Law (as amended by the EIT Law Amendment), the PDP Regulation also has the same cross-border applicability.[2]

The Right To Be Forgotten Under The EIT Law

Even with the good intention to dynamically update Indonesia's main technology legislation to contemporary developments to Europe's privacy law, the addition of the right to be forgotten under the EIT Law Amendment seems to have been made haphazardly in a few simple paragraphs. The first of these simply states: "every electronic system provider must dispose of electronic information and/or electronic documents that are not relevant which are under their control upon the request from the relevant person based on a court order".[3]

The main issue with this provision is that the Indonesian courts are placed in charge to grant or not to grant a request for a right to be forgotten court order. Notwithstanding the Indonesian court system being plagued with corruption, with no previous precedent, the Indonesian courts will for the moment decide on their own the right to be forgotten requests that are deemed worthy to be granted without any sort of guidelines to maintain uniformity.

The second paragraph obligates electronic system providers to establish a mechanism to be implemented upon receiving a right to be forgotten request.[4] The primary problem with this obligation is similar to that with the above, there are no general format or guidelines provided for electronic system providers to follow in establishing such mechanism.

The final paragraph added to the EIT Law Amendment is the mandate for a government regulation to be issued to further stipulate these provisions on the right to be forgotten.[5] This may be the solution to the above issues, providing the necessary guidelines for courts to issue orders for right to be forgotten requests and the general format for electronic system providers to establish the mechanism to fulfil right to be forgotten requests. However, in the meantime, both Indonesian courts and electronic system providers are forced to guess the intentions of the legislature when adding these right to be forgotten clauses to the EIT Law Amendment.

New Clearer Definition of Personal Data in the PDP Regulation: The PDP Regulation is applicable to electronic system providers that handle personal data, which is defined as "certain data related to an individual of which the accuracy and confidentiality is kept, maintained, and protected" which is the same definition provided under the Electronic Transactions Regulation and Law No. 23 of 2006 on Citizen Administration, as amended by Law No. 24 of 2013 (Citizen Administration Law).[6] The PDP Regulation defines further "certain data related to an individual" in the said definition, namely "any information that is true and valid, which is inherent can be identified, whether directly or indirectly, with each respective individual which is used in accordance with the provisions of laws and regulations".[7] This further elaboration provides light on what is actually referred to as

"personal data" under Indonesian law, which previous to the PDP Regulation has been only vaguely defined. With this new elaborated definition, any information that is inherent to and can be used to identify a specific person is considered as personal data. A simple example is the name of a person, which without a doubt is inherent and can be used to identify a person with the name in question.[8]

Actions Related to Personal Data under the PDP: In accordance with the said definition, the PDP Regulation is particularly relevant to electronic system providers who conduct the following actions related to personal data in their business activities in Indonesia (collectively referred to as "Actions Related to Personal Data"):

1. Acquisition and collection;
2. Processing and analysis;
3. Storage;
4. Display, announcement, transfer, dissemination, and/or providing access to; and
5. Disposal.

Consent under the PDP: The PDP Regulation obligates anyone undertaking Actions Related to Personal Data to have obtained the prior consent of the person who is the subject of such personal data. In order to secure such consent, the electronic system provider must provide a standard form in Bahasa Indonesia to be agreed by the personal data owner in question ("Consent Standard Form").[9] Note that even though the Consent Standard Form must be provided in Bahasa Indonesia, the PDP Regulation does not preclude the provision of the Consent Standard Form in other languages along with the version of the Consent Standard Form in Bahasa Indonesia. The Consent Standard Form will primarily set out:

1. The types of personal data that will be acquired and obtained by the electronic system provider;
2. The purposes of the Actions Related to Personal Data; and
3. Details on the Actions Related to Personal Data that will be undertaken.

Moreover, the Consent Standard Form is to incorporate the rights of the personal data owner [individual] pursuant to the PDP Regulation, covering the right to:[10]

1. Have access to and be provided with the opportunity to modify or update his/her personal data;
2. Request a history of his/her personal data that have been acquired or obtained by the electronic system provider;
3. Request for the disposal of his/her personal data; and
4. Determine certain of his/her personal data to be confidential (therefore, cannot be disclosed or shared with third parties).[11]

If the personal data owner is a minor, the Consent Standard Form must be agreed to by his/her parent or guardian.[12] Pursuant to the Indonesian Civil Code, any person under 21 years of age is considered as a minor.[13]

Obligations of Electronic System Providers under PDP

Electronic system providers are subject to a number of obligations and requirements under the PDP Regulation, including to:

1. Secure certification for their electronic systems;
2. Have an internal policy on personal data protection;
3. Establish security procedures and facilities for their electronic systems.

