25 YEARS
PL&B ANNIVERSARY
1987-2012

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

What role for EU and international policy makers in ensuring global interoperability?

A report by Stewart Dresner on session four of Forum Europe's 3rd Annual Data Protection and Privacy Conference, Brussels 4 December 2012

Chair and Introduction

Stewart Dresner, Chief Executive, Privacy Laws & Business

Scope of interoperability: The word interoperability suggests the model of making a telephone call. You can make a telephone call from any telephone number to any other telephone number in the world, as the telecommunications systems in every country work with each other. On a smaller scale, interoperability works as a technical standard within the North Atlantic Treaty Organisation (NATO) so that military equipment is manufactured to the same technical specifications. In this context interoperability means that, in principle, bullets manufactured in one country will be compatible with guns made in another member country.

In the context of privacy/data protection, ensuring interoperability of laws or even standards, as suggested by the title of this session is clearly over-optimistic. This session should be titled *What role for EU and international policy makers in encouraging the trend towards global interoperability?* and we will conduct this discussion on this basis. In practice, is data protection interoperability a meaningful and achievable goal in the next five years?

Is "interoperability" a mirage or a realistic goal? If one aims too high, then it will not happen because privacy or data protection is too diffuse a goal. If one aims too low, then it will be more rhetoric than a meaningful concept. What should be the aim for EU and other policy makers?

PL&B research, published in February 2012, showed 89 national

Continued on p.2

SPECIAL REPORT **January 2013**

CONTENTS

This *Privacy Laws & Business* Special Report draws on contributions to session four of Forum Europe's 3rd Annual Data Protection and Privacy Conference in Brussels on 4 December 2012.
PL&B covers interoperability and related issues of international transfers of personal data in its *International Report*, annual conferences and roundtables with national Data Protection Authorities.

INTERNATIONAL report

SPECIAL REPORT **JANUARY 2013**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

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

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

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 and United Kingdom Reports* are each produced six times a year and are 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

... from p.1

privacy laws around the world and growing (nearly half of the 193 member states of the UN in 2011) [1]

Now more national privacy laws have been adopted. Privacy laws are diverse even in Europe, despite the 1995 EU Data Protection Directive which laid down a common model. There are far more differences around the world:

1. Scope, such as sectors covered
2. Supervisory authorities at national/local/sectoral levels
3. Potential for, and actual importance of, sectoral initiatives
4. Role for trust marks and "accountability agents" such as data protection law compliance auditors
5. Context of rule of law, democratic rights, and effectiveness of the national data protection law in practice.

A Euro-centric perspective is based on fundamental human rights. At first, this focus was driven by the Council of Europe now revising its data protection law Convention 108 with active participation of the EU. Company perspectives are based on ensuring uninterrupted transfers of personal data around the world at minimum cost with minimum disruption to provide goods and services for customers and other users of the data. Consumers want both legal protection of their personal data and also international services provided by companies.

REFERENCES

1 See www.privacylaws.com/Publications/special_reports/

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.

Peter Hustinx, European Data Protection Supervisor

The following is a transcript of **Peter Hustinx's** presentation also available on his organisation's website[1].

Stewart Dresner, the moderator of this panel, has simplified our task today by suggesting that we should be looking at ways to "encourage the trend towards global interoperability" and not necessarily at ways of ensuring it. This signals that there is a problem with the term.

Indeed: "interoperability" sounds as something attractive and desirable, but what works in practice with information technology, does not always work in the same way if we speak about interoperability of legal systems. In fact, interoperability in this context covers a wide variety of phenomena, but roughly speaking implies that what has been done well - or perhaps not so well - in one jurisdiction should have some effect in other jurisdictions, and generally that there should be certain ways of doing things well that work for most jurisdictions. That is obviously a worthy goal, but not necessarily one that is easy to reach.

