Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing

by **Philipp E. Fischer**, Munich, Ph.D. cand. (Barcelona), LL.M. (IP, London/Dreseden), Data Protection Officer & -Auditor (TÜV)

Abstract: The development of the Internet has made it possible to transfer data 'around the globe at the click of a mouse'.[1] Especially fresh business models such as cloud computing, the newest driver to illustrate the speed and breadth of the online environment, allow this data to be processed across national borders on a routine basis. A number of factors cause the Internet to blur the lines between public and private space: Firstly, globalization and the outsourcing of economic actors entrain an ever-growing exchange of personal data. Secondly, the security pressure in the name of the legitimate fight against terrorism opens the access to a significant amount of data for an increasing number of public authorities. And finally, the tools of the digital society accompany everyone at each stage of life by leaving permanent individual and borderless traces in both space and time. Therefore, calls from both the public and private sectors for an international legal framework for privacy and data protection have become louder. Companies such as Google and Facebook have also come under continuous pressure from governments and citizens to reform the use of data. Thus, Google was not alone in calling for the creation of 'global privacystandards'.[2] Efforts are underway to review established privacy foundation documents. There are similar efforts to look at standards in global approaches to privacy and data protection. The last remarkable steps were the Montreux Declaration, in which the privacycommissioners appealed to the United Nations 'to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights'. This appeal was constantly repeated, lastly in 2010 at the 33rdInternational Conference of Data Protection and Privacy Commissioners. In a globalized world, free data flow has become an everyday need. Thus, the aim of global harmonization should be that it doesn't make any difference for data users or data subjects whether data processing takes place in one or in several countries. Concern has been expressed that data users might seek to avoid privacy controls by moving their operations to countries which have lower standards in their privacy laws or no such laws at all. To control that risk, some countries have implemented special controls into their domestic law. Again, such

Keywords: International data transfer, international legal framework, global privacy standards, cloud computing, data protection, privacy rights infringement, data controller, data processor, European Data Protection Directive, EU-DPD, safe harbor, Standard Contractual Clauses, adequacy, adequate level of data protection, APEC, OECD, UN, accountability, Binding Corporate Rules

Recommended citation: Philipp E. Fischer, Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing, 3 (2012) JIPITEC 1, para 33.

A. Introduction

1 During the 2012 CeBIT IT fair this March in Hannover, René Obermann, CEO of Deutsche Telekom, highlighted that 'the present PC architecture is outdated; the post-PC era has begun. [...] We want to play an important role in the ecosystem cloud'.[3] This is not surprising, given that Germany's BITKOM[4] association recently issued a study finding that the annual turnover in cloud computing businesses in Germany will end up at around 5.3 billion euros in 2012, a steep increase of 50% compared with the previous year. The prediction for 2016 is even about 17 billion euros per year, a third of it through business-to-private consumer relations. Market analyst 'Gartner' recently determined the global returns of cloud computing in 2012 at 77 billion euros.[5]

2 Big market players are now pushing forward their own business models for cloud computing and installing new data centres worldwide. This dramatically increases the quantity – but not necessarily the quality – of cloud computing services offered to consumers. This development leads to a large amount ofdata transfer' around the globe at the click of a mouse',[6] data which is to be processed across national borders on a routine basis.

3 The shady side of these new opportunities for the global web community has been addressed not only by Germany's chancellor Angela Merkel – 'The more natural technologies become, the more important is the necessity of trust'[7] –but also by Viviane Reding, Commissioner of the European Union (EU):

> *Let's take cloud computing: storing information in the cloud holds much economic promise and many consumer benefits. Cloud computing is becoming one of the backbones of our digital future. However, new technologies also raise challenges for policy makers. A cloud without robust data protection rules is not the sort of cloud we need.*[8]

4 Reding went on to say that 'privacy nowadays has become a moving target: new risks need better legal remedies'.[9]

5 Few companies take data protection issues in cloud computing seriously. The Deutsche Telekom seems to understand that in order to serve the B2B market with cloud computing services, it needs some hard work on data protection measures and politics of trust. According to Mr. Obermann, 60 out of 90 data centres outside of Germany already do comply with all technical standards under German law. The negative example to prove the opposite is – again – Google: even after having suffered strong criticism because of its newest privacy policy, Eric Schmidt, a member of Google's board of directors, didn't say a word at the CeBIT fair about data protection in cloud computing surroundings; he preferred to praise the neutrality of the Net.

6 To tackle concerns of privacy and data protection in the cloud, calls from both the public and private sectors for an international legal framework for privacy and data protection have become louder. Companies such as Google and Facebook have come under continuous pressure from governments and citizens to reform the use of data.

7 Efforts are underway to review the established privacy and data protection legal framework:

8 The first remarkable step was the Montreux Declaration,[10] in which the privacy commissioners appealed to the United Nations 'to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights'. This appeal was repeated in 2008 at the 30th International Conference of Data Protection and Privacy Commissioners held in Strasbourg,[11] at the 31st conference held in 2009 in Madrid,[12] and at the 32nd conference held in 2010 in Jerusalem.[13] At the 33rd conference in 2011 in Mexico City,[14] the working group for the 'Promotion of the International Standards' resumed their efforts:

> *In line with the Jerusalem resolution, the Conference will continue to promote the Joint Proposal for International Standards in all relevant international fora (e.g. OECD, Council of Europe, APEC) and its efforts to organize an intergovernmental conference for developing a binding international instrument. In this regard, it could be envisaged to convey government's representatives at the next Conference meeting in 2012 in order to engage a dialogue in that perspective.*[15]

9 French President Nicolas Sarkozy decided to put the Internet at the top of the agenda of the French presidency of the G8/G20 in 2011. At the G8 summit in Deauville last May, all member states expressed the strong political commitment of the G8 members concerning the protection of personal data and individual privacy:

> *The effective protection of personal data and individual privacy on the Internet is essential to earn users' trust. It is a matter for all stakeholders: the users who need to be better aware of their responsibility when placing personal data on the Internet, the service providers who store and process this data, and governments and regulators who must ensure the effectiveness of this protection. We encourage the development of common approaches taking into account national-legal frameworks, based on fundamental rights and that protect personal data, whilst allowing the legal transfer of data.*[16]

10 The EU Commission addressed these issues in its factsheets on proposed data protection reform:

> *The rapid pace of technological change and globalisation have profoundly transformed the scale and way personal data is collected, accessed, used and transferred. There are several good reasons for reviewing and improving the current rules, which were adopted in 1995: the increasingly globalised nature of data flows, the fact that personal information is collected, transferred and exchanged in huge quantities across continents and around the globe in milliseconds and the arrival*

of cloud computing. In particular, cloud computing – where individuals access computer resources remotely, rather than owning them locally – poses new challenges for data protection authorities, as data can and does move from one jurisdiction to another, including outside the EU, in an instant. In order to ensure a continuity of data protection, the rules need to be brought in line with technological developments.[17]

11 In a globalized world, free data flow has become an everyday need. Thus, the aim of global harmonization should be that there is no difference for cloud users whether the processing of their personal data takes place in one or in several countries. Concern has been expressed that data processors might seek to avoid data protection controls by moving their operations to countries that have lower standards in their data protection laws or no such laws at all. To control that risk, some countries have implemented special controls in their domestic law. Again, such controls may interfere with the need for free international data flow.

12 A formula has to be found to make sure that privacy at the international level does not prejudice these goals. It is a long journey.

B. The polar caps: Cloud computing and privacy

I. Definitions of 'privacy' and 'data protection'

13 To those outside the privacy world it must seem incredible that lawyers are still debating the central issue in privacy: What are we trying to protect?[18] On an international level we are weighed down with divergences of usage with a non-uniform interpretation of this concept: privacy can rely upon a 'human right' ora 'social need'; it can be interpreted comprehensively as 'privacy of the person', 'privacy of personal behaviour', 'privacy of personal communications' and 'privacy of personal data'.

14 This article follows a definition influenced by Article 8 of the European Convention on Human Rights (ECHR)[19] and the European Data Protection Directive (EU-DPD):[20] In European privacy law, privacy is explicitly mentioned as a fundamental right. Through the Lisbon Treaty,[21] Article 8 of the 'Convention for the Protection of Human Rights and Fundamental Freedoms' (ECHR)[22] became mandatory to reach the aims of European data protection. Article1 of the EU-DPD and of the Directive 2002/58/EC[23] clearly state the ultimate purpose of the rules contained therein: to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy, with regard to the processing of personal data. The 'Article 29 Data Protection Working Party'[24] issued a document defining'personal data' in order to clarify the EU-DPD's approach. It was divided into four key elements: 1) any information 2) relating to an 3) identified or identifiable 4) natural person.

15 This illustrates that within the E.U. the concepts of data protectionand privacy are "twins, but not identical"[25], and that data protection law "seeks to give rights to individuals in how data identifying them or pertaining to them are processed, and to subject such processing to a defined set of safeguards"[26], while privacy can be seen as a "'concept which is broader than data protection, though there can be a significant overlap between the two'.[27]

16 Thus, the author of this article will keep in mind that data protection is one key element within people's privacy rights, but the scope of this element goes from protecting their 'right to be left alone'[28] to their 'right to be forgotten'.[29] The former means protecting personal data from being collected, transmitted, stored and used in an unlawful way. The latter means the possibility to manage data protection risks online; when the right owners no longer want their data to be processed and there are no legitimate grounds for retaining it, the data must be deleted. Henceforth, the author will look at issues of 'data protection 'only; other elements of people's privacy rights have to be left aside.

II. Definition of 'cloud computing'

17 Although cloud computing services have been on offer for many years, the significantly increased use of social media sites as Facebook and Google+ in cloud computing surroundings opened the public debate on the definition of 'cloud computing'.

18 The relevant players in cloud computing surroundings are as follows:

- The resource owner

A cloud computing model is composed of three service models, depending on the type of resources offered by the resource owner:

- Infrastructure as a service ('IaaS'):
IT services such as hardware components.

- Software as a service ('SaaS'):
Application packages, email, ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), ECM (Enterprise Content Management).

- Platform as a service ('PaaS'):
Resources and infrastructure-software, e.g. webserver, databases.

- The cloud provider

There are four models for deploying these resources bundled in a cloud computing service:

-Private cloud:
Services are exclusively used by one institution, even if supporting public processes are running in the background. Resource, cloud provider and cloud user are the same entity (e.g. one company).

-Public cloud :
Services can be used by everybody. All physical resources are not owned by the cloud user.

-Hybrid cloud:
A hybrid cloud mixes elements of both the public and private cloud.

-Community cloud:
The cloud infrastructure is commonly used by different organizationsthathave their common standards (e.g. security, privacy, compliance) and support a specific community.

- The cloud user
The advantages of cloud computing for the end user include the following: anytime and broad network access, hardware cost reduction, efficiency, rapid elasticity, measured service. But its key feature is what is called the 'scalability' of service, meaning that services and resources can be scaled up or down depending on the users' demand.

III. Effects of cloud computing on data protection

19 Using cloud computing to process personal data raises legal and technical questions that have yet to be adequately addressed. The use of cloud computing may become relevant for data protection in mainly six juridical dimensions.

20 Issues of solely technical risks within the cloud will – at this point – not be an object of this article. These include missing or insufficient separation/isolation of different data processing processes, lock-in effects, system and network failure and non-availability of rented resources and services, misuse of data by malicious insiders or employees and loss of data.

1. Processing of personal data

a.) Processing

21 Article 2 (b) EU-DPD provides that

> *Processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*

b.) Personal data

22 It has to be determined what type of data is normally processed in a cloud. From a data protection perspective, cloud computing becomes relevant only if this data is 'personal data'.

23 The Article 29 Working Party states that

> *personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to oneor more factors specific to his physical, physiological, mental, economic, cultural or social identity.*[35]

24 Data protection laws don't apply if sufficient aliasing of formerly personal data can be provided by the cloud provider. But it has to be remembered that aliased data can also become re-identifiable through additional information, e.g. because other cloud users or cloud providers have additional knowledge with which a re-identification is possible. One can assume identifiability regularly through individual records of persons. Especially electronic evaluability and the integration into a global network may increase the probability of the existence of a priori information that enables identification of those who are affected.