Electronic System Certification Obligation: Electronic systems used for Actions Related to Personal Data must be certified in accordance with the Electronic Transactions Regulation, specifically referring to the Electronic System Worthiness Certification. According to the Electronic Transactions Regulation, the Electronic System Worthiness Certification is a series of processes of inspections and tests that are conducted by an authorized and competent institution to ensure that an electronic system is functioning properly.[14] Electronic System Worthiness Certificates can be issued by the Minister of Communication and Information Technology (MOCIT) or institutions appointed by the MOCIT.[15]

Internal policy on personal data protection: Electronic system providers that carry out Actions Related to Personal Data are required to have in place an internal policy on personal data protection to undertake Actions Related to Personal Data.[16]

The main goal of having such internal policy on personal data protection is to prevent personal data breaches, which must be incorporated with:[17]

1. Efforts to improve the awareness of staff to provide protection for the personal data being managed by the electronic system provider; and
2. Training staff on the prevention of personal data protection failure.

Electronic System Security procedures and facilities: Electronic system providers are required to store personal data in accordance with provisions on electronic system security procedures and facilities under prevailing statutory laws and regulations, specifically under the Electronic Transactions Regulation.[18]

Electronic system providers are required to:[19]

1. Provide an audited track record of activities related to the electronic systems for purposes of law enforcement, dispute settlement, verification, inspection, and other forms of mandatory examinations;
2. Establish security measures for the components of the electronic systems;
3. Implement prevention and mitigation procedures and systems for threats and attacks that may cause disruptions, failures, and damages;
4. Ensure the confidentiality, integrity, authenticity, accessibility, availability, and traceability of electronic information and/or documents in their electronic systems;
5. Ensure electronic systems to be functioning properly according to their respective purposes, with due consideration to the interoperability and compatibility of the electronic systems; and
6. Ensure the employees of the electronic system provider fulfil their obligation to secure and protect the facilities and infrastructures of the electronic systems, which includes employing and training personnel that are in charge and responsible for the security and protection of the facilities and infrastructures of the electronic systems.

Other obligations:

1. Notify personal data owners (individuals) in case of any leak of their personal data;[20]

2. Make available contact information that is easily accessible for personal data owners to inquire regarding their personal data;[21]
3. Fulfil data and information requests from the MOCIT for the purpose of personal data protection;[22]
4. Operate electronic systems that have interoperable[23] and compatible[24] capabilities, and use legal software;[25]
5. store personal data in the form of encrypted data;[26] and
6. Place in Indonesia the data centres and disaster recovery centres that provide public services.[27]

Grace period: The PDP Regulation provides a grace period of two years for electronic system providers to fulfil the abovementioned obligations, as well as to adjust their activities with the PDP Regulation.[28]

Other key provisions in the PDP Regulation

Retention period: The mandatory minimum retention period for personal data under the PDP Regulation is at least five years, unless provided otherwise by another prevailing statutory regulation. This mandatory minimum retention period is calculated from when the personal data owner ceases to be a user of the electronic system provider.[29] After the mandatory retention period is passed, the personal data may be erased unless it is still to be used by the electronic system provider in accordance with the agreed Consent Standard Form.[30]

Any claim of the right to be forgotten based on a court order pursuant to the EIT Law Amendment will automatically override this mandatory minimum retention period as the EIT Law Amendment stands higher in the Indonesian legal hierarchy. As such, if a claim for the right to be forgotten based on a court order is filed for data that has not passed the mandatory minimum retention period as elaborated above, such data will be required to be erased.

Overseas transfer of personal data: Any overseas transfer conducted by an electronic system administrator must be reported to the MOCIT. The report must be submitted prior and after the overseas personal data transfer. The report submitted prior to the overseas personal data transfer must contain information on the country of destination, recipient, date, and reason or purpose of the overseas personal data transfer. The report submitted after the overseas personal data transfer will simply elaborate on the implementation of the overseas personal data transfer.[31]