So let me suggest that there are some factors that may help in this process. The first one is that there is now already a growing convergence of data protection principles and practices around the world. It would not be difficult to point at the differences among the growing number of privacy and data protection laws around the world. At the same time, the most striking and welcome fact is that there is also a growing consensus about the core principles and features of those laws.

Not only the EU, but also the Council of Europe and the OECD are currently reviewing and reinforcing their privacy frameworks. It is very likely that when this work has been completed, this consensus and convergence will be even more visible in the results. This will certainly have a global impact. By the way, the Council of Europe's Convention 108 will soon have its first accessions from Latin-America, where data protection laws are now also spreading.

However, we will never end up with full harmonisation across the globe. A certain degree of diversity is unavoidable and even desirable, and will always remain. Truly global standards are therefore of relative importance in this field. In other words: a United Nations approved Convention on Data Protection is not a precondition for global interoperability. I strongly believe that we are able to make quite meaningful progress in other more practical ways.

A second important factor is that there is now also a growing practice of cooperation among data protection authorities in relevant jurisdictions - both in Europe and in other continents - which can give considerable weight to more global privacy practices. By way of example, let me say that since a few years, we have a Global Privacy Enforcement Network (GPEN) where the US Federal Trade Commission is playing a very active role and is working together with supervisory authorities in Europe, Canada and other APEC countries. The FTC has also shown that it is ready to take action under US law against companies that are misbehaving in the European market. This is obviously relevant, also in view of the fact that some major Internet companies are US based and active around the world.

> "Adequacy" is not a political test or a "beauty" test basically aiming at whether a third country's law is sufficiently close to a European data protection law.

At the most recent International Conference of Data Protection Commissioners in Uruguay, some time was devoted to further structuring and streamlining this international cooperation. Canadian and UK colleagues are playing a leading role in this context. Several authorities are also entering into bilateral agreements to allow closer cooperation in enforcement. This is another signal of a positive development towards more global interoperability.

Against this background, let me say that the adequacy principle as developed in chapter V of the proposed General Data Protection Regulation, including the use of specific instruments such as binding corporate rules (BCR), is a much greater contribution to more global privacy and interoperability than is currently widely recognised. Let me explain this on two levels: the adequacy principle itself and the instruments of delivering adequacy where it does not exist. First, it should not be forgotten that the concept of an "adequate level of protection" set out in Article 25 of Directive 95/46/EC was primarily designed as a functional concept in order to allow meaningful data exchange with third countries: subject to adequate protection, but not necessarily fully equivalent with the level of protection within the EU. This approach will be even more required, if the proposed Regulation is adopted which will ensure an even greater consistency of data protection within the EU.

In other words: "adequacy" is not a political test or a "beauty" test basically aiming at whether a third country's law is sufficiently close to a European data protection law. Instead, from the very beginning[2], it has been based on two pillars: content and procedural or enforcement mechanisms. The first requirement covers certain key data protection principles that should be embodied in the third country's

framework, and the second requirement looks at available mechanisms to deliver a good level of compliance, to provide support and help to individual data subjects and to provide appropriate redress to injured parties where rules have not been complied with. This approach has been followed in all adequacy decisions adopted so far by the European Commission.

It is true that the current list of adequacy decisions is not impressive. However - apart from the fact that certain countries found adequate in the past (Hungary), are now part of the EU - the list is growing: Israel and Uruguay were added recently, and New Zealand will follow soon [Stewart Dresner: accepted formally later in December 2012]. It is also likely that the list will grow even faster in the future. The proposed Regulation has provided for more flexibility by specifically allowing adequacy decisions for a territory or a processing sector within a third country, and by introducing the possibility of an adequacy finding for an international organisation. The Commission has also committed to pursuing adequacy more actively.

It was interesting to hear US Ambassador to the European Union, William Kennard, this morning in his keynote, not criticising the adequacy principle as such, but arguing that the US should be found adequate on the basis of its current privacy laws and practices. Although this may have been overstated, I would not exclude that - if the Obama White Paper's Privacy Bill of Rights is made binding and delivered in practice - such a decision might follow in due course.