2. Ubiquity and different data protection levels

25 A cloud is by its nature not necessarily tied to any particular location; in fact, as many other IT services nowadays, it is ubiquitous. Thus, data traffic in a cloud can take effect in different countries, each withitsdifferent laws relating to acts taking place on itsterritory. As a result, each cloud computing process would have to comply with different privacy laws and levels of data protection.

26 This leads to the second dimension, which is the territorial level of data protection that exists in states

in which the above-mentioned data is processed in a cloud.

27 National rules provide that after the classification of personal data as 'sensitive data', this data may be moved only if the processing meets special requirements. From a German point of view, the application of national rules come with only minor restrictions in the EU region, but significant restrictions whenever processing is carried out in the US and other third countries, as very different levels of data protection exist in countries beyond the EU.

28 The EU provides a strict legal regime and high level of data protection under the EU-DPD. The Directive requires that any country to which European personal data is sent must have an adequate level of data protection as measured by EU standards. As many cloud computing providers are based outside the EU but wish to conduct their business within the EU, they must ensure an adequate level of protection. This fact forced the US and EU to a bilateral convention, the safe harbor agreement.[36]

29 But even within the EU, different ways of implementing the Directive's Article17 into national laws do exist. The Article 29 Working Party will hopefully contribute an expert's opinion to the necessity of common standards regarding 'technical and organizational measures'. At the moment we face a disparity of such standards, with the result that each EU-based computer centre must first comply with the laws of its own jurisdiction, including the regulations of its own data protection authorities; second, it must take into account that the cloud usually is a cross-border issue, to comply with other national laws.

3. Issues of accountability between controller and processor

30 In cloud computing surroundings, the distinction between controller and processor is not always clear in practice and has to be subjected to a comprehensive consideration of all circumstances, especially if a cloud service is offered on a cross-border basis or cloud sub-providers are included in the supply chain.

31 At this point, the focus of the EU-DPD has to lie on the concept of 'data controller' and 'data processor' .A controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law (Art. 2 (d) EU-DPD), while a processor shall mean 'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller' (Art. 2 (e) EU-DPD).

32 The basic concept is that a controller makes decisions about what data to collect and how to use it, while a processor performs operations on data only on behalf of the controller and according to the controller's instructions. Recommendations[37] of the Article 29 Data Protection Working Party are helpful to differentiate: The crucial question becomes who determines the purpose ('why?') and the essential means ('how?') of the processing. It is decisive which data transmitter is actually authorized to decide on these questions. Whoever determines the purpose or decides on essential elements of technical means of the data processing automatically becomes a data controller. The member states developed one helpful question on that differentiation. In Germany, for example, this question is who appears towards the affected persons as responsible for the data, or with whom the affected person has a legal relation or for whose business purposes the processing is carried out.

33 In cloud computing, the person or entity that 'determines the purposes and means of the processing' initially is the cloud user who makes the decision to use the cloud and feeds the data into it. Basically, a responsibility is not limited to the data controller's actual sphere of influence; it extends to contract data processing as well. Article 17 EU-DPD establishes that, when data is processed under contract, the controller is responsible for compliance with data protection requirements. This means that a person or entity cannot evade its responsibility by contracting with third parties.

34 The controller is responsible primarily for ensuring that the processing is allowed under substantive law, which can have implications under administrative, civil and criminal law. The Directive also brings a set of principles to be observed by the member states. Article 23 EU-DPD directs the member states to guarantee the protection of personal data by a corresponding national regulation on liability. Every instance of unlawful data processing, as well as any infringement of national laws having implemented this Directive, shall raise liability, in particular omitted information and clarification duties or the omitted conclusion of a contract for the purposes of Article 26 (2) EU-DPD. The resulting damage must be causally proven. The affected person has to meet the burden of proof concerning his damages as well as the legal cause, so causality must be proven or a 'sufficient causal link 'relating the data controller's or data processor's actions to the damage in question.

35 Although the wording of Article 23 (1) EU-DPD leaves unanswered whether the liability is dependent on fault, a fault-based liability has to be presumed or the exculpation rule of Article 23 (2) EU-DPD would

not be necessary. It is doubtful whether only material or also immaterial disadvantages are meant with 'damage' for the affected person. Even in the recitals of the EU-DPD, no statements can be found on this issue; hence, a margin of discretion can be assumed when it is turned over to any member state.

4. Jurisdiction, applicable lawand enforcement

36 Conflict of laws is central to cloudcomputing because the Internet, thevery basis of the'cloud',is multinational. While cloud computing and other e-commerce innovations are giving new prominence to this area of law, private international law is not a creation of cyberspace. It is a series of national rules and principles that have been developed over centuries to assist legislatures and courts in dealing with three questions that arise in transactions with one or more international or at least multi-jurisdictional elements. Which courts may take jurisdiction over the parties or the transaction? Which laws apply? When will the courts of one jurisdiction enforce a judgment rendered by the courts of another jurisdiction?[38]

a.) Private cloud vs. public cloud

37 Robert Gellman of the World Privacy Forum highlighted the issues raised by data location:

38 The European Union's Data Protection Directive offers an example of the importance of location on legal rights and obligations. Under Article 4 [...] [o]nce EU law applies to the personal data, the data remains subject to the law, and the export of that data will thereafter be subject to EU rules limiting transfers to a third country. Once an EU Member State's data protection law attaches to personal information, there is no clear way to remove the applicability of the law to the data.[39]

39 As a result, it becomes important which national laws are applicable to the (first) processing of personal data in a cloud solution. It has to be considered where the relevant data is processed and from which legal system this data may originate.

40 The geographical location of personal data in the cloud has an important impact on the legal requirements of a court's jurisdiction and the law that applies to the case. At this point, the differentiation between private cloud and public cloud becomes crucial. For instance, for a private cloud solution thatprocesses 'German data'– data processed on servers, computers and storage systems exclusively operated in Germany–only German law applies. Thus, a private cloud poses no special problems in international private law (IPL) as lon gas the transfer of personal data into a cloud is carried out on German territory. Whenever personal data is processed in a public cloud, however, it has to be assumed that this data is being processed on computers and storage systems in different states. The exact place where data is located is not always known, and it can change in time. In a public cloud, the cloud services are not aimed at specific countries but as ubiquitous services. In this case, questions of jurisdiction and applicable law have to be examined.

b.) Jurisdiction

41 The choice of forum for settling disputes between the cloud provider and the cloud customer can be included in the terms and conditions of the contract. Providers usually specify a jurisdiction where the headquarters is based or its main business is carried out.

42 In the absence of a choice of forum provision, courts generally will take jurisdiction if there is a 'real and substantial connection' between the jurisdiction and either the people involved (personal jurisdiction) or the subject matter of the dispute (subject matter jurisdiction). The courts will take jurisdiction over people resident or domiciled in their jurisdiction as well as over property situated in their jurisdiction. They may also take jurisdiction where an accident occurred or damages were suffered in the jurisdiction.

43 If a person or company is domiciled or based in a member state of the EU, it shall be sued in the courts of that member state. If these are not nationals of the member state in which they are domiciled or based, they shall be governed by the rules of jurisdiction applicable to nationals of that state (Art. 2 Brussels I).[40] They can be sued in the courts of another member state only by virtue of the rules set out in Sections 2 to 7 of Brussels I Regulation.

44 Article 5 Brussels I provides that

> *a person domiciled in a Member State may, in another Member State, be sued: 1. (a) in matters relating to a contract, in the courts for the place of performance of the obligation in question; (b) for the purpose of this provision and unless otherwise agreed, the place of performance of the obligation in question shall be: [...] in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided.*

45 Asserting jurisdiction can become a significant problem whenever the ubiquity of cloud computing services imposes questions such as the following:

46 What are the international elements in the case at hand and what is the question that we are seeking to answer? Are we asking if the court in the jurisdiction of the customer will take jurisdiction over a dispute

between an online supplier of cloud computing services and a customer? Or are we asking whether the criminal laws of Oregon apply to a Russian website that allows you to store and play your music from anywhere around the globe?[41]

c.) Applicable law

47 The contract statute may result from an effective choice of law, from the perspective of European IPL determined by Article 3 (1) Rome I.[42]

48 In its absence, the law of the state applies where the provider of the service – given that a cloud computing service is qualified as a tenancy law issue – has its 'habitual residence' (Art. 4 (2) Rome I). If rules of an employment contract shall govern cloud computing, Article 4 (1b) Rome I leads to the same result.

49 Furthermore, it has to be considered that, for the benefit of consumer protection rules, atypical choice of law clauses are inapplicable; in this case, the national law remains applicable in which the consumer resides (Art. 6 (1b) Rome I). Mandatory national consumer protection rules always remain applicable in favour of the consumer (Art. 6 (2) Rome I).

50 For companies wanting to store data in the cloud, there is a minefield of data protection laws to negotiate, so it is essential to know in which country your data is physically stored. 'Most organizations don't even know what data they have,' says Tony Lock, program director at IT services consultancy Freeform Dynamics. 'They are unsure where all the data is and once they've found it they are unsure how to protect it.'[43] But which laws apply, for example, to a German company storing data about German customers via a contract with a US cloud provider whose servers are located in Poland? At the moment, the answer is all three due to the very debatable rules of applicable law in the EU-DPD.

d.) Subcontracting

51 Whenever a cloud provider uses a third-party subcontractor to carry out its business, issues of jurisdiction and applicable law get even more complex, because the existence of a subcontracting relationship is likely to be invisible for the cloud user and the location of the subcontractor or the data processed by him difficult to ascertain.

e.) Enforcement

52 As a consequence, the question arises whether the flow of data adequately meets the regulatory requirements of each jurisdiction through which it flows. In theory, each controller could be sued in various states worldwide for a breach of data protection laws. But in practice, law enforcement is more difficult.

53 Whenever the violation of data protection laws is committed outside European territory, there is generally no way to investigate it, because under the law, the oversight of supervisory authorities is limited to the territory of each state. An administrative assistance, provided in inner-European cases, doesn't apply to cases beyond the EU.

54 Thus, data controllers processing data in third-party countries that want to evade data protection authorities' oversight can use clouds specifically for that purpose. Another negative effect of the cloud is that any monitoring is contingent on contractual monitoring rights granted by the cloud and resource providers, and furthermore these rights must be exercised by the cloud user, which generally has no vested interest in data privacy oversight.

5. Contract data processing

55 The element of contract data processing has been implemented in Article17 EU-DPD in order to secure personal data within the collecting, processing or use of data on behalf of others. Article17 EU-DPD applies if

> *a contract between a controller and processor has been concluded, requiring that the processor act only on instruction of the controller;*

and

> *a (cross-border) data processing takes place within the member states of the European Union (EU) or European Economic Area (EEA).*

56 Article17 (2) EU-DPD then requires a controller to 'implement appropriate technical and organizational controls to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access'.

57 Article17 EU-DPD remains inapplicable if the processor can be qualified as a third entity that does not act on the instruction of the controller, or the processing of personal data is carried out outside of the EU. In this case, the data transfer is lawful only if the cloud provider complies with the provisions set out in Articles25, 26 EU-DPD.[44]

58 The EU-DPD states clearly that data cannot leave the EU unless it is transmitted to a country with 'adequate level of protection'. That means that many cloud providers outside the EU have to study and follow one of four different methods to ensure adequate protection as long as they wish to conduct cloud services business inside the EU: first, be one

of the countries that have laws enacted that the EU deems to be adequate protection; second, achieve adequacy through compliance with safe harbor provisions; third, use a standard contractual clause prepared and adopted by the EU; or fourth, use binding corporate rules.[45]

6. International data transfer

59 Cloud providers established in countries outside the EU and EEA have to conduct a two-step test whenever they want to process personal data of a European data subject in a lawful way. First, the transfer of personal data into the cloud and the processing in the cloud must have a legal basis. Secondly, an adequate level of data protection must be ensured at the cloud location outside the EU/EEA. For the latter, safe harbor, binding corporate rules and EU standard contractual clauses (or model contracts) are mainly relevant. Unfortunately, several data protection offices and authorities do not always clearly distinguish these two basic steps.