REFERENCES

1 In Bahasa Indonesia: "Setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain". See: Article 1 number 6a of the EIT Law Amendment and Article 1 number 6 of the PDP Regulation.
2 EIT Law, Article 2.
3 In Bahasa Indonesia: "Setiap penyelenggara sistem elektronik wajib menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan". See: Article 26 paragraph (3) of the PDP Regulation.
4 EIT Law Amendment, Article 26 paragraph (4).
5 EIT Law Amendment, Article 26 paragraph (5).
6 In Bahasa Indonesia: "Data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya". See: Article 1 number 1 of the PDP Regulation.
7 In Bahasa Indonesia: "Setiap setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan". See: Article 1 number 1 of the PDP Regulation.
8 Assegaf Hamzah & Partners, "Personal Data Protection Regime Gets Boost with New Regulation," 29 December 2016. Retrieved 3 February 2017 from www.ahp.co.id/client-update-29-december-2016
9 PDP Regulation, Article 6.
10 PDP Regulation, Article 26.
11 PDP Regulation, Article 9 paragraph (3).
12 PDP Regulation, Article 37 paragraph (1).
13 As a Consent Standard Form is considered as an agreement or contract, the Indonesian Civil Code shall prevail even though other prevailing Indonesian statutory laws and regulations stipulate otherwise on the age which is considered as a minor. See: Article 330 of the Indonesian Civil Code.
14 Electronic Transactions Regulation, Article 1 number 12.
15 Electronic Transactions Regulation, Article 31 paragraph (1) and Article 32 paragraph (1).
16 PDP Regulation, Article 5 paragraph (1).
17 PDP Regulation, Article 5 paragraph (4).
18 PDP Regulation, Article 18.
19 Electronic Transactions Regulation, Article 18, Article 19, Article 20 paragraphs (1) and (2), Article 22 paragraph (1), Article 23, and Article 28.
20 PDP Regulation, Article 28 letter c.
21 PDP Regulation, Article 28 letter i.
22 PDP Regulation, Article 35 paragraphs (3) and (4).
23 Interoperability refers to the capability of different Electronic Systems to operate in an integrated manner. See: Article 11 paragraph (3) of the PDP Regulation.
24 Compatibility refers to the suitability of one Electronic System with other Electronic Systems. See: Article 11 paragraph (4) of the PDP Regulation.
25 PDP Regulation, Article 11.
26 PDP Regulation, Article 15 paragraph (2).
27 For an elaboration on what is considered as providing public services in Indonesia, see: Scott Livingston, Graham Greenleaf, "Data localisation in China and other APEC jurisdictions" *Privacy Laws & Business International Report*, Issue No. 143, October 2016, p.22.
28 PDP Regulation, Article 38.
29 PDP Regulation, Article 15 paragraphs (1) and (3), and Article 16.
30 PDP Regulation, Article 19.
31 PDP Regulation, Article 22 paragraph (2).
32 PDP Regulation, Article 28 letter c and Article 29 paragraphs (1) and (3).
33 PDP Regulation, Article 31.
34 PDP Regulation, Article 32.
35 PDP Regulation, Article 36 paragraph (1) and paragraph (2).
36 See: Andin Aditya Rahman, "Indonesia introduces a comprehensive privacy Bill," Privacy Laws & Business International Report, Issue No. 139, February 2016; Zacky Zainal Husein, Andin Aditya Rahman, "Developments in Indonesia's Privacy Rules," *Data Privacy Asia Newsletter*, 22 March 2016. Retrieved 8 February 2017 from newsletter.dataprivacyasia.com/march/2016/3/22/developments-in-indonesias-privacy-rules

Legal exposures for non-compliance: As elaborated above, electronic system providers that undertake any Action Related to Personal Data are required to notify personal data owners [individuals] in case of any leak of their personal data. Failing to do so or delay in doing so (written notification is to be delivered within 14 days of the personal data leak), the personal data owners will have the right to file a formal complaint with the Minister of Communication against the electronic system provider in question.[32] A formal complaint can only be filed with the Minister of Communication against the electronic system provider in question for failure or delay in notifying the personal data owner regarding any leak of his/her personal and does not apply to any other form of non-compliance with the PDP Regulation by the same electronic system provider.