On the second level - instruments to deliver adequacy where it does not exist - the proposed Regulation also brings interesting innovations. The most important one is the more prominent place for binding corporate rules (BCR). This instrument has now been regulated explicitly and it will require approval by one DPA only, in accordance with the consistency mechanism set out in the Regulation in order to ensure consistency across the EU. The instrument of BCR will also be available for processors [Stewart Dresner: from 1st January 2013], which is potentially also highly relevant in the context of cloud computing. Further innovation will no doubt follow in due course, when the number of BCR will increase or otherwise. By way of example, let me just mention that the WP29 is looking into potential convergence with the system of Cross Border Privacy Rules (CBPR) developed in APEC. In short, would it be possible to envisage a system of "certification" of the same BCR under both EU and APEC rules? This will soon [Stewart Dresner: late January and early February 2013] be discussed at a joint meeting in Djakarta.

Let me come back to my starting point. Interoperability is not an easy concept, but we are in fact making good progress in delivering it in practice, in a step by step process. The adoption of new legal frameworks at both sides of the Atlantic would be very helpful to this process. It is also clear to me that the instrument of BCR is a very powerful tool in helping to promote and ensure good privacy practices at a global scale. I am quite confident that we will see important and decisive steps ahead along this line in the next five years. This will be to the benefit of all citizens and businesses in an increasingly globalising world.

REFERENCES

1 www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-12-04_Forum_Europe_EN.pdf
2 See WP29 Working Document "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), adopted on 24 July 1998.

Ruth Cullinane, EMEA Data Protection Officer, Dell, Brussels

Ruth Cullinane said that Dell is a global organisation whose customers want its services to work throughout the world. Therefore, the company needs to apply global standards to its products and services. This also applies to the data protection and privacy issues. Dell has created a policy and compliance program for how it manages personal data within its global organisation by looking at the various regimes around the world and focusing on the key principles

Therefore it is key for Dell that regulators recognise that new technologies bring new realities and work and co-operate with each other in creating common standards which address new risks. "We need the European regulators to recognise that it is no longer possible to tie personal data to a specific geography. Standard controls and principles need to apply globally and those standards need to be consistent across regions and countries."

"The Data Protection Authorities have a chance now to build regulation that fits today's reality of how personal data moves seamlessly across geographical boundaries." Key concepts, such as the internet and cloud computing, mean that data flows cannot be tied to a single geography.

"Although the EU is often seen as the global leader in privacy legislation, companies want the EU regulators to be realistic in what can be achieved. There is now a chance to learn from other countries who have also implemented their own laws. For example, we can learn from the US what does and does not work in regard to regulating data breach notification, such as the negative result of notification fatigue and the cost of notification to business."

Thomas Boué, Director Government Affairs, EMEA, Business Software Alliance

The following is based on notes provided by **Thomas Boué**

It is essential to aim for global interoperability of data privacy rules in order to support the free flow of data within and beyond European borders[1] . This is especially true in an era of cloud computing, where the real benefits of the cloud are to be realized by moving data on a global scale.

A European framework that does not align with privacy rules outside the EU will create barriers to market access for companies outside Europe who want to provide valuable and innovative services to European end users. It will also inhibit the competitiveness of European service providers if they cannot leverage the global scope and nature of the cloud, insofar as they are collecting, processing and storing European data.

Collaboration and bilateral/multilateral dialogues are the way forward to achieve a global, cloud-ready privacy framework.

The critical point is that Europe's data protection rules must not, deliberately or inadvertently, prevent companies from offering their services around the world, or deprive European citizens of the opportunity to obtain these services.