60 Article 25 ff. EU-DPD is relevant regarding the second step. Article 25 (1) EU-DPD requires that member states prohibit the transfer of personal data to third countries lacking similar legal protections, unless a) the national supervisory authority (Art.25 (2) EU-DPD) or the European Commission approves the data transfer, b) one of several limited exceptions apply (Art.26 (1) EU-DPD) or c) approved safeguards are in place (Art. 25 (6), Art.26 (2), Art. 26 (4) EU-DPD).

61 The European Commission has recognised through 'adequacy tests' (Art.25 (4) EU-DPD, Art.25 (6) EU-DPD, Art.31 (2) EU-DPD) a sufficient level of protection (Art.25 (1) EU-DPD) for only a few countries.[46] EU member states must allow a data transfer to one of these countries (Art. 31 (2), Art. 25 (6) EU-DPD). Other countries should soon be under review for a possible addition to the white list if their laws are deemed adequate.[47] For the remaining countries, an adequate level of data protection must be guaranteed individually. Four of these are most often used: unambiguous consent and several contractual instruments ensuring accession to safe harbor principles, the conclusion of standard contractual clauses (SCC) or the adoption of binding corporate rules (BCR).

62 It has to be carefully taken into account where Article 26 EU-DPD stands within the system of principles and derogations on a European and on a national basis. The Article 29 Data Protection Working Party states that

> *[t]he juxta position of these different rules on transfers of personal data may givea paradoxical impression, and can easily give rise to misunderstanding. [...] Under these provisions, the data controller originating the transfer neither has to make sure that the receiver will provide adequate protection nor usually needs to obtain any kind of prior authorisation for the transfer from the relevant authorities, if this procedure would be applicable. Furthermore, these provisions do not require the data receiver to comply with the Directive requirements as regards any processing of the data in his own country (e.g. principles of purpose, security, right of access, etc.).*[48]

63 On the one hand, derogations of Article 26 (1) EU-DPD can apply, e.g. Article 26 (1) a) EU-DPD: Such consent must be given by the person whose personal data is to be transferred. It must be 'clear, freely, given and informed' (Art.26 (1) EU-DPD). Consent can be refused and withdrawn at any time. Technological measures to ensure a consent that may be evidenced and enforced later on can greatly vary from one another. For instance, the range includes user pop-ups with an option to consent by ticking the box of their choice before they may continue entering the website. A problematic issue is the freedom of consent in an employment context. The Article 29 Data Protection Working Party has released a document in which it states that employees would not be able to freely give their consent due to their subordination link with their employer ('reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment'[49]). In practice however, this form of consent can be a valid derogation under certain circumstances, as when the data transfer is submitted to the works council or it is made clearly for the benefit of the employee, without small print. Nevertheless, the Article 29 Data Protection Working Party considers that 'consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question'. This opinion is clearly opposed to the exemptions in Article26 (1) EU-DPD.

64 On the other hand, to transfer the derogation provisions of Article26 (2), (4) EU-DPD into practice, several instruments have been developed: safe harbor-principles, PNR, BCR, SCC I,[50] SCC II[51] andSCC-DP.[52]All of these instruments with their beautiful abbreviations differ in terms of standardization level and liability rules and remain to be mentioned below under 'Perspectives of global standards'.

C. The present means of travel: Perspectives of global standards

65 Answers for the above-mentioned problems could be found in global data protection legislation. In recent years, an increasing number of states have adopted data protection legislation, and a fundamental, legally binding right to privacy is recognized both in the national law of numerous states –particularly in Europe –and in certain regional legal instruments. The questions that then arise are whether privacy is similarly recognized in international law as a bind-

ing legal concept, whether existing models of privacy are diverse and how privacy is considered in data protection legislation.

I. Public law

1. US legal framework

a.) Facts

66 The US approach deals with data protection in so many narrow sectors that this article can't claim to touch all of them and will have to focus on the most important ones:

67 The implications of the 'Graham-Leach-Bliley Act'[53] (GLB) on cloud providers is that the cloud provider has to comply with the relevant parts of GLB by demonstrating how it prevents unauthorized access to personal data and/or contractually agree to prevent this unauthorized access. The safeguards rule mandated by the GLB and enforced by the Federal Trade Commission (FTC) requires that all cloud providers involved in financial services and products must have a written security plan to protect customer information.

68 The FTC promulgated so-called 'Red Flag Rules' in 2007, based on the 'Fair and Accurate Credit Transaction Act of 2003'[54] (FACTA). These flags also apply to cloud providers that are creditors as well as to other companies in online spaces. Therefore, the cloud provider must also have a written security plan and monitoring systems in place.

69 A data breach is a loss of unencrypted electronically stored personal data that can occur, for example, if a laptop has been stolen or a server has been compromised. Almost all 50 states now require notification from cloud providers of the affected persons and coordination with the cloud users.

70 In the US health sector, the 'Health Information Technology for Economic and Clinical Health Act' (HITECH Act) requires notification of any breach of unencrypted health records for all entities that have to comply with the 'Health Insurance Portability and Accountability Act'[55] (HIPAA). A service provider cannot use or disclose health records in a way that conflicts with the HIPAA standards. Thus, an entity covered by HIPAA could violate HIPAA by processing patient records through a cloud providers' service that allows the publication of any information stored on its facilities on the basis of its terms and conditions.

71 The 'USA Patriot Act'[56] has important effects on cloud provider behaviour in the US. The Act widens the US government's possibilities to, for example, install devices to record all routing, addressing and signalling information kept by a (cloud) computer and gain access to personal financial information and student information stored in the cloud. The only legal requirement for the US government lies in a governmental certification that the information obtained be relevant to provide information to an on-going criminal investigation. This concept basically leads to the gathering of personal data in the cloud – without any suspicion of wrongdoing.

72 The 'Electronic Communications Privacy Act'[57] (ECPA) applies to 'any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature', as long as it is transmitted electronically. Although this law is difficult to apply, particularly because the law is old and based on a model of electronic mail and Internet activity that is generations behind the current technology, it appears to provide probable protection for most data processed by cloud providers.

73 Besides the data breach laws (see above), many states[58] require that technology vendors (including cloud providers) provide adequate security in their contractual guarantees.

74 Customers of tax preparers enjoy some statutory and regulatory privacy protections. These customer protections in turn limit the ability of a tax preparer to use a cloud provider.[59]

75 The 'Violence Against Women Act'[60] prohibits all disclosures not compelled by statute or a court, except disclosures with the consent of the data subject. Thus, the terms and conditions of a cloud provider have to comply with this non-disclosure standard.

76 The US approach reflects a 'basic distrust of government; markets and self-regulation rather than government oversight shape information privacy in the U.S. and as a result the legislation that does exist is reactive and issue-specific; protection tends to be tort-based and market orientated rather than legislative or regulatory'.[61] Therefore, this approach is also called a 'patchwork of rules'[62] or 'piecemeal model'[63] that deals with data protection in specific sectors and problems in a 'haphazard manner'.[64]

77 On the other hand, they address specific and sometimes narrowly targeted privacy issues.[65] Self-regulation is another pillar of the US system and could be a useful contribution to global standards. An online privacy seal program exists, e.g. for labelling schemes. But authorities such as 'TRUSTe'[66] or 'BBBOnline'[67]have faced some criticism that they do not go far enough to punish seal holders that break the rules, and that the organizations are not quick

enough in revoking the seal on companies that violate privacy standards.

b.) Observations

78 The self-certification of US companies to safe harbor alone is not enough to reach a data security level corresponding to EU standards. Cloud contracts that are orientated by safe harbor are also insufficient. Safe harbor, however, cannot handle the stricter data security regulations in Europe. Cloud suppliers such as Google or Salesforce with headquarters in the US identify themselves for purposes of proof of trustworthiness with a SAS-70-Typ-II certificate. This means that the data centres should be checked by an independent third party. This measure is only partially enough for the requirements of the order data processing. For example, it does not consider the material and procedural interests of affected persons in transmissions. It is also possible that the companies involved in a cloud present themselves to BCRs, by which an adequate level of protection after Article 26 par. 2 EU-DPD could be reached.

2. EU legal framework

a.) Facts

(1) CoE Convention 108

79 The principles that the EU-DPD establishes are based on a range of Articles 7 and 8 ECHR and the CoE Convention 108.[68] The CoE Convention 108 was based on the 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' and called for national implementation of data privacy laws by individual European states. However, it is also envisaged to be potentially more than an agreement between European states (Art. 23). The CoE Convention 108 is not intended to be self-executing, and it permits derogations in some significant areas (Art. 3, 6 and 9). In addition, depending on the rules in national law regarding the adoption of international conventions, if a convention is implemented into domestic law, then the relevant provisions can be amended under the constitutional law of that state, regardless of its obligations under international law. Still, these legislations had no effect on international legislation.

(2) European Data Protection Directive and its reform

80 On 25 January 2012, Viviane Reding, European Commissioner for Justice, presented plans to enhance data protection rights for individuals across Europe and increase the responsibility and accountability of organizations processing personal data. The draft 'guidelines' show a growing concern about the way in which personal datais collected, processed and used. Viviane Reding's aim is that the rules will be implemented with consistency and clarity across all European Union member states and also apply to organizations based outside Europe that do business within the community.

81 The new legislation will replace the present EU-DPD, an important component of EU privacy and data protection legislation under which organizations in both the public and private sector have been operating for now thirteen years.

82 These are the key elements of the proposed reform:

- A 'right to be forgotten' will help people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed.
- Easier access to one's own data and the right of data portability, i.e. easier transfer of personal data from one service provider to another.
- Companies and organizations will have to notify serious data breaches without undue delay, where feasible within 24 hours.
- A single set of rules on data protection, valid across the EU.
- Companies will only have to deal with a single national data protection authority – in the EU country where they have their main establishment.
- Individuals will have the right to refer all cases to their home national data protection authority, even when their personal data is processed outside their home country.
- EU rules will apply to companies not established in the EU if they offer goods or services in the EU or monitor the online behaviour of citizens.
- Increased responsibility and accountability for those processing personal data.
- Unnecessary administrative burdens such as notification requirements for companies processing personal data will be removed.
- National data protection authorities will be strengthened so they can better enforce the EU rules at home.[69]

83 Christian Toon, Head of Information Security Europe, Iron Mountain, is on the right track by stating that

> *it remains to be seen how much of the draft proposal makes it into the final legislation; but the announcement of the plans has given organizations across Europe a valuable opportunity to review and enhance their information handling policies. We must seize that opportunity. Once the new EU legislation is finalised and comes into effect, it will be too late.*[70]

(3) European Cookie Directive

84 The Directive 2009/136/EC71 requires consent for the placement of cookies on the Internet by tightening existing legislation in this regard, namely the e-Privacy Directive (2002/58/EC).

85 The Cookie Directive requires end user consent to the storing of cookies on their computer. It states that a cookie can only be stored on the computer or accessed from the computer if 'the user has given his or her consent, having been provided with clear and comprehensive information'. The cookie can only be placed when it is absolutely necessary for the provision of a service that has been requested by the user or information storage is for the sole purpose of carrying out an online communication. This Directive is relevant for cloud computing issues only if cloud providers include advertising into their services; then they need users' consent for the provision of cookies.

86 In practice, this Directive is likely to affect mainly organizations offering applications that attempt to access personal data; this will require user consent via the opt-in principle.

(4) EuroSOX

87 The 'Sarbanes–Oxley Act'[72] of 2002, more commonly called SOX, is a US federal law thatset new or enhanced standards for all US public company boards, management and public accounting firms. It has been drafted as a reaction to the stocktaking scandals around the companies of Enron and Worldcom.