The formal complaint will initiate mediation between the electronic system provider and personal data owner by an official or team appointed by the MOCIT to resolve the dispute. During the mediation, the official or team assigned may recommend to the MOCIT the imposition of administrative sanctions on the electronic system provider involved.[33] If the mediation fails to produce an amicable settlement between the electronic system provider and personal data owner, the personal data owner may file a civil lawsuit against the electronic system provider.[34]

In addition to the potential exposure to formal complaints and civil lawsuits, non-compliance with the PDP Regulation may be subject to administrative sanctions, including verbal and written warnings, temporary suspension of business activities, and public disclosure of the violation. There are no financial penalties included as a form of an administrative sanction, which makes enforcement through the imposition of such sanctions rather questionable. Nevertheless, the procedures for imposing these administrative sanctions will be stipulated in detail under a separate regulation to be issued by the MOCIT.[35]

Conclusion

One drawback of the PDP Regulation, despite being the first comprehensive privacy law in Indonesia, is the lack of means for enforcement. Personal data owners [individuals] are only enabled to submit formal complaints against electronic system providers for personal data leaks (rather than for any non-compliance with the PDP Regulation) and the intention of the Minister of Communication and Information Technology in omitting administrative fines for non-compliance is certainly questionable. However, a lawsuit for any unlawful use of personal data can still be made based on the EIT Law (as amended by the EIT Law Amendment), which is at least a weak form of enforcement.

On the positive side, the PDP Regulation finally provides an accurate definition on what is meant by personal data for Indonesia's privacy legal framework, which have been vague for more than 10 years since it was first defined under the Citizen Administration Law in 2006, and addresses most critical issues for personal data protection. The PDP Regulation does however have a limited scope of applicability, which is personal data in electronic form. This is expected to be addressed by a more general legislation on personal data protection that is in the pipeline in the Indonesian legislature, which will cover personal data in both electronic and traditional forms.[36]

AUTHOR AND INFORMATION

Andin Aditya Rahman is an Associate at Assegaf Hamzah & Partners. The views and opinions expressed in this article are his own. The information contained in this article are for general information only and is not intended to be taken as formal legal advice or opinion, or replace a formal consultation with a legal counsel. Credit also goes to Graham Greenleaf for his editorial inputs and comments on the PDP Regulation and privacy law in general.

INTERNATIONAL report

ISSUE NO 145 **FEBRUARY 2017**

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
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Andin Aditya Rahman
Assegaf Hamzah & Partners, Indonesia

Tim Hickman, Matthias Goetz and Chris Ewing
White & Case LLP UK

Dr Detlev Gabel
White & Case LLP Germany

Edward Hasbrouck
The Identity Project, US

Jim Halpert and Michelle Anderson
DLA Piper, US

Publisher's note: The 1987 – 2004 editions of this publication are freely available at:
www.worldlii.org/int/journals/PLBIRp/

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

More laws, more awareness

This 30th Anniversary February edition includes a comprehensive table of 120 privacy laws and 31 proposed laws worldwide (p.14). While more and more laws are adopted outside Europe, the influence of the EU Data Protection Directive, and indeed the EU Data Protection Regulation (GDPR), can be seen. Just as we were going to print, Argentina issued a draft Bill to update its existing law to be more in line with the latter (p.11). Indonesia has already amended its law to make it comprehensive (p.1).

In Europe, all efforts are now on national implementation of the GDPR. The EU Commission is worried that national emphasis and use of available derogations somewhat erode the goal of harmonisation (p.1). Germany has an advanced draft, which includes several points that differ from the GDPR text, while the Netherlands is looking for a more mainstream adoption of the provisions (p.35). Another urgent topic on the EU agenda is the revision of privacy rules for the telecoms sector – their scope is being extended and this brings additional challenges for business (p.27).

The need for Data Protection Officers (DPOs) will increase in the future in the EU. DPOs please note that all *PL&B* events offer Continuing Professional Development (CPD) points – for example, 18 CPD hours at *Promoting Privacy with Innovation*, our 30th Anniversary International Conference in Cambridge, 3-5 July, at St. John's College, Cambridge. A list of 35 confirmed speakers is at www.privacylaws.com/annualconference from where you can click through to the registration page.

At last month's CPDP conference in Brussels, there was much talk about adequacy and the EU-US Privacy Shield. EU Commissioner for Justice, Věra Jourová, announced that the EU is monitoring developments closely and that she will visit the US this spring to discuss the working of the Shield with US counterparts (p.5). We return to this issue at the Cambridge conference, where speakers from the European Commission and the US will reveal the latest state of play.

In the US, the cybersecurity framework is being revised (p.29). Much attention has been paid to President Donald Trump's executive order threatening privacy rights of non-US citizens (p.34).

Finally, we return to the Court of Justice of the European Union decision on IP addresses. They are personal data in many circumstances – but were the right questions asked, and will the GDPR change the outcome, our correspondents ask (p.32)?

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.

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 100+ 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 100+ 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, Chief Privacy Officer, BT Group, UK**"

Subscription Fees

Single User Access

International Edition **£550 + VAT***

UK Edition **£440 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

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