The Business Software Alliance (BSA's) member companies operate in a truly global capacity and can attest to the benefits that can be realised by utilizing resources on a global scale. This is especially true in an era of cloud computing where interaction and information exchange is increasingly taking place in a virtualized environment. The geographical location of users and services is becoming less and less relevant.

The current EU Data Protection Regulation outlines a set of very specific rules for how European data must be treated within and beyond EU borders. It's a framework that is inward-looking and overly prescriptive, and frankly, it fails to consider the global nature of the digital economy.

If European policymakers go down a road of establishing rules for Europe that are not in keeping with those outside the EU, the geographical boundaries of the single market are going to close in very quickly. It will create barriers to market access for companies outside the EU who want to provide valuable and innovative services to European enterprises and end users. That means less choice for European citizens and businesses. And, it will inhibit the competitiveness of European service providers if they cannot leverage the truly global scope and nature of the cloud, insofar as they are collecting, processing, and storing European data.

While I don't assert that a single set of rules would apply around the world, policymakers here and abroad must recognize the importance of global markets for data services. They need to set achievable goals for data privacy and security, while leaving "breathing room" for how those goals can be achieved.

For example, consider the adequacy mechanism which is how the EU currently assesses whether countries' legal frameworks meet European expectations for data protection.

As it stands, very few countries have been found adequate. So far, only a few jurisdictions (such as Argentina, Canada, Guernsey, Isle of Man, Israel and Switzerland and in December, New Zealand,) have qualified, with the US partially covered by the Safe Harbour Agreement. One difficulty in the adequacy process is an apparent focus on the existence of formal rules rather than an assessment of the actual, real-world protections extended to personal data. In any case, other countries which have an established privacy framework should be rapidly assessed.

Keep in mind that the fastest-growing technology markets are actually emerging markets outside the EU. That's where the greatest opportunity lies for European and global technology companies. Creating barriers to the free flow of data beyond Europe will not only create inefficiencies, but will also cut European companies off from the fastest-growing cloud markets in Asia and elsewhere around the world. There is a vast opportunity for European service providers and end users to fully participate in the emerging global, cloud-driven, Internet economy — if we get the data protection framework right.

How to ensure that rules around the world are good enough for each other? Just like when customers entrust their data with companies and Business Software Alliance (BSA) Member companies, it is about trust. EU and their partners should trust each other and work closely to allow for free movement of data.

30 years after the Organization for Economic Cooperation and Development (OECD's) Privacy Guidelines,

There is a vast opportunity for European service providers and end users to fully participate in the emerging global, cloud-driven, Internet economy — if we get the data protection framework right.

the "importance of effective, global, practical approaches to governing the collection, use and transfer of personal data has never been greater." How can this occur?

1. Through Bilateral and regional free trade agreement negotiations – Free trade agreements provide an important forum for raising the bar for open access to digital goods, services and information with willing trading partners. Negotiators should seek to introduce language expressly permitting cross-border information flows for different sectors; prohibiting measures that link market access or other commercial benefits to local infrastructure, investment or establishment.

2. Through existing multilateral and regional forums – Improving the multilateral framework for digital trade at the World Trade Organization (WTO) should be a high priority for all governments seeking to promote innovation. The Organization for Economic Cooperation and Development (OECD), which has organized a series of high-level dialogues and developed a set of principles on Internet policy-making, is another useful forum to engage some of the world's most innovative economies. The Asia Pacific Economic Cooperation (APEC) forum is also a constructive way to build trust and understanding among governments.

These are just a few examples of how governments, international organisations such as the EU can cooperate to ensure that data protection rules are good enough for each other.

Technology is a demand-driven phenomenon. Users know what they want and they use their choices to drive technology providers and tools developers to adapt constantly. So it is essential that the data protection framework sets clear rules that ensure respect for the basic rights of individuals and enterprises, without hindering innovation. There needs to be "breathing room" for technological progress to accommodate future trends in user demand. And it needs to be a balanced framework that will allow European companies to exploit the opportunities here in Europe, and abroad.