88 'EuroSOX'– the nickname for the 8th EU Company Law Directive 2006/43/EC[73]–is a reaction to the US SOX initiative, though EuroSOX is less similar to US Sabanes-Oxley (SOX) than the nickname may try to imply. In Germany the Directive is adopted in the new law called 'Bilanzrechtsmodernisierungsgesetz' (BilMoG). From a data protection point of view, the Directive demands high conditions for information security systems and internal IT control systems. Although the Directive doesn't mandate a specific standard or framework, 'it clearly shows that established international standards and frameworks such as ISO 27001/27002, COBIT and COSO (Enterprise Risk Management) are very solid instruments to ensure that the company will pass the audit of their internal IT control and information security management system.'[74]

89 Thus, central goals to meet the requirements of this Directive are as follows:

- transparent and documented business processes,
- transparent and documented IT architecture,
- identity management, and
- compliance through internal control system (ICS).

b.) Observations

(1) General

90 Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, including EU data protection reform and cloud computing, tried to summarize the positive impacts of the data protection reform for cloud businesses:

> *[..W]e have proposed rules more relevant to a networked, connected world. Clouds cross borders, and so does the data they hold. So we will make it easier to operate Clouds both within and outside our Single Market.[...] Globally operating businesses will benefit from changes to the use of binding corporate rules. They only have to get authorisation from a single authority; and there is more recognition of the variety of structures used in Cloud Computing. That will make the use of BCRs less burdensome and more effective.This legal framework is a sound basis for the Cloud. But I am confident that many Cloud providers will choose to go further, and take additional steps. Because strong protection and respect for privacy make good business sense. From our public consultation, we know people are concerned about which Cloud providers they can trust. And let's not forget that even in established areas like online shopping today less than one in five people feel in complete control of their personal data. [...] our proposal balances protection with efficiency. Safeguarding Europeans' rights – without putting the development of valuable new products and services 'off limits'. These three concrete things – Cloud-friendly data protection rules, a Cloud Partnership to make our public money count, and a supportive home for legal content – only make up a part of the European Cloud Computing Strategy.[...]*[75]

91 In the author's opinion, there are still some issues that have to be addressed in the reform's further consultations:

(2) Concept of personal data

92 The current definition of personal data in the EU-DPD is unclear. Information may be personal data or not depending on how it is encrypted or anonymized before being processed. In many cases, cloud providers may not even know if data processed by their services is personal data. Liability for cloud provid-

ers outside the EU or EEA depends on their customers' choices.

93 Thus, the future concept of personal data in the cloud should be based on the realistic risk of identification. Whether data protection rules apply or not should be based on all facts of the situation that carry the risk of harm.

94 It should also be clarified which procedures for encryption or anonymization are accepted by the updated EU-DPD.

(3) Jurisdiction and applicable law

95 The current legal uncertainties (see above) may discourage the use of European data centres or European cloud computing service providers. This could lead to a significant disadvantage for European e-commerce. It is clear that data protection laws may differ between EU member states, and that practical recommendations are needed relating to whether the Directive can be enforced in non-EU countries. Therefore, clarification is needed by the Commission on which and when a country's security requirements and other rules apply to a cloud computing user or provider. The European framework on data protection is still based on the country-of-origin rule, so data protection obligations should apply to entities based on this rule within the EU, and based on directing or targeting their services to EU consumers for non-EU providers. The present EU-DPD does not adequately balance the interests of data protection and the free flow of data, especially if services of cloud providers in third countries beyond the EU are concerned. Clearer rules are needed on the determination of 'establishment' and 'context of activities' for controllers in Article 4 (1a) EU-DPD.

(4) Accountability

96 The Directive fails to acknowledge the interacting positions between controller and processor in a cloud surrounding. They may overlap, and cloud computing service providers may be unaware that the data they process or store on behalf of a customer is classified as 'personal data', possibly because the controller fails to inform the processor. Ian Walden, professor of information and communications law, says:

> *The law should be updated to treat cloud computing service providers, in certain circumstances, as neutral intermediaries with immunities from data protection obligations. [...] If they unwittingly store 'personal data' they should have defences based on lack of knowledge or control. There should be different levels of responsibility depending on the nature of the service being provided.*[76]

(5) International data transfer

97 The Directive places restrictions on personal data being exported out of the EU, which seems outdated, particularly as remote access is now the norm on the Internet. 'We suggest that the Directive's focus on data location and the restriction on exporting data outside the EU should be replaced by requirements on accountability, transparency and security. It is not where information is stored, but how securely it is stored, and who can access it, that matters most,'[77] says Kuan Hon, paper co-author and researcher on the Cloud Legal Project.[78]

98 Until then, European users of non-EU/EEA clouds should make sure that their cloud agreements include both the EU standard contractual clauses and comply with their respective national rules regarding contract data processing. Furthermore, the parties should give specific attention to the description of the locations of data processing facilities and the identity of the cloud's operators; they also should agree on data security certifications or independent third-party audits. In the best case, cloud providers do offer different options for security levels and data processing locations.

3. Bilateral conventions

a.) Facts

99 Cloud computing businesses take place primarily between the big players in this area, the US and the EU. To avoid difficulties of a multilateral convention, it could be helpful if the US and EU led the way by preparing and exemplarily drafting a bilateral convention, at the same time getting over the never-ending story of transatlantic dispute.

100 The last decade illustrated significant EU-US differences about the meaning of privacy and data protection. Such a dispute became evident when 1) the impact of data protection regulation could not be limited to the geographic territory of the originating jurisdiction, and 2) state capabilities and authorities in other affected jurisdictions were 'constrained to the point where impacts cannot be mitigated'.[79]

101 Particularly the EU-DPD had an impact on transatlantic conflicts. This Directive was designed to protect Europe's data privacy. As mentioned above, in a world where data flow is likely to be a cross-border issue, 'that regulation must reach beyond the EU if it is to be meaningful, it must apply wherever the data are transferred and processed'; thus, 'domestic legislation' has a transnational footprint'.[80]

(1) Transfer of Air Passenger Name Record (PNR) Data

102 Following the terrorist attacks of 9/11, the US passed legislation in November 2001 providing that air carriers operating flights to, from or across US territory had to provide US customs authorities with electronic access to the data[81] contained in their automated reservation and departure control systems, called 'passenger name records' ('PNR'). The following political negotiations between the European Commission and the US Department of Homeland Security (DHS) concerned the transfer and use of European air passengers' data to US authorities in the fight against terrorism and other serious crimes.

103 A new, controversial PNR interim agreement between US and EU was signed in July 2007 and expired on 31 July 2007. On 1 August 2007, a new agreement, which has a maturity of seven years, entered provisionally into force, replacing the interim agreement.[82]

104 On 5 May 2010, the European Parliament decided to postpone the vote on PNR until the use of PNR is clarified with respect to EU law and European Parliament concerns about privacy, proportionality and redress. Nevertheless, the European Parliament clarified its conditions for approval:

- PNR data can only be used for fighting terrorism and organized crime.
- Use of PNR data must be in line with EU data protection standards.
- Use of PNR for data mining and profiling is to be forbidden.
- Forwarding of data to third countries must be limited to a specific need and regulated by means of a binding international treaty.
- PNR data may only be provided on request – i.e. the push method.

105 On 21 September 2010, the new package of proposals was presented by Commissioner Malmström. 'The Commission's proposals largely reflect the requirements set out by the European Parliament,' said Sophie in 't Veld, rapporteur for the resolution on the agreements with the US and Australia on the transfer of PNR, in her initial reaction. She continued,

> *One of the main demands, namely that the use of passenger data has to be drastically restricted, has been accepted. The proposals will have to be studied by Parliament's Civil Liberties committee but they have been welcomed by Liberals and Democrats as a constructive package that represents a big improvement on the past. The main outstanding point of criticism is that the need for massive storage of data still has not been proven. It is not enough to say that the collection of data of passengers is 'useful' or 'valuable'. It must be 'necessary' and 'proportional'.*

106 As far as Ms In 't Veld is concerned, the Commission proposals still need some improvement on these points.'We will carefully scrutinise the outcome of the negotiations. The European Parliament will pull the plug if it is not satisfied with the progress,' she continued. 'The EP, under the Lisbon Treaty, has the right to vote down the agreements already in place, as well as giving its consent to any new agreements.'[83]

(2) Safe harbor

107 The objective of the US-EU negotiations leading to the 'safe harbor agreement'[84] was to find a solution that would ensure the adequacy of protection of European data consistent with American preferences for reliance on self-regulation and market mechanisms. Safe harbor includes principles thatare consistent with both the OECD Privacy Guidelines and the EU-DPD. An organization can enter safe harbor by either joining an approved self-regulatory program or developing its own compliant privacy policy and certifying it annually to the Department of Commerce. Each organization subscribing to these principles would be presumed to be providing adequate privacy protections. Enforcement of safe harbor is achieved by prosecution for unfair or deceptive advertising or promises by the FTC. Kobrin describes safe harbor as 'not an overwhelming success on either side of the Atlantic',[85] and Reidenberg argues that it is a 'weak, seriously flawed solution for e-commerce' that is no more than a mechanism to 'delay facing tough decisions about international privacy'[86]. European criticism about safe harbor concerns the fact that the number of organizations self-certifying under safe harbor is lower than expected, many of those do not really meet the requirements of the agreement and less than half of those organizations post privacy policies that reflect all seven safe harbor principles.

108 German data protection authorities have placed a significant new duty on German companies transferring personal data to the US. The joint panel of the German data protection authorities (so-called DüsseldorferKreis) passed a resolution on 28/29 April 2010,[87] setting stricter due diligence requirements for the personal data transfer under the safe harbor principles. German companies should now document their due diligence inquiries and responses. US companies importing data from Germany should accordingly expect requests for appropriate documentation and be prepared to assist their German counterparts with this new due diligence process.

> *With regard to the US, the European Commission adopted the decision on safe harbor whereby for the purposes of Article25 (2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the safe harbor privacy Principles [...] as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked*

questions [...] are considered to ensure an adequate level of protection for personal data transferred from the Community to organizations established in the United States.[88]

109 Safe harbor principles and the accompanying Frequently Asked Questions[89] set forth the provisions ensuring the adequate level of data protection. Nevertheless, national supervisory authorities often look critically at the level of protection in these principles. Sometimes the representation by a US entity that it is safe harbor-certified is not enough now according to national supervisory agencies because, in their view, EU and US regulators currently do not ensure that the US companies comply with the self-certification.

b.) Observations

110 Concurrent to European Commissions consultations on the reform, a new bilateral EU-US agreement could be drafted as a first important step in bridging the existing differences on the application of data protection laws that 'would make it then easier to achieve a common approach on protecting personal data online in the businesses world'.[90] Although the EU is negotiating with the US on data protection in judicial and police cooperation in criminal matters, it will not constitute in itself the legal basis for transfers of personal data related to cloud computing issues. Such transfer of personal data will still require a specific agreement providing a legal basis. An EU-US agreement could become the reference for data protection standards that apply whenever personal data needs to be transferred across the Atlantic. It would also save time and energy in any future negotiation of data transfer agreements because these talks would be based on this umbrella agreement. The aim has to be to negotiate a data protection agreement that contains all the necessary high-level data protection standards. It could lead to a win-win situation: The US could benefit immediately since high data protection standards would guarantee legal certainty and facilitate data transfers to and from the US much more easily than is currently possible. At the same time, the EU should continue to promote the development of high data protection standards at the international level by cooperating with relevant international organizations and actors (e.g. the OECD, the CoE, and the UN).

4. Multilateral conventions

a.) Facts

(1) United Nations (UN)

111 International recognition of privacy as a human right can be traced back to Article 12 UDHR.[91] The UDHR was the first international instrument to deal with the right to privacy. Because of its form as a resolution it is not legally binding; the same applies to the 'International Covenant on Civil and Political Rights' (ICCP).[92] The only instrument explicitly mentioning privacy issued so far by the UN also takes the form of a non-binding guidance document, the 'UN Guidelines concerning computerized personal data files'.[93] These guidelines contain minimum guarantees in privacy law that should be implemented in national legislation and are expressed in basic principles. But the UN has not made privacy principles enforceable within UN organizations.