REFERENCE

1 See www.bsa.org/country/Public%20Policy.aspx

Koji Ouchi, First Secretary, Mission of Japan to the European Union, Brussels

Stewart Dresner introduced this presentation by stating that the two main challenges for interoperability were those relating to EU-USA transfers of personal data and EU-Asia Pacific Economic Cooperation (APEC) transfers of personal data. Peter Hustinx referred above to efforts to build bridges between the different privacy protection systems.

The APEC Member Economies are: Australia, Brunei Darussalam, Canda, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, chinese Taipei, Thailand, United States of America, and Vietnam[1].

On 22 December 2011, APEC's Data Privacy Sub-Group announced that 15 authorities from Japan had joined the APEC Cross-border Privacy Enforcement Arrangement.

Koji Ouchi said that Japan's current data protection law was adopted in 2005. The various government ministries supervise compliance with the data protection law in their various sectors, such as telecommunications. The work of all these ministries in the data protection field is co-ordinated by Japan's Consumer Protection Agency. 15 of these Japanese ministries, agencies and the Cabinet Office were the authorities which were accepted as members of APEC's Cross-Border Privacy Enforcement Arrangement in December 2011.

The ministers can make non-binding orders, and one of them did so against Google. Binding orders are rare. Compensation for breaches of privacy are low. Even though Japan's data protection law is regarded as weak compared with other Asian laws, other privacy tools are being developed in Japan, such as trustmark accountability agents.

Even though Japan's data protection law is regarded as weak compared with other Asian laws, other privacy tools are being developed in Japan, such as trustmark accountability agents.

Q: Japan's legislation does not meet a significant number of the EU's requirements for 'adequacy'. Is Japan requesting an EU adequacy declaration?

A: Japan has never requested the adequacy test and will not do that in a foreseeable future. One of the main obstacles is that we do not have an independent DPA. Rather, each Ministry/Agency is responsible for implementing the Data Protection Act in each sector, independent of one another and their respective sectors. And it has long been politically difficult to create a new agency as it runs counter to

administrative reforms taking place under the pressure of government deficits. But at the same time, we are not necessarily convinced that we cannot ensure the appropriate protection of personal data without a single independent DPA.

Q: It was announced on 22nd December 2011 that 15 authorities from Japan had joined the APEC Cross-border Privacy Enforcement Arrangement. In what ways has this arrangement had an impact in Japan or on companies and individuals doing business in Japan?

A: We first need to take a closer look at the extent to which third countries are protecting citizens' privacy in a real sense rather than just to compare structures. It will certainly take time. But having a better understanding of what is really taking place in the rest of the world is the best way and maybe a shortcut to come up with a global interoperability mechanism.

Japan is considered as not adequate compared with the EU Data Protection Directive by several experts, including those in Namur University, Belgium. They express their views based on the lack of an independent DPA in Japan as well as the low level of law enforcement. But it is not necessarily easy to see the correlation between the independence of regulators and the level of protection. As Christopher Graham, the United Kingdom's Information Commissioner, stated in the morning at this conference, it is not necessarily the sole role of a statutory system to protect privacy, especially in the cyber context. Actually we need more interactions between public and private sectors to manage privacy in an effective way.

JOSH HARRIS – VIDEO ADDRESS

Josh Harris, Associate Director, Office of Technology and Electronic Commerce, International Trade Administration, Washington DC and Vice-Chair, APEC Data Privacy Sub-Group, addressed the conference by video.
He explained the APEC's work in this area which is covered in detail at www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group
The APEC work on privacy, as can be seen at this website, is part of the wider work on encouraging electronic commerce in contrast with a European-centric fundamental rights focus.

REFERENCE

1 www.apec.org/About-Us/About-APEC/Member-Economies.aspx

Pat Walshe, Director, Privacy, GSMA, London

The GSMA (www.gsma.com) represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem.