112 The UN Computerized Guidelines were the earliest such guidelines to contain high-level data protection principles, but as they are not legally binding they have been of limited practical relevance. The OECD Privacy Guidelines 1980 are also not legally binding but have been highly influential in inspiring the enactment of privacy legislation in many regions around the world.[94]

113 The International Standards on the Protection of Personal Data and Privacy adopted in Madrid on 5 November 2009, at the 31st International Conference of Data Protection and Privacy Commissioners was the turning point for global data protection standards.[95] It is a non-binding resolution, but the intention was to pave the way for an internationally binding agreement, probably via the UN. The advantage of the Madrid Resolution is that it has been backed by representatives from the major Internet companies[96] as well as by data protection authorities; this gives it some authority. The key element of the agreement could be that it is based on the higher data protection standards of the EU rather than the lowest common denominator, so it harmonizes up rather than down. The language used is very close to that of European data protection law, which suggests that it would require non-EU privacy standards to be significantly improved. Thus, 'the agreed international standards are a milestone for modern privacy. Now it all depends on filling these standards with life.'[97]

114 The 32nd International Conference of Data Protection and Privacy Commissioners continued this trend by enacting a resolution, this time with special respect to the adoption of global privacy standards. It called for an intergovernmental conference to negotiate a binding international agreement guaranteeing respect for data protection and privacy and facilitating cross-border coordination of enforcement efforts. It repeated the same appeal in 2012:

In line with the Jerusalem resolution, the Conference will continue to promote the Joint Proposal for International Standards in all relevant international fora (e.g. OECD, Council of Europe, APEC) and its efforts to organize an intergovernmental Conference for developing a binding international instrument. In this regard, it could been visaged to convey govern-

ment's representatives at the next Conference meeting in 2012 in order to engage a dialogue in that perspective.[98]

(2) Organisation of Economic Cooperation and Development (OECD)

115 In 1980 the OECD published the OECD Privacy Guidelines, whose core is made of eight privacy principles for both the private and the public sector. The Guidelines are not legally binding on OECD member states but have been 'highly influential on the enactment and content of data protection legislation in countries outside Europe' and for the APEC Privacy Framework.[99] The following OECD Guidelines dealt not directly with privacy but with information society,[100] cryptography policy[101] and consumer protection in electronic commerce.[102] Some OECD declarations and reports have served as the basis for the OECD privacy protection work since 1985.[103]

(3) Asia-Pacific Economic Cooperation (APEC)

116 Far from the EU perspective, privacy is treated as a consumer concern, taking personal data as marketable goods and trying to balance their protection with private interests. This was the approach when drafting the' APEC privacy framework'.[104] The significance of the APEC economies cannot be doubted, as they are located on four continents, with more than a third of the world's population and almost half of the world trade.[105] The goal – and the advantage of the framework compared with the EU-DPD–is to 'establish a more flexible framework within which member economies can develop their own laws and policies that are compatible with other economies in the region'.[106] The framework consists of nine 'APEC Privacy Principles' in part III.

117 These principles can be criticized in several points. First, they are based on the 'OECD Privacy Guidelines' principles, which are no longer adequate to deal with the new dimensions of privacy related, for example, to the Internet. Secondly, the framework further weakens the OECD principles, does not reproduce all of the OECD principles, lowers the content of principles and improves on some OECD principles in only minor ways. The only new principles 'carry inherent dangers and have little to recommend them'.[107] Furthermore, the APEC framework does not include any considerations on how to treat the EU adequacy (Art. 25 EU-DPD) issue. Last, it ignores the regional legislation and experience of privacy law.[108] Thus, the APEC framework is largely consistent with the OECD Privacy Guidelines, and was therefore only an acceptable framework on privacy principles from twenty years ago. Particularly, the principles are 'for the most part unremarkable and deal with issues normally covered by international privacy laws'.[109] It might eventually emerge as a counterweight to European efforts because of its flexibility, its facilitation oftrans-borderdata-flows and the positive impact on economies in the Asian-Pacific region without any privacy legislation, but 'it remained a policy document with little implication for cross-border regulation'.[110]

118 On 13 November 2011, the APEC leaders endorsed the APEC Cross-Border Privacy Rules[111] (CBPR) system at an APEC meeting in Honolulu, Hawaii. The leaders agreed, among other things, to 'implement the APEC Cross-Border Privacy Rules System to reduce barriers to information flows, enhance consumer privacy and promote interoperability across regional data privacy regimes.' It is necessary to understand the opportunities and challenges offered by the CBPR system.

119 The ratification by the Ministers established the Joint Oversight Panel (JoP), commenced the recognition of Accountability Agents (AAs), and facilitated participation by economies in the CBPR system.The work plan of 2012 includes the development of the website that will list participating businesses, recognized AAs and Privacy Enforcement Authorities (PEAs), and further promotion and explanation of the system. It remains to be seen which economies will agree to put resources into the JoP – a minimum of three economies need to join the JoP. Those with existing privacy and data protection laws and PEAs may not, given their existing requirements for international data transfers. The whole system of the CBPR programme requirements is hard to understand, and participating businesses could possibly face a more onerous application process and bureaucratic requirements than they do in those APEC member economies with privacy laws, and arguably even than they do in EU member states, whose 'notification' regimes the APEC initiative was designed to avoid replicating. However, if the CBPR certification process and subsequent monitoring are carried out in good faith (a big 'if'), then the result could be a higher level of proactive compliance with privacy rules than most regimes have managed to achieve to date.[112]

(4) Other non-binding policy standards

120 Various groups have issued non-binding policy documents, e.g. the 'Global Privacy Standard'[113] by the Ontario Information and Privacy Commissioner or the 'Global Network Initiative' by a number of companies, non-governmental organizations, and academics, which is defined as 'a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector'.[114]

b.) Observations

121 A multilateral convention could produce a greater degree of harmonization, since it results in a single text that is legally binding on states that enact it.

But such a binding nature can also make states reluctant to do so. The possible convention could be faced with reservations made by states that are party to it, which can result in a diminution of the very harmonization that the convention was supposed to accomplish, and a convention can be difficult to amend in the face of changing practices or technological evolution.[115] Furthermore, the drafting of any such convention could take many years. Moreover, although a multilateral convention is legally binding in international law, it may still not produce a harmonized legal framework.

122 It is also doubtful which international body could bridge these differences. In the author's opinion, there are only a few bodies nearly sufficiently strong, dynamic and representative. A multilateral convention on privacy could be drafted by the International Law Commission (ILC). The ILC was established in 1948 under a resolution of the UN General Assembly;[116] it is charged with promoting 'the progressive development of international law and its codification'[117] and has adopted the 'protection of personal data in trans-border flow of information' in its long-term work program,[118] which could potentially result in the draft of an international convention. Another option could be to sling this issue over the shoulders of the General Agreement on Trade in Services (GATS) under the auspices of the World Trade Organization (WTO). The focus of the GATS is on trade liberalization and promoting economic growth.[119] Thus, although the commercial purposes of ubiquitous data flows across national borders seem to fit with the WTO focus, it is doubtful whether the WTO would have the ability to negotiate such an agreement quickly and efficiently; its ability would be 'hampered by its commercial bias'.[120] Other international organizations such as the United Nations Educational, Scientific and Cultural Organisation (UNESCO) and the International Telecommunications Union (ITU) are too specialized and may not be well prepared to produce standards in an area as diverse and multi-faceted as privacy.

123 The APEC framework is designed to be a more flexible system than the adequacy approach. It can be implemented in the vastly differing cultural and legal frameworks of the twenty-one APEC member states, but it would likely take years for it to become widely accepted on an international scale. Although the APEC model of self-regulation is likely to spread widely, it would spread thinly. And although the Asia-Pacific Privacy Authorities Forum (APPA) since 2005 'is becoming more organised and purposeful, it has not yet found a substantive role in the region's privacy protection'.[121]

124 The suggestions from the APEC consultations in 2011 of meeting the CBPR programme requirements was taken further in a paper that addressed the problems of interoperability. This paper was drafted by the International Chamber of Commerce (ICC) and stated that businessescould be recognized as compliant with the APEC Privacy Framework Principles without having to go through the processes established for the CBPR system. This illustrates that CBR still needs some work on bridging problems of interoperability. A positive effort of APEC is encouraging to see participation in APEC processes by more NGOs; the Electronic Frontiers Foundation (EFF), Center for Democracy and Technology (CDT), the Internet Society (ISOC) and Privacy International attended some of the 2011 meetings. The EU's system of binding corporate rules has some similarities with the CBPR system, reflecting its overall non-binding approach. It also remains uncertain whether, or how, the CBPR will be implemented over the next few years.

II. Private law

1. Terms and conditions

a.) Terms of use

125 Terms of use could provide an adequate protection of personal data if some key issues have been observed in the contractual relationship between cloud provider and cloud user:

- Anonymization of the data for trans-border data flow is possible
- Movement of data will be controlled
- Data encryption is provided
- Cloud user can access all of data anytime anywhere
- Exit scenarios for the future transfer of the data to other cloud providers
- Backup/restore plan
- Data breach notification
- Service levels and emergency plan in case of unavailability
- Commitment can be obtained regarding
  - the place where the data will be processed;
  - the exact chain of supply;
  - contract parties, their roles, rights and obligations, especially in case of multiple cloud platforms involved; and

- the period of data retention and treatment of data after termination or insolvency.

b.) Consent

126 The processing of data in a non-EU/non-EEA country may be lawful if the affected people (e.g. customers or employees) have agreed expressly and voluntarily to the processing of their personal data in an 'unsafe' third country. However, because of the strict requirements for a legally binding approval and the possibility of cancellation at anytime, this instrument is not often practicable.

2. Standard contractual clauses (SCC)

127 The Council and the European Parliament have given the Commission the power to decide, on the basis of Article 26 (4) of Directive 95/46/EC, that certain SCCs offer sufficient safeguards as required by Article 26 (2). However, it is admitted that individual contracts do not, of course, provide an adequate level of protection for an entire country. The European Commission has approved two alternative sets of SCCs for use in transferring personal data to a data 'controller' outside the EU/EEA (SCC I and SCC II), and a set of SCCs to be used when transferring data to a 'processor' (SCC-DP).

128 SCCs are contract defaults, complementing and specifying the demanded minimum standards of data protection (Art. 25 (2) EU-DPD). The rights and duties of the parties are regulated and must be adopted consistently. The member states are bound by the decisions of the EU commission. Thus, the member states must recognize that the companies which use the SCCs show an adequate data protection level. Then permission by the supervisory authority is not obligatory if the supervisory authorities are able to check the use of the contractual clauses and they are presented to the authority on inquiry. As soon as modified contractual clauses are used, however, an official authorization by the supervisory authority must be caught up.

129 SCCs are not used where data is being transferred to a US company that participates in the safe harbor program, or to a company relying on informed consent, Binding Corporate Rules approved by one national supervisory authority, or one of the other derogations under Article 26 EU-DPD. US companies that have not self-certified for safe harbor and other countries beyond the EU still have a further possibility to ensure an adequate level of protection. According to EU-DPD, a transfer to a third country that does not ensure an adequate level of protection may take place in cases 'where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights'; the Directive continues by stating that 'such safeguards may in particular result from appropriate contractual clauses' (Art.26 (2) EU-DPD).

130 In some way,the SCCs recognize the difficulty of data subjects to seek compensation–not only by establishing the applicable law and the responsibility of the data exporter, but also by providing that alternative dispute resolution (ADR) could be used as well as that the data subject could be represented by entities (recitals number 20, 21 and 22 of Decision 2010/87/EU). In case it is not possible for the data exporter to seek compensation, the same decision says that the data importer should offer the means for ADR.

131 The SCC I was adopted by the EU in 2001. However, it appeared afterwards in practice that the realities of the data transfers as well as the application of current business models had not been adequately considered. Thus, practitioners often did not apply these contract defaults. The most practice-related case in which data should be transferred by a data controller to a data processor was not covered, and the bureaucratic requirements were relatively high. This hindered the application of SCC I although SCC I was especially intended to facilitate the data flow. Besides, companies often did not accept their obligation to agree on conciliatory proceedings over liability.

132 Under SCC I, the data exporter and data importer were jointly and severally liable. They were indemnified from it only if neither would have been found responsible for the violation of personal data (clause 6 (1)). Between the parties, data exporter and data importer are obliged to declare indemnity if they have included the optional clause 6 (3) in the contract. In particular because of the problems thatresult from this joint and several liability, SCC I wascriticized and seldom used.

133 From 15 November 2010 on the new SCC II must be used; the old clauses were amended. Already-existing arrangements keep their validity as long as data is transferred and transmission as well as processing remains unchanged in the contractual relationship. The concerns addressed in SCC II are that processors today often subcontract some processing, storage and technical support functions to third parties. This is common in cloud computing, where several entities might be involved in handling and storing the data. SCC II is designed to ensure that the company that remains responsible as the data controller in Europe is informed about any proposed subcontracting, and that all parties handling the data are subjected to the same obligations of confidentiality and security. It contains a mandatory arbitration clause to which many companies have objected. Four different liabilities for the breach of data protection rules can be identified: contractual liability according to SCC II (either between the contracting

parties or against third person), and tortious liability (based on SCC II or national law).