Stewart Dresner in his introduction, stated that GSMA has made strong efforts to apply privacy principles to its sector, mobile phones and other mobile devices[1] . Pat Walshe said that there are 4 billion mobile devices in use outside the EU.

Is data protection interoperability a meaningful and achievable goal in the next five years? No. Walshe is optimistic that we will reach interoperability on a number of fronts, but this is not without significant challenges. He said that his response "no" to the question above was in the context of whether we would see some formal legal agreement within 5 years.

Walshe considers that we will see Codes of Conduct take a prominent role to facilitate interoperability. We live in a world that is based on disclosure and data sharing in ways never envisaged. It is incumbent on all stakeholders to work together and establish trust via multiple processes and mechanisms – trust will be key to interoperability.

How do we create meaningful privacy protection around the world? Long company privacy policies are not the answer. Legally binding sectoral codes, such as the GSMA's are helpful.

REFERENCE

1 See GSMA's 27 February 2012 media release at www.gsma.com/newsroom/gsma-announces-new-initiative-addressing-mobile-app-privacy and the Mobile and Privacy Privacy Design guidelines for Mobile Application Development document at www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf

Conclusion: Interoperability – a five-year goal?

Both the panel and the audience doubted that data protection interoperability would be a meaningful and achievable goal in the next five years in a legal sense.

However, as to the question whether there is a role for EU and international policy makers in encouraging the trend towards global interoperability, the majority agreed that they are already taking steps in this direction and would continue to do so.

Stewart Dresner, Session Chair and Chief Executive, Privacy Laws & Business

Your Subscription **includes**

1. Six Reports a year
The *Privacy Laws & Business (PL&B) International* Report, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from more than 100 countries – new laws, bills, amendments, codes and how they work in practice.

2. Helpline Enquiry Service
Subscribers may telephone, fax or email us with their questions such as: contact details of Data Protection Authorities, the current status of legislation and amendments, and sources for specific issues and texts.

3. Email updates
We will keep you informed of the latest developments.

4. Index
A cumulative Country, Subject and Company index is available at www.privacylaws.com/Publications/report_index/. Subject headings include Binding Corporate Rules, data breaches, data security, encryption, enforcement, sensitive data, subject access and transborder data flows.

Electronic Option
The Report is available, for an additional enterprise licence fee, in PDF format for uploading onto your Intranet or network. This format enables you to see the Report on any computer on your network as it appears in the paper version. It allows you to print out pages at any location.

Privacy Laws & Business has clients in more than 50 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times *lists; and 10 of the Global Top 20 in the* Fortune *list.*

Privacy Laws & Business also publishes the United Kingdom Report, *a publication which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.*

Subscription Form

Subscription Packages

(VAT will be added to PDF subscriptions within the UK)

❑ **Print** ❑ **PDF** (please tick preferred delivery format)

❑ Send a FREE sample of the *UK/International* Report

❑ *PL&B International* Report Subscription **£405**

❑ *UK/International* Reports Combined Subscription **£650** or an extra **£245** for existing International Report subscribers)

❑ Special academic rate – 50% discount on above prices

Multiple Subscription Discounts

❑ 2-4 copies: 70% discount (indicate no. of copies ...)

Intranet Enterprise Licence (inc. up to 10 printed copies)

❑ *PL&B International* Report **£2,025**

❑ *PL&B UK* Report **£1,550**

❑ Both *International/UK* Reports **£3,250**

❑ I wish to receive *PL&B's* FREE email news service

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Accounts Address (if different):

Postcode:

VAT Number:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

Please return completed form to:
Subscriptions Dept, Privacy Laws & Business,
2nd Floor, Monument House, 215 Marsh Road,
Pinner, Middlesex HA5 5NE, UK
Tel +44 20 8868 9200 Fax: +44 20 8868 5215
e-mail: sales@privacylaws.com 23/1/2013

www.privacylaws.com

Guarantee

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