134 Between the parties of SCC II, every contracting party is liable 'inter partes' for the damages caused by an offence against the clauses. This liability is limited to the de facto suffered damage; 'punitive damages' are therefore excluded.[122]

135 In case of damages to a third person, every party is liable for damages caused by the infringement of rights that arise for an affected third person directly from the SCC II. The affected person can immediately assert his right against the data importer or data exporter as a third-party beneficiary under one condition: if the data importer infringes obligations from the SCC II, the data exporter must first take action for the affected person and act upon the data importer to fulfil the latter's obligations. Only if the exporter is not able to remedy the wrong conduct of the data importer within one month can the affected person proceed directly against the importer.

136 When the tortious liability is to be applied, the data exporter is liable for offences conducted by the data importer because of fault through the poor choice of one's vicarious agent (culpa in eligiendo) if he did-not assure himself within a reasonable scope of time that the data importer was able to fulfil his juridical obligations. Nevertheless, the data exporter can absolve himself from liability if he proves that he has taken all reasonable efforts to fulfil his obligations of choice (Annex, Clause III b s. 2).

137 All the SCC II regulations mentioned do not change the liability of the data exporter according to national data protection laws, which remain untouched because these cannot be excluded by contractual arrangement between the contracting parties of the SCC II. If the SCC II default documents are adopted by the parties without changes, an authorization by a data protection authority of an EU member state is not necessary. The current SCC II permits the simplified employment of subsidiaries. Indeed, an EU-based company must make sure that the subsidiary complies with the European data security level.

138 If personal data is transmitted within the scope of contracted data processing from the EU in a third country, the SCC-DP[123] applies. Contracted data processing is when a company orders personal data – for example, customer data or employee data – to be processed by a foreign company (see above). In this particular respect,relevant areas of contracted data processing are forms of IT outsourcing (external data servers, external human resources data management, etc.). The SCC-DP covers transfers from the EU to a data in a third country, although data protection authorities 'may' allow use of the SCC-DP in such situations as well.

139 Annex Clause 6 (1) SCC-DP obliges the parties to grant to the affected person a contractual claim for compensation against the data exporter because of certain breaches of obligations of the data importer and/or the subcontractor. Annex Clause 3 (1) SCC-DP provides direct claims of the affected person against the data exporter. Exceptionally, the affected person can also proceed directly against the data importer if the latter or his subcontractor is responsible for a breach of obligations and the data exporter no longer exists on a factual or juridical basis (Annex Clause 3 (2) SCC-DP). The arbitration clause has been deleted.

3. Binding corporate rules (BCR)

140 BCRs serve to create a uniform contractual basis for the exchange of personal data in an affiliated group (Privacy Policy). An adequate data protection level can thereby be guaranteed at all companies of the group but not to group-external companies. This solution, also called 'Safe Haven', is based on the expression of safe harbor.

141 A liability regime corresponding to Article 22, 23 EU-DPD has to be included in the BCR. If the head office of the affiliated companies involved in the data transfer is inner-European, this office is liable for the breaches of contract of all itsaffiliated companies beyond the EU. If it is not seated in the domestic market, a group member resident in the EU must be named by the group of companies. This 'liable team member' must prove that it has sufficient assets to pay compensation for damages resulting from the breach of the BCRs.[124] If the involved companies have their seats in different EU countries, the regulations in the BCR must be approved by everysingle responsible authority (in Germanythis is coordinated with the 'DüsseldorferKreis'[125]). The liable team member must not compensate for breaches of other inner-European team members.[126]

142 The same rights must be granted to the affected person towards the liable team member, as if the liable action had been committed by a member within the EU. This regime has contractual rather thanlegal liability. Its results are determined by the applicable (substantive) law – e.g. in Germany or Spain, according to the BCR. This shows how important the determination of the applicable law is for cases of data transfers to third countries. Another significant question then remains: To what extent are restrictions of liability allowed? The Article 29 Data Protection Working Party gives no exact statement on this.

4. Observations

143 An adequate data security level is thereby guaranteed at all companies of the group, but not to com-

panies beyond this group. Besides, until recently the implementation of these required company regulations was still relatively complicatedin spite of some simplifications. It is also possible for the companies involved in a cloud to submit themselves to BCRs, by which an adequate level of protection (Article 26 par. 2 EU-DPD) should be produced by contract. According to the recommendations of the Article 29 Working Party, the head office or one group member named by the group of companies must answer within the scope of BCR for the offence of all affiliated companies beyond the EU. These BCRs need authorization by the responsible data protection authorities.

144 At the international level, the Cloud Security Alliance[127] (CSA), dominated by the US, has been formed; its aim is to compile guidelines for secure cloud computing. With the advent of EuroCloudDeutschland_eco[128] there is also a new organization for the German cloud computing industry, which is integrated into the European EuroCloud network. EuroCloudDeutschland_eco has come along to the assignment to create more transparency for the users, to introduce a quality seal, to clear legal questions, to promote the dialogue between suppliers and users and to provide cloud computing competence. An international framework would certainly make it possible to lift the local dependence of data processing and to exclusively apply the legal framework where the cloud user or the direct contracting partner of the user as a cloud supplier is based. Up to now, however, attempts in this direction have not been evident. In view of the non-uniform and partially lacking and insufficient national laws for data processing in general and especially for data security, international norms are not yet realistic. Hence, there is no alternative to the enforcement of a clear juridical protective regime that begins at the responsible place where the cloud user is based. Researchers, economists and supervisory authorities are asked to compile standards – to elaborate so-called Protection Profiles for Clouds with the responsible organizations – as well as to develop auditing procedures. Specific standard contract clauses still to be compiled or Binding Corporate Rules can serveas a preliminary stage for a global standard. The still-existing basic principle of a 'free cloud' is not enough for the requirements of modern data security; it can be understood only as an experimental application from which 'trusted and trustworthy clouds'[129] have to be developed with integrated data security guarantees. These trustworthy clouds must be made available in the market.

145 If the requirements of contract data processing are fulfilled, the SCC should be used for processing to a third-country service provider. If the transmission of the data must be considered not as contract data processing but as a transfer of function, then the use of the SCC-DP is recommended. If both purposes overlap – for example, if parts of a data transfer are contract data processing while other parts are classified as a function transfer – given that both parts of the data are separable, the SCC should be used for the first and SCC-DP for the second part. If such a separation is not possible or practical the SCC should apply.

III. Technological and private sector perspectives

146 An exhaustive review of the necessary technical and organizational precautions is impossible in this legal analysis, but it is vital to illustrate some of their most important impacts on the regulation of cloud computing issues. Based on common technological solutions, businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems are actually meeting data protection laws and enhancing privacy.

147 Professor Lawrence Lessig famously proclaimed that 'code is law', that 'the software and hardware that make cyberspace what it is regulate cyberspace as it is'.[130] Technical standards for data processing could probably lead to globally harmonized data protection practices more swiftly and effectively than an international convention could. They have been promulgated by international bodies such as the International Telecommunications Union (ITU) and the World Wide Web Consortium (W3C). Regional bodies and several organizations are also working on data protection standards.[131] These 'have proven highly influential for the processing of personal data'.[132] Similar to the advantages of the accountability principle, technical standards may be more influential in determining how personal data is processed than most laws are. One weakness of technical standards is that they may be implemented differently in different regions and sectors; thus, European regulators are taking steps toward drafting them carefully and integrating them into the framework of data protection laws. They must also be rapidly adapted to new technological developments; otherwise they could be overtaken by them. Thus, while technical standards are likely to play an increasingly important role to support data protection laws if the goals and techniques of social and economic regulation are clearly distinguished, they are unlikely to be a complete solution.

1. The technical and organizational data security measures required by Article 17 EU-DPD 1

148 These measures must be expressly set out in the cloud computing service contract. Security by trans-

parency together with state-of-the-art security measures should be the aim.

149 This could be achieved with a multi-level access regime, encryption capabilities and possibly aliasing tools. In cloud computing, multiple users work on the same computers and platforms—a practice that presents risks unless stored data are adequately separated. To ensure compartmentalization of individual contract relationships, the cloud contract must clearly specify the methods used to separate data from different principals. If this is achieved with encryption, tests must be run to ensure that the system offers adequate security and cannot be easily compromised by other users or by the provider itself. The user must be given access to the abovementioned range of options via a convenient interface, along with the support required to implement user-driven application security. Both the cloud provider and the entire cloud network must implement a documented data privacy management system, to include IT security management and an event management system. We have already discussed the need for transparent audits by an independent entity. Unfortunately, however, the laws regulating this type of audit remain extremely limited.[133]

2. Certificate authorities, guidelines and elements of self-control

a.) German guidelines of BITKOM and BSI

150 The German 'Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V' (BITKOM) issued guidelines on cloud computingin October 2009. The BITKOM focuses mainly on cloud computing as a business innovation, a business model, its integration in IT architecture and its scenarios for application.

151 The 'Federal Office for Information Security'(BSI) defined minimum requirements for cloud computing providers. Cloud computing/compliance is explicitly addressed on page 16 of the guidelines.134

b.) ENISA

152 The European Network and Information Security Agency offers a risk assessment on cloud computing business model and technologies. The result is an in-depth and independent analysis[135] that outlines some of the information security benefits and key security risks of cloud computing. The report also providesa set of practical recommendations.

c.) Observations

153 Elements of self-control do in fact support compliance with data protection laws only if each partner of the cloud service contract meets the guidelines' requirements. The problem remains for cloud users to prove that the contract partner fulfils all requirements set out in the contract. Approaches could be as follows:

- conclusion of a Service Level Agreement (SLA);
- periodic control/audit (not realizable in a dynamic cloud surrounding);
- ISO 27000;
- reliance on BSI (cloud user within Germany) or ENISA (cloud user within EU) Guidelines;
- agreement upon a Privacy Seal, e.g. the Privacy Seal of the Data Protection Authority of Schleswig-Holstein;[136]
- common criteria; or
- restriction on networks of trusted partners instead of direct audits.

3. International standards

a.) Ontario Global Privacy Standards and Privacy by Design

154 In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, a Working Group was convened for the purpose of creating a single Global Privacy Standard. This Group tried to harmonize various sets of fair information practices into one Global Privacy Standard. The first step was a 'Gap Analysis', a process of comparing leading privacy practices and codes from around the world, comparing their various attributes and the scope of the privacy principles enumerated therein. After identifyingstrengths and weaknesses of the major codes in existence, the Group tabled its Gap Analysis with the Working Group of Commissioners. The work on harmonizing the principles into a single set of fair information practices led to the development of the Global Privacy Standard (GPS),[137] which builds upon the strengths of existing codes containing privacy principles and reflects an enhancement by explicitly recognizing the concept of 'data minimization' under the 'collection limitation'principle. After some subsequent drafts, the final version of the GPS was formally tabled and accepted in the UK on 3 November 2006 at

the 28th International Data Protection Commissioners Conference.

155 Privacy by Design is a concept brought to light by Ann Cavoukian, Information & Privacy Commissioner from Ontario, Canada:

> *Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS Plus — taking a positive-sum (full functionality) approach, not zero-sum. That's the 'Plus' in PETS Plus: positive-sum, not the either/or of zero-sum (a false dichotomy). Privacy by Design extends to a 'Trilogy' of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure. Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.*[138]

b.) Privacy Toolkit

156 The 'Privacy Toolkit',[139] published by the Task Force on Privacy and the Protection of Personal Data of the International Chamber of Commerce (ICC), is an example of another private sector instrument. This toolkit is an international business guide for policymakers and aims at governments seeking an innovative approach to privacy that balances the needs of governments, individuals and the economy as a whole. It outlines guiding principles for privacy that draw upon the OECD privacy guidelines and suggests practical ways to put the principles to work:

> *ICC fully supports the fundamental right to privacy and encourages businesses to comply with national and international privacy rules. But working with governments to implement privacy protection requires early policy input into how privacy rules are created while keeping in mind that overly restrictive or conflicting privacy requirements can be a big barrier to international business. Privacy Toolkit was developed to communicate the business approach to privacy protection and to serve as a guide for governments developing their own policies. It outlines the characteristics and benefits of flexible privacy protection regimes that are built into business processes. The booklet was prepared by the ICC Commission on E-Business, IT and Telecoms. Christopher Kuner, Partner, Hunton & Williams, Brussels, and Chair of ICC's data protection task force, said: 'Privacy and business competitiveness are not either/or options. Appropriate privacy protection is a business enabler, not a barrier. But it's an ongoing process that needs to be responsive to new technology, business methods and opportunities. Flexibility is essential. Privacy Toolkit shows that the most important aspect of privacy protection is not how it is achieved, but simply that it works.' The booklet also includes a series of steps for governments to achieve appropriate and effective privacy protection regimes. Following Privacy Toolkit recommendations will ensure that the resulting privacy regime serves both business and the consumer without running the risk of stifling development, innovation and growth.*[140]

c.) ISO and IEC

157 ISO, the International Organization for Standardization, developed international standards in many areas that are essential to everyday life. On technology standards ISO and IEC, the International Electrotechnical Commission, which is responsible for standards in the field of electrics and electronics, are cooperating together.

158 In addition to legal standards, technical standards for effective data protection have a high priority because a large number of technical standards affect privacy interests to a considerable extent. Through a privacy-friendly design in these standards at an early stage, potential risks for privacy of individuals could be reduced or entirely eliminated. Unfortunately, the Data Protection Authorities rarely have an adequate possibility to apply their expertise in the relevant bodies, due to their existing equipment and staff and the great variety of technical standards.

159 The German Data Protection Authority of Schleswig-Holstein (ULD)[141] is involved in the joint Working Group 'Identity Management and Data Protection Technology' of ISO and IEC. Central standards the ULD is working on include the 'ISO 29100 - Privacy Framework', a framework standard that defines basic concepts and principles regarding privacy, and 'ISO 29101 - Privacy Reference Architecture', which outlines privacy-friendly IT architecture.

D. The destination: A privacy regime across the globe

160 Bygrave states that 'the chances of achieving, in the short term, greater harmonization of privacy regimes across the globe are slim'.[142] There are still substantial cultural and legal differences between various states and regions regarding their approach to data protection, and most of them still have no data protection law at all. In addition, there is increasing tension between the global nature of data processing and the still mainly national or regional nature of data protection law. Thus, there do not yet seem to be sufficient grounds for recognizing a global legal right to data protection in the same way that other fundamental, universal human rights are recognized.

161 Nevertheless, there is still hope, consisting in a mixture of many little steps and one simultaneous big stride. But what steps must be taken? The former

should combine some main rationales of the different legal frameworks on a short-term basis:

- The avoidance of gaps in data protection. The lack of harmonized standards for data protection around the world and the lack of any data protection legislation in most states create risks for the processing of personal data.[143]

- The facilitation of global data flows. A growing number of databases are made accessible globally on the Internet. Thus, the same data transfer may be subject to a large number of differing data protection standards, which creates substantial compliance burdens and uncertainty for business, and particular problems with transatlantic data conflicts.

- The installation of an international body, responsible for further consultations towards an international legal analysis of a draft paper on global data protection. As data protection law is a mixture of various legal areas – such as human rights law, public law, private law, and others – it makes it difficult to find a sufficiently strong, dynamic and representative international body. The WTO is occasionally named as such a body, but it is hampered by its commercial bias. The ILC already has produced instruments in many areas of public international law, but it does not seem well suited to deal with a strongly politically charged area like data protection. Institutions such as the Council of Europe seem to be too closely tied to one region, and the OECD has a limited membership. Other international organizations such as the ITU, UNESCO or the WTO seem too specialized. Thus, the draft of a truly international convention within the framework of the UN seems more promising, initiating a UN Human Rights Council-sponsored process with a view to a future global treaty.

- The recognition of the technology itself as a third party between data controllers and data subjects, using new technologies towards information and communication technology (ICT) privacy measures. The authorities charged with data protection must penetrate the forums[144] where important decisions are being made-about technical network infrastructure, communication protocols and the characteristics of our browsers.

- The unification of the most eminent specialists worldwide in data protection law under the ILC authority, as the official legal advisor for the UN and responsible for the further development of worldwide principles. These should require the following: the principles of openness in personal data systems, liability in operation of the systems and responsibility of the data-keepers for following legal and procedural guidelines. Furthermore, data held should not be excessive in relation to the stated purposes of the systems, proscribing release or sharing of data held in files without the consent of the individual, and foreseeing creation of national-level public offices charged with monitoring and enforcing individuals' interests in treatment of 'their' data.[145]

162 Solve problems within the EU-DPD's reform, which Professor Millard, leader of the Cloud Legal Project at Queen Mary, University of London, perfectly outlines:

> *Unless further changes are made to clarify and harmonise data protection rules across the EU, the draft Regulation may drive business away from Europe, and still fail to deliver effective protection for individuals. Uncertainty will persist as to whether particular non-European cloud providers and cloud users are regulated in the EU and, if so, which law(s) will apply to them. This may discourage the development of EU data centres and the use of EU cloud services generally. Furthermore, the draft Regulation fails to close a loophole which may undermine protection for some EU residents when they use services provided by non-EU cloud providers. The use of cloud computing may also be inhibited by additional restrictions on the transfer of personal data outside Europe, including cumbersome regulatory approval requirements. Given the ease of global data transmission and remote access over the Internet, and the increasingly fragmented nature of data storage, what matters most for privacy and security is who can access the data in intelligible form. This is now more important for privacy than data location. The draft Regulation will impose substantial new compliance obligations on businesses, as well as greatly expanding the roles of the European Commission and national regulators, all of whom will need extra resources. It is unclear how this will be financed, especially in the current economic climate. The proposed abolition of registration fees is a step towards reducing red tape, but proper provision for the adequate funding of supervisory authorities in performing their expanded duties will be essential if the draft Regulation is to protect individuals and facilitate the free flow of data.*[146]

- The political integration of APEC into the draft of an international convention, maybe through a membership of the trade-friendly but at the same time EU-friendly WTO into the APEC Community, accessing APEC states to the CoE Convention 108 and to the Additional Protocol.

- The reduction of the scope of instruments to data protection, perhaps containing exceptions such as data processing by law enforcement.

- The finding of a balance between security and privacy issues. Maintain the efforts to prevent future terrorist attacks without infringement of individual privacy rights and civil liberties.

- The adaption of the level of strictness of global data protection standards. Kuner states that this balance puts future data protection law in a dilemma, because

if global standards were set too high, then it is likely that many States would be reluctant to enact them, while if they were set too low, then States and entities with a long tradition of data protection law might oppose them as watering down their existing standards (this could be a particular problem for the European Union).[147]

163 The latter should not let the ultimate goal out of sight of a globally binding convention of data protection. This big stride should be realized through a globalization of the CoE Convention 108. It is true that it would take longer to draft and approve such a multilateral convention, and experience shows that states tend to give a low priority to the implementation of such conventions; in addition, this convention would be subject to many more political hurdles, especially because of the difficulty of re-opening an existing instrument. But there are more advantages that cannot be ignored. The CoE initiative under Article 23 (1) signals a possible way of side stepping the cumbersome process of developing a new convention on privacy by starting with an instrument already adopted 'within the region with the most concentrated distribution of privacy laws, Europe'.[148] Thus, it would be a much quicker solution than waiting for some new globally enforceable treaty. Its membership includes forty European states, twenty of whichhave acceded to its Additional Protocol; five accessions are from outside the EU. The CoE Convention 108 is based on the most important minimal right of data protection law, the human right of privacy. This principle is recognized worldwide. The CoE Convention 108 and Additional Protocol could provide a reasonable basis (a common and moderate privacy standard) for guarantee of free flow of personal data between parties to the treaty, both as between Asia-Pacific countries and as between those countries and European countries. Such invitation and accession to both would be likely to carry with it the benefits of a finding of adequacy under the EU Directive, or make one irrelevant.[149]

164 Summing up the problems between the poles of privacy and cloud computing, a truly remarkable recommendation[150] has been issued by the European Network and Information Security Agency (ENISA). The agency determined legal recommendations to the European Commission: 'Most legal issues involved in cloud computing will currently be resolved during contract evaluation (i.e., when making comparisons between different providers) or negotiations. The more common case in cloud computing will be selecting between different contracts on offer in the market (contract evaluation) as opposed to contract negotiations. However, opportunities may exist for prospective customers of cloud services to choose providers whose contracts are negotiable. Unlike traditional Internet services, standard contract clauses may deserve additional review because of the nature of cloud computing. The parties to a contract should pay particular attention to their rights and obligations related to notifications of breaches in security, data transfers, creation of derivative works, change of control, and access to data by law enforcement entities. Because the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide ranging effects, the parties should carefully consider whether standard limitations on liability adequately represent allocations of liability, given the parties' use of the cloud, or responsibilities for infrastructure. Until legal precedent and regulations address security concerns specific to cloud computing, customers and cloud providers alike should look to the terms of their contract to effectively address security risks'[151]

■

1 Christopher Kuner, 'An international legal framework for data protection: Issues and prospects'', Computer law & Security Review, 2009, vol. 25, p. 307-317 [308]; cited as: ''Kuner, An international legal framework for data protection''.

2 ''Google is calling for a discussion about international privacy standards which work to protect everyone's privacy on the internet. These standards must be clear and strong, mindful of commercial realities, and in line with oftentimes divergentpolitical needs. Moreover, global privacy standards need to reflect technological realities, taking into account how quickly these realities can change''; <http://googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html>.

3 Die Welt, 'Die Post-PC-Ära hat begonnen', 6 March 2012, p. 11

4 http://www.bitkom.org/

5 Frankfurter Allgemeine Zeitung (FAZ), 4 March 2012.

6 Christopher Kuner, 'An international legal framework for data protection', p. 308.

7 Speech of Angela Merkel at the CeBIT fair, FAZ, 6 March 2012.

8 Viviane Reding, 'Privacy standards in the digital economy: Enhancing trust and legal certainty in transatlantic relations', 23 March 2011, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/210>.

9 Viviane Reding, 'Privacy matters: Why the EU needs new personal data protection rules', 30 November 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700>.

10 <http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf>.

11 <http://www.privacyconference2008.org/>.

12 <http://www.privacyconference2009.org/>.

13 <http://www.privacyconference2010.org/>.

14 <http://www.privacyconference2011.org/>.

15 <http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_R_001_Intnl_Standards_ENG.pdf>.

16 http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html

17 <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf>.

18 Hazel Grant, 'Data protection 1998-2008', in: Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 44-50 [p. 44].

19 Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950, CETS No. 194.

20 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities of 23 November 1995, No L. 281, p. 31.

21 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13 December 2007, <http://europa.eu/lisbon_treaty/full_text/index_en.htm>.

22 Last amended by its Protocol No. 14 (CETS No. 194) as from the date of its entry into force on 1 June 2010.

23 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

24 <http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm>.

25 Paulde Hert / Eric Schreuders, 'The Relevance of Convention 108. European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future', from DP Conference (2001) Reports, p. 63-76, The Council of Europe (ed.), <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/conferences/DP%282001%29Proceedings_Warsaw_EN.pdf>, p.42.

26 ChristopherKuner, 'An international legal framework for data protection', p. 308.

27 ChristopherKuner, 'An international legal framework for data protection', p. 309.

28 Stated already in the 19th century by Warren/Brandeis, 'The Right to Privacy', Harvard Law Review, vol. IV no. 5, 15.12.1890, <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

29 Now addressed by the European Commission during its consultations for the proposal of a comprehensive reform of the EU's 1995 data protection rules, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

30 as an example on the image from right to left: storage, print, compute.

31 Ina Schiering / Markus Hansen: Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

32 Ina Schiering / Markus Hansen: Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

33 Ina Schiering / Markus Hansen: Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

34 Ina Schiering / Markus Hansen: Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

35 Art. 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>.

36 See below.

37 Art. 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', 16 February 2010, WP 169

38 C. Ian Kye, / Gabriel M.A. Stern, 'Where in the World Is My Data? Jurisdictional Issues with Cloud Computing', 30 March 2011, p. 1, <http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf>.

39 Robert Gellman, 'Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing', 23 February 2009, <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf>.

40 Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 12, 16 January 2001, p. 1–23.

41 C. Ian Kye, / Gabriel M.A. Stern, 'Where in the World Is My Data? Jurisdictional Issues with Cloud Computing', 30 March 2011, p. 5, <http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf>.

42 Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), Official Journal of the European Union, L 177/6 EN.

43 Juliette Garside, 'How global laws protect your data', The Guardian, 17 October 2011, <http://www.guardian.co.uk/cloud-technology/global-laws-protect-your-data>.

44 See below.

45 These methods will be examined below.

46 Switzerland, Canada, Andorra, Faeroe Islands, Argentina, Guernsey, Isle of Man, Israel.

47 Some Latin American countries and Morocco, which has recently adopted new legislation to protect personal data.

48 Art. 29 Data Protection Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC', 24 October 1995, WP 114, p. 6.

49 Art. 29 Data Protection Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context', 13 September 2001, WP 48, p. 3.

50 Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, Official Journal L 181 , 04/07/2001, p. 0019 – 0031.

51 Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, Official Journal L 385 , 29/12/2004, p. 0074 – 0084.

52 Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal-data to processors established in third countries under Directive95/46/EC of the European Parliament and of the Council, Official Journal L39, 12/02/2010, p. 0005 – 0018.

53 Pub.L. 106-102.

54 Pub.L. 108-159.

55 Pub.L. 104-191.

56 Pub.L. 107-56, 115 Stat. 272 (2001).

57 Pub.L. 99-508.

58 As an example, on the basis of its data security regime (201 C.M.R. 17.00), Massachusetts requires entities to develop and implement a written information security plan to create technical and physical safeguards for the protection of personal data of Massachusetts residents.

59 26 U.S.C. §§ 6713, 7216; 26 C.F.R. § 301.7216.

60 After 2005 amendments, 26 C.F.R. §301.7216-3(b)(4).

61 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 115].

62 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global

governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 115].

63 Cécile de Terwangne, 'Is a Global Data Protection Regulatory Model Possible?', in: Reinventing Data Protection?, Gutwirth, Poullet, De Hert, de Terwangne, Nouwt (ed.), Springer Science, 2009, p. 179.

64 Michael P.Roch, 'Filling the Void of Data Protection in the United States: Following the European Example', Santa Clara Computer and High Technology Law Journal, February 1996, p. 71-96 [p. 93].

65 Video Privacy Protection Act, 18 U.S.C. 2710.

66 TRUSTe is an independent, privately held organization best known for its web privacy seal. TRUSTe runs the world's largest privacy seal program, with more than 2,000 websites certified, including the major Internet portals and leading brands such as IBM and eBay; <http://www.truste.com/index.html>.

67 <https://www.bbbonline.org/reliability/Rel_EN.asp>.

68 'CoE Convention 108', Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.01.1981, <http://conventions.coe.int/treaty/en/treaties/html/108.htm>.

69 <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf>.

70 Christian Toon, 'The new EU data protection guidelines', 23 February 2012, <http://www.continuitycentral.com/feature0957.html>.

71 Official Journal of the European Union, L 337/11, 18 December 2009.

72 Pub.L. 107-204, 116 Stat. 745, enacted July 29, 2002.

73 Official Journal of the European Union, L 157/87, 9 June 2006.

74 GuidoSanchidrian, 'EuroSOX is not US-SOX ', 20 March 2009, <http://www.symantec.com/connect/articles/eurosox-not-us-sox>.

75 NeelieKroes, Vice-President of the European Commission responsible for the Digital Agenda, EU Data Protection Reform and Cloud Computing 'Fuelling the European Economy' event, Microsoft Executive Briefing Centre Brussels, 30 January 2012, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/40&format=HTML&aged=0&language=EN&guiLanguage=en>.

76 Ian Walden / Christopher Millard / Kuan Hon,'Data protection law creates cloud of uncertainty for cloud computing', 21 November 2011, <http://www.ccls.qmul.ac.uk/news/2011/59982.html>.

77 Ian Walden / Christopher Millard / Kuan Hon, 'Data protection law creates cloud of uncertainty for cloud computing', 21 November 2011, <http://www.ccls.qmul.ac.uk/news/2011/59982.html>.

78 <http://www.cloudlegal.ccls.qmul.ac.uk/>.

79 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 111].

80 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 112].

81 While the minimum data for completing a booking is quite small, a PNR data typically contains 34 fields of data of a sensitive nature, like the passenger's full name, date of birth, home and work address, telephone number, e-mail address, credit card details, as well as the names and personal information of emergency contacts.

82 Council Decision 2007/551/CFSP/JHA of 23 July 2007, OJ L204/16.

83 Sophia In't Veld, 'New PNR proposals an improvement on past', Press Release, 22 September 2010, <http://www.alde.eu/press/press-and-release-news/press-release/article/new-pnr-proposals-an-improvement-on-past-33971/>.

84 <http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2000:215:SOM:DE:HTML>.

85 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 121].

86 Reidenberg, 'E-Commerce and Transatlantic Privacy', in: Houston Law Review, 2001, iss. 38, p. 717-749 [717], <http://reidenberg.home.sprynet.com/Transatlantic_privacy.pdf>, cited as: 'Reidenberg, E-Commerce and Transatlantic Privacy'.

87 <https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10neu.pdf>.

88 Art. 1 of the Decision regarding the Safe Harbor Principles as an Adequate Level of Protection; [2000] O.J. L 215/7.

89 <http:///www.export.gov/safeharbor> [Last accessed: 30 May 2011].

90 Viviane Reding, 'Privacy standards in the digital economy: Enhancing trust and legal certainty in transatlantic relations', 23/03/2011, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/210>.

91 On December 10, 1948 the General Assembly of the United Nations adopted and proclaimed the 'Universal Declaration of Human Rights' (UDHR), http://www.un.org/en/documents/udhr/index.shtml

92 'ICCP', 16 December 1966, http://www.un.org/millennium/law/iv-4.htm

93 'UN Computerized Guidelines', 14 December 1990, UN Doc E/CN.4/1990/72

94 LeeBygrave, 'Data Protection Law: Approaching Its Rationale, Logic and Limits', The Hague/London/New York, Kluwer Law International, 2002, p. 32

95 http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24464/20091.pdf

96 http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24465/20092.pdf

97 <http://www.bfdi.bund.de/bfdi_forum/showthread.php?t=689>.

98 <http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_R_001_Intnl_Standards_ENG.pdf>.

99 LeeBygrave, 'International agreements to protect personal data', in: Global Privacy Protection: The First Generation, James B. Rule & Graham Greenleaf (ed.), 2007, p. 28.

100 'Guidelines for the Security of Information Systems', in the following 'OECD 1992 Security Guidelines', 26 November 1992; Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, in the following 'OECD 2002 Security Guidelines', 25 July 2002.

101 Guidelines for Cryptography Policy, in the following 'OECD Cryptography Guidelines', 27 March 1997.

102 Guidelines for Consumer Protection in the Context of Electronic Commerce, in the following 'OECD Consumer Protection Guidelines', 9 December 1999.

103 The 'Declaration on Transborder Data Flows', the 'Declaration on the Protection of Privacy', the report 'Privacy Online: OECD Guidance on Policy and Practice', the report 'Making Privacy Notices Simple: An OECD Report and Recommendations' and the 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy'.

104 <http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+privacy+Framework.pdf/$file/APEC+privacy+Framework.pdf>.

105 Graham Greenleaf, 'Five years of the APEC privacy framework: Failure or promise?', in: Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 28-43 [p. 28].

106 Gabriela Kennedy / Sara Doyle / Brenda Lui/ et al., 'Data protection in the Asia-Pacific region', Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 59-68 [p. 60].

107 Graham Greenleaf, 'Five years of the APEC privacy framework: Failure or promise?', in: Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 28-43 [p. 31]; see also a critical examination of these principles in Kennedy / Doyle / Lui / et al., p. 61; de Terwangne, p. 184.

108 Graham Greenleaf, 'Five years of the APEC privacy framework: Failure or promise?', in: Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 28-43 [p. 32].

109 Gabriela Kennedy / Sara Doyle / Brenda Lui / et al., 'Data protection in the Asia-Pacific region', Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 59-68 [p. 61].

110 Abraham L. Newman, 'Protectors of Privacy: Regulating Personal Data in the Global Economy', Cornell University Press, 2008, p. 103.

111 <http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf>.

112 Nigel, 'APEC Cross Border Privacy Rules: Ready to party but will anyone come?', 30 September 2011, <https://www.privacyinternational.org/article/apec-cross-border-privacy-rules-ready-party-will-anyone-come>.

113 <http://www.ipc.on.ca/index.asp?navid¼46&fid1¼575>.

114 <http://www.globalnetworkinitiative.org/index.php>.

115 Souichirou Kozuka, 'The economic implications of uniformity in law', in: Uniform Law Review, 2007, part 4, p. 683-696, <http://www.unidroit.org/English/publications/review/articles/2007-4-kozuka-e.pdf>, p. 693, stating that 'ironically, the more popular a Convention is, the more difficult it is to amend the uniform law in a timely manner'.

116 UNGA Res 174(II) (21 November 1947).

117 Statute of the International Law Commission, Art.1(1).

118 ILC, Report on the Work of its Fifty-Eighth Session, UN Doc A/61/10 para. 257.

119 Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations: Annex 1b, General Agreement on Trade in Services (GATS), Preamble.

120 LeeBygrave, Lee, 'Privacy protection in a global context: A comparative overview', in: Scandinavian studies in law, Peter Wahlgren (ed.), Stockholm Institute for Scandinavian, Law, iss. 47, 2004, p. 348, cited as: 'Bygrave, Privacy Protection in a Global Context'.

121 GrahamGreenleaf, p. 41.

122 This limitation is probably also valid for the relation to the third person affected by the offence.

123 Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/ECof the European Parliament and of the Council, Official Journal L39, 12/02/2010, p. 0005 – 0018.

124 Art. 29 Data Protection Working Party, 'Working document setting up a table with the elements and principles to be found in Binding Corporate Rules',24 June 2008, WP 153.

125 The 'DüsseldorferKreis' is a working group of representatives from Germany's sixteen state data protection authorities that provides a uniform 'German' approach to data protection questions.

126 Art. 29 Data Protection Working Party, 'Working document setting up a framework for the structure of Binding Corporate Rules', 24 June 2008, WP 154.

127 <http://www.cloudsecurityalliance.org/>.

128 <http://www.eurocloud.de/>.

129 <http://www.tclouds-project.eu/>.

130 Lawrence Lessig,'Code and other laws of cyberspace', Basic Books, 1999, p. 6.

131 For example, the International Organization for Standardization (ISO), TMB Task Force on Privacy, June 2008.

132 ChristopherKuner, 'An international legal framework for data protection', p. 314; for example, the ITU's international allocation of radio-frequency spectrum has established a de facto standard that is followed in 191 ITU member states, and the W3C has published over 110 technical standards for the World Wide Web; see <http://www.w3.org/consortium>.

133 Thilo Weichert, 'CloudComputing & Data Privacy', p. 10-11, <https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf>.

134 <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile>.

135 <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport>.

136 <https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm>.

137 <http://www.ipc.on.ca/images/Resources/gps.pdf>.

138 <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf>.

139 <http://www.iccwbo.org/uploadedFiles/TOOLKIT.pdf>.

140 <http://www.iccwbo.org/policy/ebitt/id5289/index.html>.

141 <https://www.datenschutzzentrum.de/>.

142 LeeBygrave, 'Privacy protection in a global context: A comparative overview', p. 48.

143 Christopher Kuner, 'An international legal framework for data protection', p. 308.

144 Many international private organizations are defining specifications of the network´s and terminal functioning without oversight or control by governments, such as the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN) or the World Wide Web Consortium (W3Consortium)

145 James B. Rule, 'Conclusion', in: 'Global privacy Protection: The First Generation', James B. Rule and Graham Greenleaf (ed.), Edward Elgar Publishing, 2009, p. 262-263

146 Christopher Millard, 'Proposed EU Data Protection laws unlikely to promote cloud computing, warns Professor Millard', 1 February 2012, http://www.qmul.ac.uk/media/news/items/hss/63123.html

147 Christopher Kuner, „An international legal framework for data protection', p. 316.

148 Graham Greenleaf, p. 41.

149 Graham Greenleaf, p. 42.

150 http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

151 ENISA Report, 'Benefits, risks and recommendations for information security', p. 6, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport