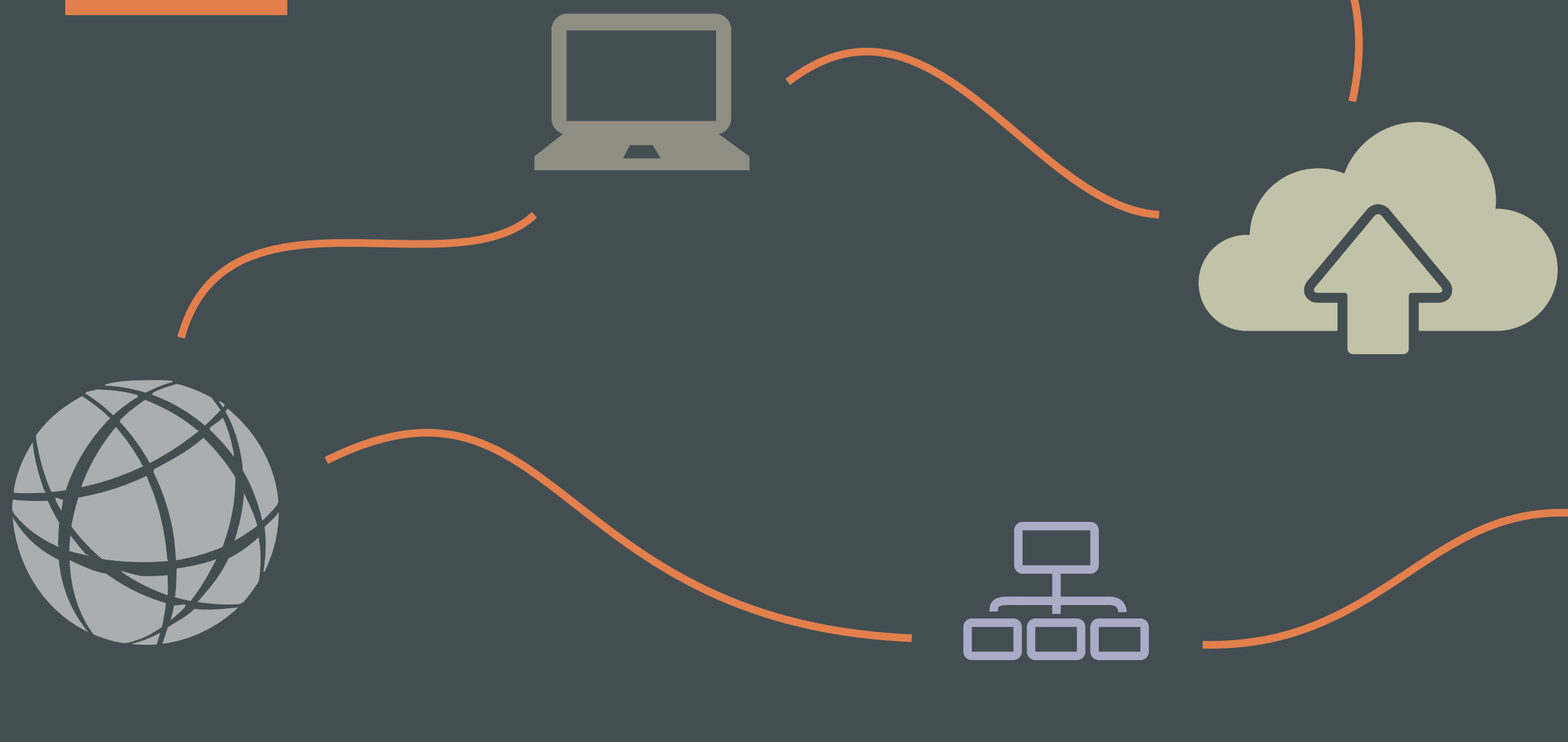
Bird & Bird & Cloud computing & your legal questions answered

Enter >



Contact us

Roger Bickerstaff

Co-Head of International IT Group

Call me on: +44 (0)20 7905 6000

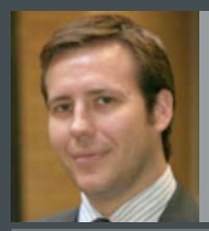
Email | Profile

Fabian Niemann

Partner

Call me on: +49 (0) 211 2005 6000

Email | Profile



Barry Jennings

Senior Associate

Call me on: +44 (0)20 7905 6000

Email | Profile

About this guide

Whether you are a supplier or a user of cloud services, the legal ramifications of cloud computing are complex, fast changing and different in every jurisdiction. Thinking internationally can have a big impact on costs and profit. There are wide-ranging strategic issues and day-to-day operational matters to consider.

This guide covers the main legal issues you need to think about when setting up a cloud service on a pan-European basis. It provides short answers to your questions on what you need to do to ensure you are legally compliant. And makes it easy to understand the implications of operating in and across different jurisdictions.

We are keen to develop the guide further and welcome suggestions for additional areas that we could cover in future updates. Feel free to email us at cloudservices@twobirds.com with any suggestions.

To stay across changes in the law sign up for updates to this guide (cloudservices@twobirds.com)

Thank you

About Bird & Bird

Bird & Bird is an international law firm, with a rare and invaluable grasp of strategic commercial issues. We combine exceptional legal expertise with deep industry knowledge and refreshingly creative thinking, to help you achieve your commercial goals.

We're strategic thinkers who view commercial issues from a legal perspective. We see our role as helping you achieve tangible business results, and maximise opportunities, through the law. Information technology is one of our key strengths and an area that requires the international expertise we can offer.

Our cloud computing clients have included banks, healthcare organisations, public bodies, retailers, globally located manufacturers, publishers and aerospace and defence companies.

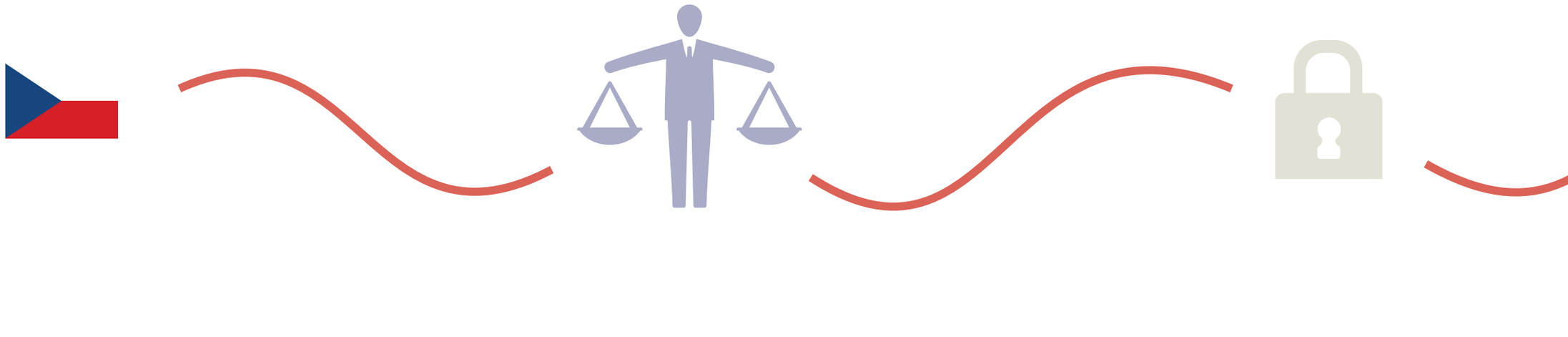
Find out more
+44 (0)20 7415 6000
www.twobirds.com/cloudpdf/Information_Technology.aspx

Czech Republic

In the Czech Republic, cloud computing is emerging as a disruptive force for both IT vendors and users. While most enterprises are still in the process of trying to understand its opportunities and challenges, cloud computing is becoming a strategic priority for early adopters being driven by a need of cost reduction, faster innovation, improved scalability and flexibility.

Moreover, although there is no "Government Cloud" operating in the Czech Republic, the Czech authorities are also very interested and are seriously considering establishing certain cloud strategies.

Since there is no specific law aimed at cloud services, vendors and users must in particular comply with the regulations related to the protection of personal data or sector specific law. Generally, however, legal requirements for cloud computing are subject to debate and development. Some of the answers provided below therefore may be subject to change in the future. ■



General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   Yes, with respect to copyright licenses. Other contracts can be more problematic under current law. ■

Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes, but there are rules that may apply irrespective of contractual provisions (data protection, consumer protection, public order, mandatory provisions of Czech law). The option to choose may vary depending on whether contractual parties are inside or outside the EU.

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   If no international element is involved, Czech law applies. Otherwise, the contract would be governed by the law of the country:

   - mutually agreed by parties;
   - where the service provider has its habitual presence or central administration (Article 4 of the Regulation 2008/593/EC – Rome I).

   Where Rome I is not applicable, governing law can be determined by the general rules of private international law.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   If no international element is involved, Czech law applies. Otherwise, the contract between a consumer and a professional would be governed by the law of the country:

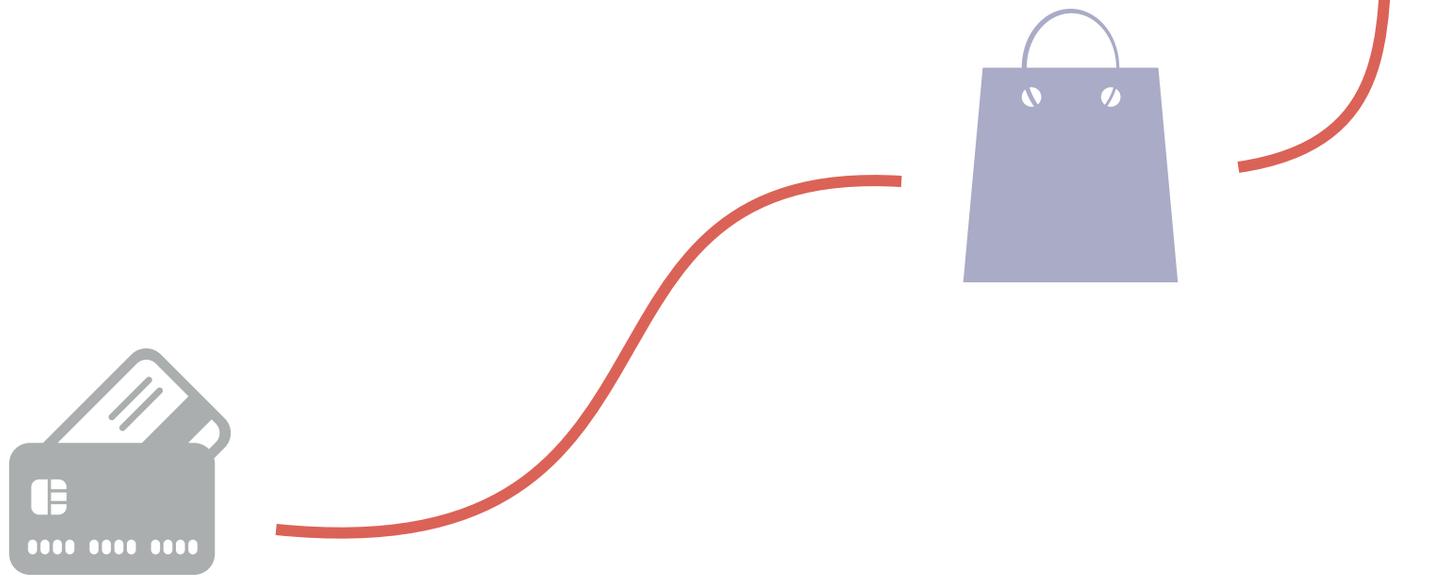
   - mutually agreed by parties;
   - where the consumer has his/her habitual residence.

   Where Rome I is not applicable, governing law can be determined by the general rules of private international law. The choice of the applicable law cannot deprive the consumer of the protection provided by the country of his/her habitual residence.

4. Are there any other relevant issues related to applicable law and cloud computing?
   When EU law is applicable, the choice of law cannot override certain mandatory provisions that are regarded as crucial for safeguarding public interests (Article 9 of the Regulation 2008/593/EC – Rome I). When EU law is not applicable, the law of a foreign state is not applied if its contrary to the main principles of the social and state system of the Czech Republic and its mandatory laws. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?
   There is no consumer protection legislation that specifically applies to cloud computing. In a contract between a consumer and a professional, obligations relating to general consumer protection should be fulfilled (Directive 97/7/EC). ■



Data protection

1. Is the data protection law compatible with the EU Data Protection Directive on cloud computing issues?
   Yes, data protection law is generally compatible with the EU Data Protection Directive on cloud computing issues.

2. Which law is applicable in the case of a dispute concerning data protection and cloud computing?
   The Czech Data Protection Authority (Czech DPA) has competence over the data controllers/processors that control/process data on the territory of the Czech Republic. Therefore, the Czech DPA claims competence when controllers/processors:

   - have their registered office within the territory of the Czech Republic;
   - use technical means located within the territory of the Czech Republic.

   The EU Data Protection Directive has not been fully implemented in the Czech Republic (e.g. cookies) and there is no practical experience, and no guidelines issued by the Czech DPA, making it difficult to predict the official position.

3. Who is the data controller in a cloud computing service?
   The data controller is the person/entity that determines the purpose and manner in which any data is processed. The official position of the Czech DPA confirms that, in most cases, the user of cloud computing services is the data controller (see www.uoou.cz/uoou.aspx?menu=14&loc=331#a71 – in Czech).

4. Who is the data processor in a cloud computing service?
   The data processor is the person/entity who processes data on behalf of the data controller. The official position of the Czech DPA confirms that, in most cases, the provider of cloud services is the data processor (please see www.uoou.cz/uoou.aspx?menu=14&loc=331#a71 – in Czech).

5. If the cloud provider is a data processor, what are its obligations under data protection law?
   Both the controller and the processor must:

   - adopt measures preventing unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transmission, other unauthorised processing and other misuse of personal data; ▶

- develop and document the technical-organisational measures used to ensure personal data protection in accordance with the law and other legal regulations;
- perform a risk assessment for:
  - carrying out instructions for processing by people with immediate access to personal data;
  - prevention of unauthorised access to personal data;
  - means for processing;
  - prevention of unauthorised reading, creating, copying, transferring, modifying or deleting records containing personal data;
  - measures to enable determination and verification of the recipients of transferred personal data.

The processor must also monitor and report any breach of data protection law to the Czech DPA.

6. Is there a requirement to notify end users about the use of cloud services?
Besides the standard notification regarding processing personal data, the subject of personal data must be informed if the cloud service takes place outside the EEA (e.g. personal data is processed on servers outside the EEA) and about the nature of the data.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?
There are no specific requirements applying to cloud services. The standard notification regarding any processing of personal data is mandatory.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?
Personal data can be transferred to third countries:
- if the prohibition restricting free movement of personal data ensues from an international treaty, or if the personal data is transferred on the basis of the decision of an institution of the European Union (i.e. SCCs or Safe Harbour);
- if the controller proves that:
  - the data transfer is carried out with the consent of, or on the basis of, an instruction by the data subject;
  - sufficient specific guarantees for personal data protection has been created in a third country;
  - the transfer is necessary for negotiating the conclusion or change of a contract, carried out on the incentive of the data subject, or for the performance of a contract to which the data subject is a contracting party; ►

- the transfer is necessary to perform a contract between the controller and a third party, concluded in the interest of the data subject, or to exercise other legal claims; or
- the transfer is necessary for the protection of rights or important vital interests of the data subject, in particular for rescuing life or providing health care.

In this case, the controller must apply to the Czech DPA for authorisation before transfer to third countries.

9. Are cloud providers permitted to use sub-processors?
Czech DP law only recognises the direct agreement between a controller and a processor. Based on longstanding interpretation of the Czech DPA, chaining of processors (sub-processors) was not allowed at all, and direct agreement was always required. The approach has not changed much even after the new C2P SCCs were adopted in 2010 allowing sub-processing. The Czech DPA continues to require only direct contracts in C2P relationships.

10. What are the security requirements connected with processing data?
See Q5 – obligations of the data processor. Since the security requirements are defined broadly it is necessary to adopt a specific written policy.

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?
Sensitive data can only be processed if:

- the data subject has given his express consent – the data subject must be provided with information about the purpose of processing, the personal data involved, the controller and the period of time consent is being given for;
- the processing is necessary to keep the obligations and rights of the controller responsible in the fields of labour law and employment;
- the processing pursues political, philosophical, religious or trade-union aims and is carried out within the scope of legitimate activity;
- the processing concerns personal data published by the data subject;
- the processing is necessary to secure and exercise legal claims; ▶

- the sensitive data is processed exclusively for archival purposes.

The regulation of specific sectors (e.g. banking) needs to be considered. Given that the Czech National Bank considers cloud computing a type of outsourcing, it is important to look at its position (see http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/en/legislation/official_information/v_2011_05_20811560_en.pdf – in English).

12. Is there existing or planned legislation relating to data protection and cloud computing that may be relevant?

No, there is no cloud specific data protection legislation existing or planned. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   The Czech Standardization Institute (CSI) is the official institution for standardisation. CSI has not issued any standardisation document on cloud computing yet.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   No.

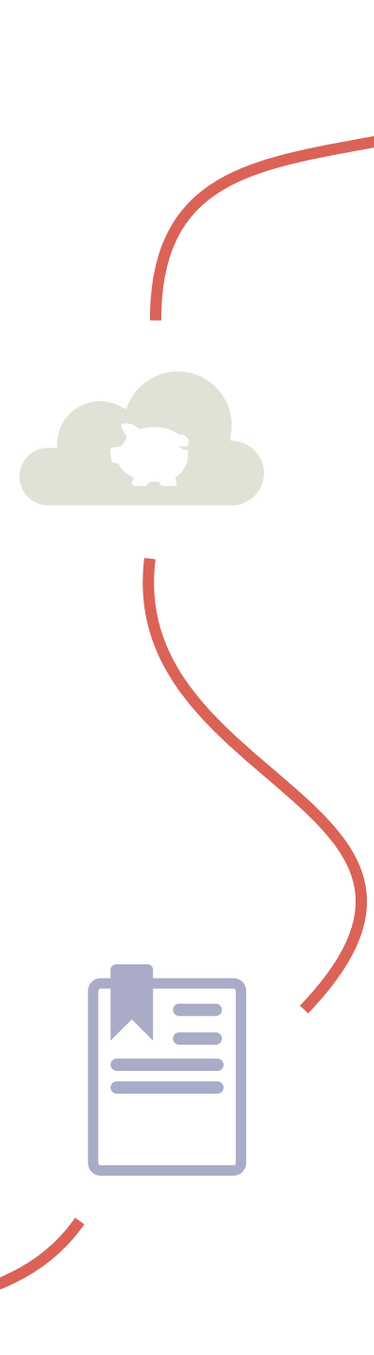
4. Are there applicable international standards relevant for cloud computing that are commonly used?
   We are not aware of any international standards.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   Depending on the type of cloud service, standard SLAs and EULAs tend to be dictated by cloud providers. There are none that are commonly used.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   No. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?
   Yes, the Czech Banking Act contains special duties for financial institutions. These concern outsourcing activities and processes which are essential for the performance of banking transactions, financial services or other services typically performed by these institutions. While using cloud computing services, financial institutions have to comply with MiFID security requirements. ■



Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, but right to sub-license must be expressly contained in the license agreement.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   No.

3. Is it possible to use Open Source Software for cloud computing?
   Yes.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   The general principles and sanctions of intellectual property law can apply, depending on the circumstances of the case.

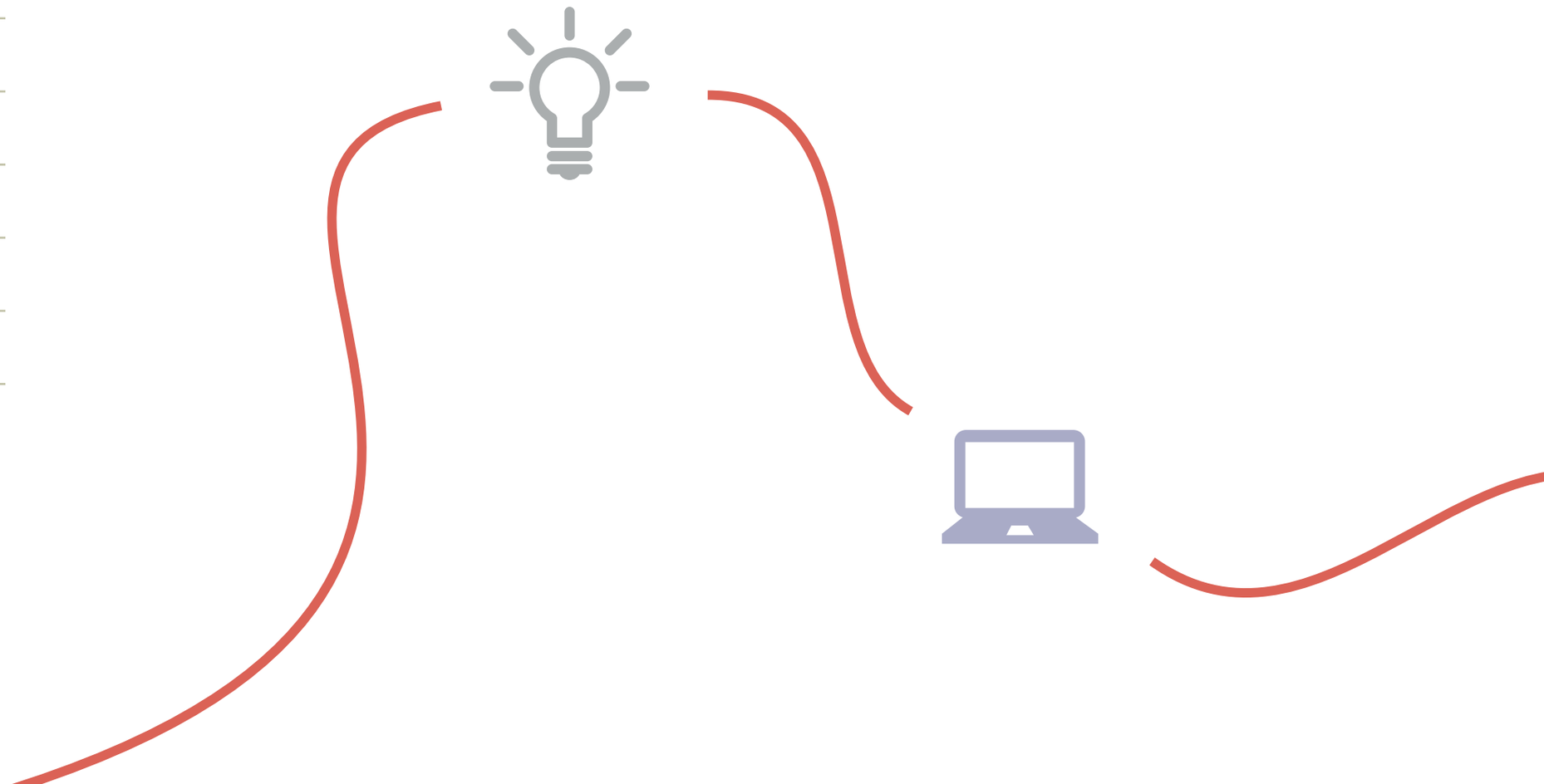
5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   The general principles and sanctions of intellectual property law can apply, depending on the circumstances of the case.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes, what are the possible sanctions for the ISP?
   The ISP would only be liable for intellectual property rights infringement if it assists a third party in distributing such material, or fails to delete the infringing content without delay once it finds out about it. Possible sanctions primarily comprise of cease-and-desist orders, injunctions and damages.

7. Is there any notice-and-takedown procedure that can oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?
   Yes, but not standardised – see Q6 of this section. ISPs are generally obliged to respond only to queries by certain state authorities.

8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?
   If not agreed otherwise, the licensor (author) can withdraw from an exclusive license agreement when the licensee does not utilise it at all or utilises it inadequately, and where utilisation has a considerable unfavourable ▶

effect on the legitimate interests of the licensor. The licensor may withdraw from the license agreement if his work, which has not yet been made public, no longer corresponds with his conviction where making the work public would have a significantly unfavourable effect on his legitimate personal interests. ■



International issues

1. Are there specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   No. ■

Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   It depends on contractual arrangements. The general principles of civil law would apply (i.e. breach of obligation, damage/loss of profit and causal link between the breach of obligation and damage/loss of profit. Also, regulatory liability can apply.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   In B2B situations, liability can be excluded except in cases of the intentional breach of obligations of the cloud services provider. In B2C situations, the limitation of liability is not possible. Czech civil law will significantly change from 1 January 2014 and in B2C situations, the limitation of liability will be generally possible (except in cases of intentional breach or abuse of significantly dominant position between contractual parties).

3. Are there any binding norms in context of warranties that may be relevant for cloud computing?
   No.

4. What will happen in the case of insolvency/bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   In case of insolvency/bankruptcy of the cloud computing provider, all day-to-day operation would be administered by the insolvency administrator. There is a high risk that cloud data would be inaccessible or the obligation arising from the contract would not be duly fulfilled. The contractual arrangement usually enables the customer to withdraw from the contract in such case. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   Ownership of data is theoretically problematic under Czech law. Usually, the customer would hold all intellectual property rights and grant the provider of the cloud services license (or sub-license) for the limited rights that are necessary to provide the service in the cloud contract.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud? Who is the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   Ownership of data is theoretically problematic under Czech law and contractual arrangements may vary. Generally, the use of data is agreed on the basis of the license under which the data was placed in the cloud. ■

Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes, Czech authorities are highly interested in cloud computing. Establishment of cloud strategies is included in the eGovernment Strategy of the Czech Ministry of Interior.

2. Is there any kind of government cloud operating? Do you know if any public institution is operating using cloud computing services?
   There is no government cloud operating in the Czech Republic. Czech authorities are interested in cloud computing and seriously considering establishment of cloud strategies.

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   No.

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   In order to raise awareness, certain companies are communicating their cloud computing services (opportunities and risks) to state authorities and the public (e.g. WMware, Microsoft).

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
   No.

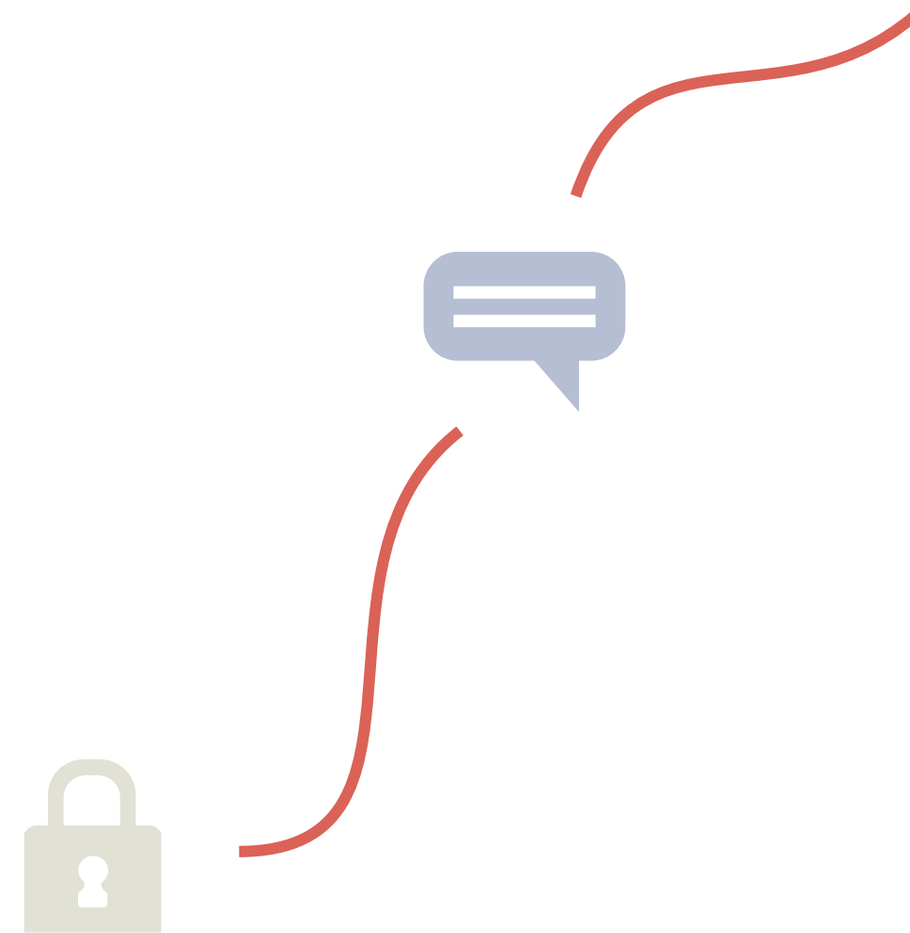
6. Who is or would be the responsible regulator for cloud services?
   On the data protection level, the responsible regulator would be Czech Data Protection Office. If cloud computing is provided in relation to financial services (for banks), the responsible regulator may also be the Czech National Bank.

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
   Unknown. ■

Security issues

1. Are cloud services providers free from content filtration or censorship obligations?
   The provider of the cloud services may be subject to an obligation to content deletion for content marked as infringing the rights holder.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   There is no specific law aimed at cloud services. Cloud service providers must comply with the regulations related to the protection of personal data (see Data Protection Q5.) or other sector specific regulation (e.g. financial services). ■



Denmark

In Denmark cloud computing has been largely embraced by the business sector; driven by a need to cut costs. SaaS is now often used for new applications and we are beginning to see organisations build their IT strategies around the cloud. Businesses are keen on the flexibility and scalability that the cloud provides, but remain concerned about the lack of control with their data and difficulties in shifting to a new supplier (lock-in).

The public sector shows great interest in the cloud, but there has been reluctance due particularly to personal data protection concerns. This reluctance has not least been fuelled by the restrictive approach taken by the DPA towards cloud computing in the widely reported case about the use of Google Apps by Odense municipality (http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/).

Recently, however, the Danish rules on data protection and the DPA's stance have eased in certain areas and it is expected that this will accelerate public authorities' use of the cloud. First of all it is no longer required to make a filing to the DPA for the transfer of non-sensitive data to a third country if the controller uses the EU standard contractual clauses for data transfers. Secondly, the DPA has issued statements about Microsoft's Office 365 (http://www.datatilsynet.dk/english/processing-of-personal-data-in-the-office-365-cloud-solution/) and the IT-university's use of this solution, (http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/it-universitetet-i-koebenhavns-brug-af-microsofts-cloud-loesning-office-365/) where the DPA seems to take a less strict stance towards cloud computing than in the infamous Odense case.

Finally, the Danish government has appointed a task force to investigate if there are areas of Danish legislation, in particular with respect to processing of personal data, which may be amended to further facilitate the use of cloud solutions while we are waiting for the new EU data protection regulation. ■

General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   In general yes, but unusually strict terms are unlikely to be upheld by the courts, especially in relation to consumers. ■

Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   In B2B, any law/jurisdiction may be chosen, provided the terms relating to the law/jurisdiction are part of the agreement. In B2C, consumers will not be bound by terms that are less favourable to them than Danish law. A term will only apply to the parties' contractual relations, not the applicability of Danish public law, such as the Data Protection Act, the Competition Act and the Marketing Practices Act.

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   For contractual obligations, the Rome Convention applies (Rome I does not apply to Denmark). This stipulates that, where no law has been expressly chosen in the contract, the law of the country in which the party who will perform obligations characteristic of the contract has its central administration or habitual residence will apply. This will typically be the country where the cloud service provider has its main office or the country in which the servers used to deliver the cloud services are situated (which may be difficult, if not impossible, to determine).
   Jurisdiction is according to the Brussels Convention and is likely to be the domicile of the party being sued or the country where the service is being provided.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   Choice of law is governed by the Rome Convention. The law likely to apply is that of the country where the consumer is domiciled if the provider is marketing or actively providing service to this country. According to the Rome Convention it is not possible to contract out of certain protection provisions of the law of the country in which the consumer is domiciled.

   The relevant jurisdiction, if the consumer sues, is generally the country of the provider. The country of the consumer will be the relevant jurisdiction if the provider is marketing or actively providing the service there. The service provider must sue in the country of the customer. ►

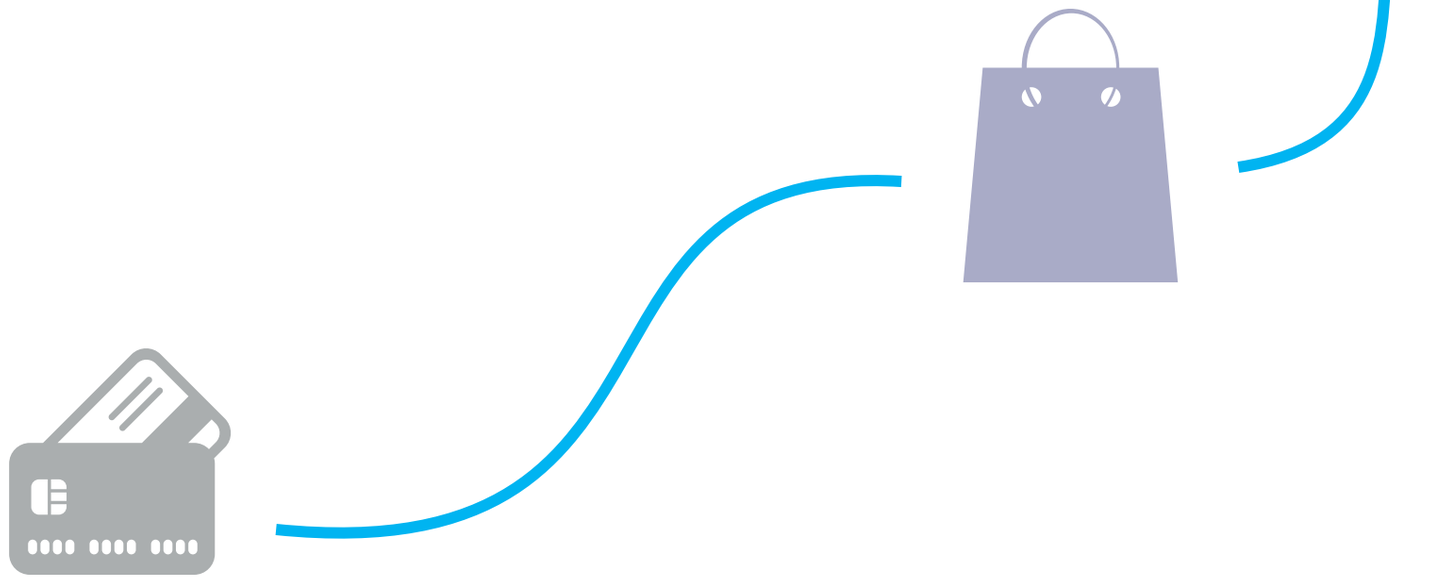
4. Are there any other relevant issues related to applicable law and cloud computing?

Denmark has not adopted the Rome I regulation. The Rome convention therefore applies. See above in Q2 and Q3.

The Rome I regulation may, however, still apply to Danish parties of legal proceedings taking place at a venue, where Rome I applies. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?
   Danish consumer protection laws will apply to cloud services to the same extent as to other online services. Apart from data protection issues, no consumer law issues seem to arise relating to cloud computing. ■



Data protection

1. **Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?**
   The Danish Personal Data Act (Persondataloven) implements the EU Data Protection Directive. In relation to security measures, Denmark has adopted additional requirements by way of an executive order (Sikkerhedsbekendtgørelsen) which presents particular challenges to international cloud computing providers.

2. **Which law is applicable in the case of a dispute concerning data protection and cloud computing?**
   The Danish Personal Data Act (Persondataloven) is applicable to all data controllers established in Denmark if their activities are conducted within the EU.
   It also applies to data controllers domiciled outside the EU/EEA if:

   - If the controller is established in another EU member state, then the data protection laws of that country will apply; also with respect to the processing of information about Danish data subjects;
   - data is gathered in Denmark for the purpose of processing abroad.

3. **Who is the data controller in a cloud computing service?**
   The data controller is the person or entity, alone or together with others, that decides the purposes and means of the processing. Usually this would be the customer (i.e. the company/authority using the cloud service).

4. **Who is the data processor in a cloud computing service?**
   The data processor is the person or entity processing data on behalf of the data controller. The cloud service provider is in most situations considered the data processor, but may also act as controller for some parts of the data processing depending on the circumstances.

5. **If the cloud provider is a data processor, what are its obligations under data protection law?**
   In general, the data controller is liable for all data processing. The data processer, however, is independently co-responsible for ensuring that processing satisfies the security requirements. ▶

6. Is there a requirement to notify end users about the use of cloud services?

In general, it is not necessary to inform users that a cloud service is being used. However, if data is transferred outside the EEA, this information must be communicated in order to obtain consent to transfer data to third countries not ensuring an adequate level of protection. Alternatively transfer of personal data could be based on Safe Harbor or the EU model contract clauses for data transfer to third countries. If the model clauses are used without any changes an authorisation from the DPA for such a transfer is no longer required (as of 1 January 2013).

7. Is there a requirement to notify local data protection authorities about the use of cloud services?

If the cloud service involves the transfer of personal data to third countries, the DPA has to authorise the transfer unless (i) consent has been obtained from the data subjects, (ii) the transfer is of non-sensitive data to a company in the US covered by the Safe Harbor arrangement or (iii) the transfer is based on the EU model clauses (without any changes). Processing of sensitive or semi-sensitive data, however, requires authorisation from the DPA.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?

Yes, data can be sent outside the EU/EEA:

- To third countries, which are considered by the commission to ensure an adequate level of protection. Transfer of sensitive or semi-sensitive data requires authorisation.
- To Safe Harbor companies in the US. Transfer of sensitive or semi-sensitive data requires authorisation.
- Where data subjects consented to the transfer. No authorisation is required.
- Other specific situations, including: performance of a contract between a data controller and data subject; conclusion or performance of a contract between a data controller and third party in the interest of the data subject; the protection of vital interests of the data subject. Transfer of sensitive or semi-sensitive data may require authorisation.
- Transfer based on EU standard contractual clauses. No authorisaton is required if the standard contractual clauses are unchanged.
- In other situations authorisation is required for the transfer of both sensitive and non-sensitive data. ▶

Additionally authorisation for processing may also be required, particularly with sensitive and semi-sensitive data.

9. Are cloud providers permitted to use sub-processors?
Yes, provided the sub-processors are bound by a processor agreement with the data controller (which can be entered into by the first data processor with mandate from the data processor). The data controller must be able to control security etc. at all processors.

10. What are the security requirements connected with processing data?
Appropriate technical and organisational security measures must be adopted. More in-depth requirements are stated in Sikkerhedsbekendtgørelsen (executive order on security), which only apply to public authorities, but are used as a guide in relation to private companies as well. In recent cases regarding cloud computing and public authorities, the Danish DPA has set high standards on security.

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?
For processing sensitive or semi-sensitive data (i.e. data that is not sensitive but is strictly private, such as information on crime or social problems) authorisation from the DPA is required. For transferring such data, authorisation is needed, even when transferring to a safe third country or to Safe Harbour companies, unless transfer is based on unchanged EU standard contractual clauses. In general the security requirements are higher if sensitive or semi-sensitive data is processed. In relation to financial information, it is a requirement that a company's accounting material is stored in Denmark, though storing in Sweden, Norway, Finland and Iceland is accepted. Exemption can be obtained but case law on this is quite strict.

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?
Not formally planned, though discussions are taking place on and off, particularly in relation to making it possible/easier for public authorities to use cloud computing. Further, a task force established by the Danish government has recently published a report with suggestions for changes of certain parts of Danish legislation which seem to present unnecessary restrictions on cloud computing. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   Dansk Standard (DS) is responsible for national standards. In relation to cloud computing, Digitaliseringsstyrelsen (the public authority responsible for implementing public digital ambitions) is also relevant.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   No.

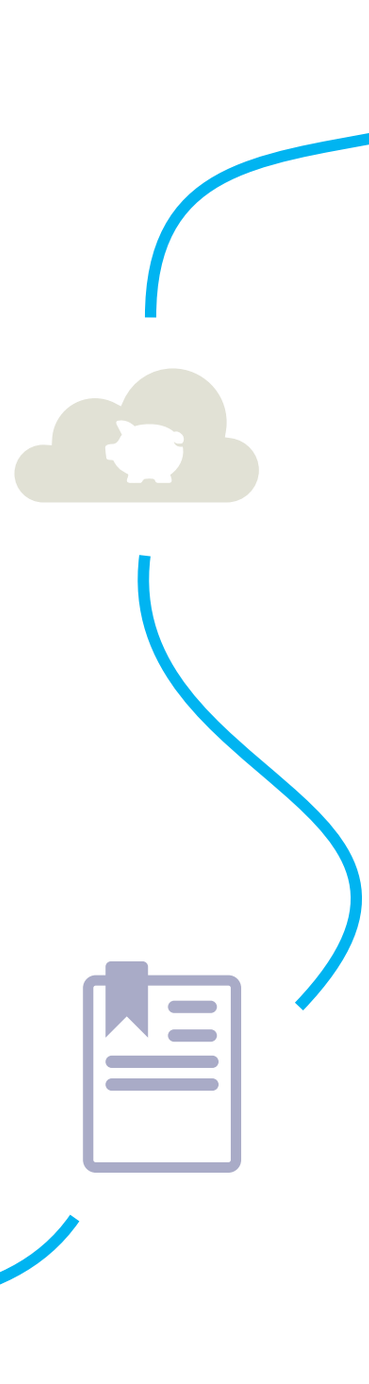
4. Are there applicable international standards relevant for cloud computing that are commonly used?
   The security standards are commonly used (e.g. ISO 27000 series and ISAE 3000 series).

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   No.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   No. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?
   Yes. Outsourcing of data processing may be covered by “Outsourcingbekendtgørelsen” (executive order on outsourcing), which applies when companies in the financial sector are outsourcing substantial activities, including to a cloud service provider. ■



Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, but it depends on the license terms.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   No.

3. Is it possible to use Open Source Software for cloud computing?
   Yes.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   No special sanction in relation to cloud. The standard legal regulation on IPR applies.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   No special sanction in relation to cloud. The standard legal regulation on IPR applies.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   There is no obligation to look for infringements, but if the ISP becomes aware (e.g. by being informed by the owner of the IPR) of infringing material, it must be removed, otherwise the ISP becomes jointly liable for the infringement. Standard civil and criminal sanctions apply.

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?
   Not as such. However, see Q6 of this section.

8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?
   We are not aware of such issues. ■

International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   We are not aware of any specific provisions. ■

Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   If not stated in the agreement, the provider of the service would, generally speaking, be liable. In the Personal Data Act, both controller and processor are under an obligation to ensure that data is not lost. Data loss could lead to payment of damages, both to controller and data subject.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   There are no specific prohibitions. Limitations on liability do not apply if the damage is caused by gross negligence or wilful acts.

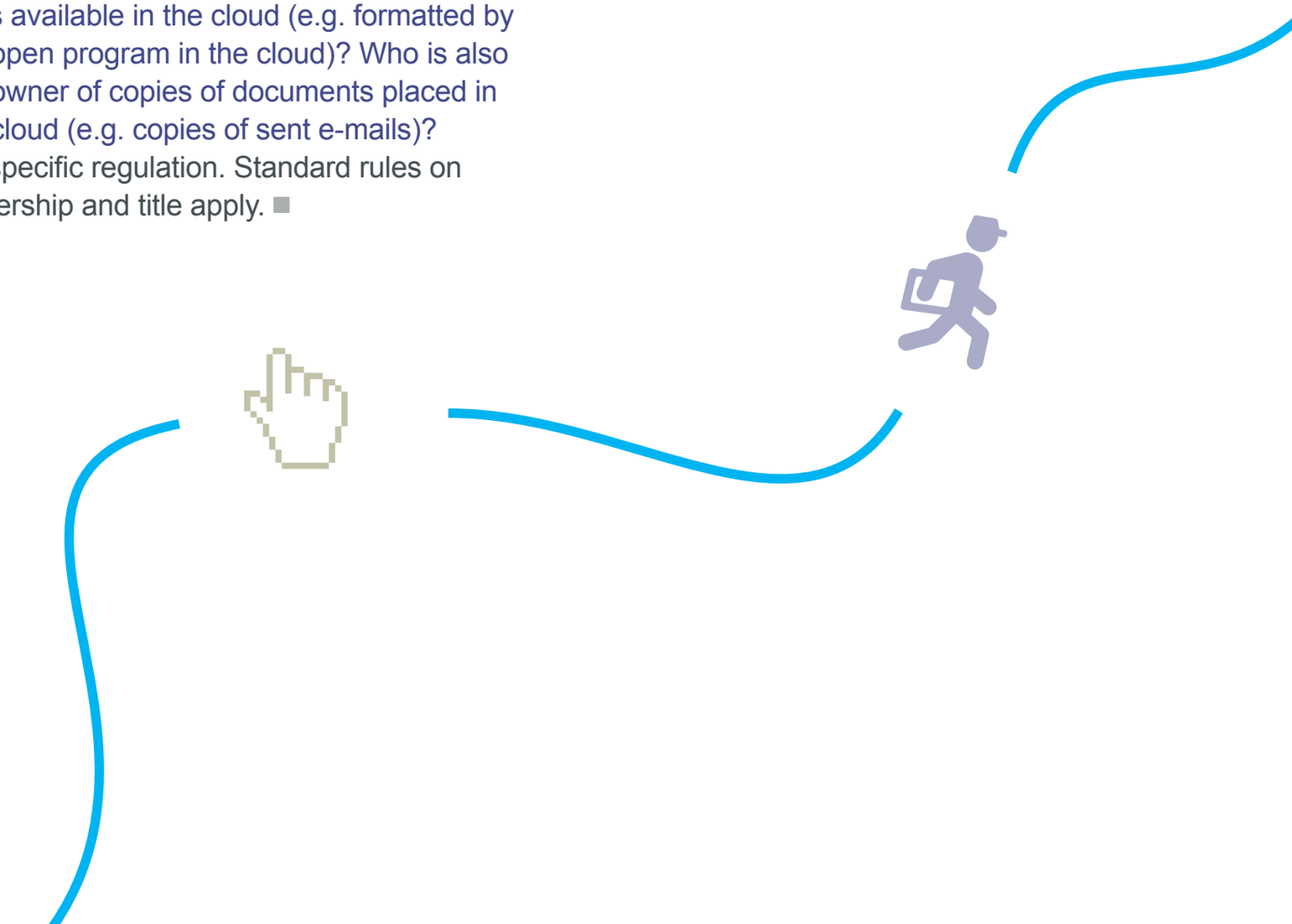
3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   No.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   If the provider goes bankrupt, the user is generally entitled to its data. The official receiver may become data controller in relation to personal data. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   No specific regulation. Standard rules on ownership and title apply.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud)? Who is also the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   No specific regulation. Standard rules on ownership and title apply. ■



Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes. Danish public institutions are looking into using cloud computing. Due to privacy requirements, public authorities have not yet fully embraced it. Many are awaiting the outcome of the case regarding the municipality of Odense's use of Google apps. The Danish DPA refused to grant an approval for the Municipality's planned use of Google Apps. The Municipality is likely to make another attempt to obtain an approval based on new information from Google on their privacy and security practices. Recently, however, the DPA seem to have taken a more pragmatic approach towards cloud computing in the public sector in some decisions about Microsoft's cloud solution, Office 365.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
   No. Public authorities have started using cloud services. They are generally hesitant due to the Google Apps and Odense Municipality case where the DPA rejected clouding of sensitive public information due to security issues.

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   Yes. A general guide regarding cloud and a guide in relation to security have been issued by the former IT and telecom authority. Not just for public bodies.

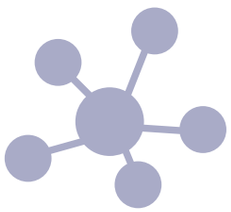
4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   The government has set up an IT security committee (IT-sikkerhedskomitteen), whose role among other things is to strengthen security in relation to cloud.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
   The 02.19 framework agreement issued by the Danish purchasing organisation SKI A/S may be used for obtaining cloud services via a mini tender or direct contracting. BvHD (which as of 1 May 2013 will be Bird & Bird Denmark) has been involved in drafting the service contracts under the 02.19 framework agreement.

6. Who is or would be the responsible regulator for cloud services?
   Regarding personal data, the Danish DPA (Datatilsynet) is responsible for supervision. ►

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?

Government bodies have to follow the security standard DS484 or ISO 27001 (these are more or less the same). Special regulation may apply (e.g. for the military). The 'war-rule' in the Personal Data Act prescribes that, in case of war or war-like conditions, it must be possible to remove or delete any personal data processed on behalf of public institutions that could be of interest to foreign powers. ■



Security issues

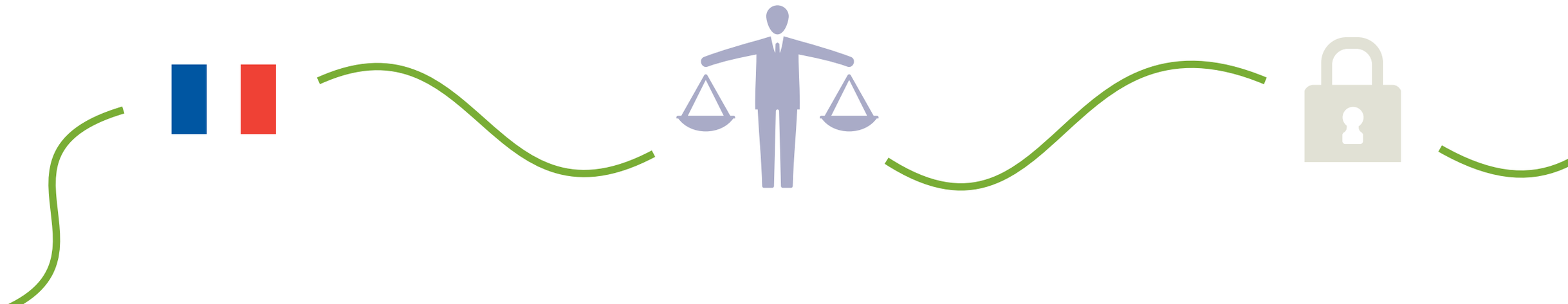
1. Are cloud services providers free from content filtration or censorship obligations?
   In general yes. Service providers can be required by the courts to restrict access to specific material. There have been cases in Denmark, but none focused on cloud services.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   Only in relation to personal data and outsourcing of financial services. ■

France

Awareness, interest and generally, faith, in the use of cloud computing in the business environment has been slow to take effect in France but is rapidly catching up and adoption of the cloud is on the increase; largely driven by cost savings. Both the public and private sectors are incorporating cloud computing into their ICT strategies given the flexibility and scalability of cloud computing.

There still remains an element of "distrust" in the use of cloud computing, particularly in the data protection field, with the CNIL's recent guidance being rather cautious as to the transfer of data in the context of cloud computing. The data security issue, the idea of losing physical control over data and IT systems generally, remains a major inhibitor to a number of ICT directors. However, attitudes are changing as more and more businesses report good experiences. ■



General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   Yes, French law requires online agreements to be entered into through a double-click process. It is possible to implement some processes more simply, especially if the consent expressed in one click is sufficiently informed (e.g. Amazon has a one click to purchase process). ■

Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes, bearing in mind certain public policy rules (consumer law, data protection law, etc.)

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   For contractual obligations, Rome I stipulates that a contract shall be governed by the law chosen by the parties. When none has been chosen, the contract is governed by the law of the country to which it is most closely connected. Typically, this is the country in which the party who will perform obligations characteristic of the contract has its central administration or habitual residence.

   For non-contractual obligations and where there is no law expressly chosen by the parties to the contract, Rome II will apply – as a general rule, and in order of priority, the applicable law is the law of the country:
   - where the damage occurs;
   - where both parties were habitually resident when the damage occurred;
   - with which the case is most closely connected.

   It authorises the parties to choose, by mutual agreement, the law that will be applicable to their obligation.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   According to Rome 1, the applicable law is the law of the country in which the consumer has habitual residence. Under the French Consumer Code, the consumer may bring a case before the court in the jurisdiction where he/she had residence when the contract was entered into, or when the damage occurred.

4. Are there any other relevant issues related to applicable law and cloud computing?
   No – the nature of cloud computing may make the application of jurisdictional rules difficult. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?

Consumer protection laws are public policy rules. The Consumer Code provides that all business suppliers of goods or services must, prior to conclusion of the contract, ensure that the consumer is made aware of the essential characteristics of the goods or services. Additionally, information must be given in French. The civil sanction regarding this issue can be termination of the contract.

The French Consumer code provides that, in contracts between a business and a non-business or consumers, clauses are unfair if they aim to create or result in the creation, to the detriment of the non-professional or consumer, of a significant imbalance between the rights and obligations of the parties. Unfair provisions shall be deemed null or void. The commission in charge of unfair provisions may order a change of or deletion of unfair provisions.

The Consumer Code imposes legal guarantees of conformity and against defects of the item sold. The seller is required to deliver a product that conforms to the contract, and is held liable for any lack of conformity.

Under the French Civil code, a seller is bound to a warranty in respect of any latent defects that render the item sold unfit for the intended use, or which impair use so that the buyer would not have acquired it, or would have given a lesser price for it, had he known of the defects. ■

Data protection

1. Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?
The data protection directive has been transposed into French law. French data protection law is not tailored to deal with cloud computing issues.

2. Which law is applicable in the case of a dispute concerning data protection and cloud computing?
The Data Protection Act (Loi Informatique et Libertés) applies to the processing of personal data if the data controller is established on French territory (establishment includes limited companies, branches, subsidiaries, or any real economic presence) or uses means of processing located on French territory (such as servers or a processor) except means used only for the purposes of transit through the territory).

3. Who is the data controller in a cloud computing service?
This question is not resolved. The French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), recently issued guidelines on cloud computing services. These suggested that, even though the customer is primarily liable for the data it provides, the cloud service provider and the customer could be joint controllers of the processing, especially when the cloud service is a standardised offer. Non-negotiable adhesion contracts are made so that the customer cannot give instructions to the cloud service provider, or control the effectiveness of the guarantees of security and confidentiality made by the provider.

4. Who is the data processor in a cloud computing service?
The data processor should be the cloud service provider, unless the latter is considered to be joint controller of the processing.

5. If the cloud provider is a data processor, what are its obligations under data protection law?
Under the French Data Protection Act the data processor can only process the data according to the instructions of the data controller and is bound by strict obligations of security and confidentiality. These must be stated in the agreement between the data processor and the data controller. ►

6. Is there a requirement to notify end users about the use of cloud services?

Under the French Data Protection Act the data controller or his representative must provide the data subject with information on:

- the processing;
- the recipients or categories of recipients;
- the intended transfer of personal data to any non-EU state;
- the recipient countries and the level of protection they offer;

In case of non adequacy they need to provide:

- the guarantees put in place (EU Standard Contractual Clauses or binding corporate rules or use of the exceptions);
- the purpose of transfer;
- the categories of data.

Therefore, end-users of a cloud computing service should be informed of the identity of the processor and of every country and entity to which their personal data are transferred. This raises issues, since the client is not always able to provide the end-user with the list of countries where the cloud could store the data.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?

There are no requirements to notify the French Data Protection Authority about the use of cloud services. However, when services involve transfers outside of EU/EEA, the common requirements of obtaining the authorisation of the French Data Protection Authority for transfer and signing data transfer agreements apply.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?

Under the Data Protection Act, personal data cannot be transferred to a state that is not a Member of the European Union unless this state ensures an adequate level of protection of individuals' privacy, liberties and fundamental rights with regard to the actual or potential processing of their personal data.

Except for transfers to Iceland, Liechtenstein, Norway, Argentina, Canada, Israel and Switzerland (etc.), the data controller must comply with one of the cases provided by the exceptions of the Data Protection Act, or provide for contractual guarantees to ensure an adequate level of protection during the transfer. For example signing a data transfer agreement along with the prior authorisation of the French Data Protection Authority (CNIL). ►

9. Are cloud providers permitted to use sub-processors?

Nothing in the French Data Protection Act prohibits the use of sub-processors.

The CNIL guidelines concerning cloud computing recommend that in the event of the provider using sub-processors, the client should be informed and give its consent. The contract between the CSP and the sub-processor should mirror the obligations of the contract between the CSP and the client, and should organise the liability between the CSP and the sub-processors.

10. What are the security requirements connected with processing data?

The CNIL has published guidance. For contracts binding organisations with sub-contractors, it recommends a specific clause covering the confidentiality of the personal data they are entrusted with. It also recommends making provisions that ensure the effectiveness of the guarantees offered by the sub-contractor regarding data protection. That includes measures such as security audits and installations visits. Conditions of restitution of data and its destruction must be specified in the event of contract termination.

The CNIL advises against resorting to services offering cloud computing functions in the absence of any guarantee regarding the effective geographical location of the data.

Specific measures must be implemented regarding sensitive data processing. For example, health data hosting services must receive an approval issued by the Secretary of Health.

See the CNIL's website for more information: http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf and http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf.

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?

Consent of the data subject is systematically required as a principle, for the processing as well as for transfer outside the EU/EEA.

Healthcare data can only be stored by a certified host, and disclosure of specific healthcare data (e.g. a personal medical file) is subject to a very strict procedure. ▶

Financial information is not as strictly regulated as sensitive data (see Financial Sector section).

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?

No. However, following its public consultation, the European Commission intends to issue a strategic document promoting cloud computing services to companies and public administration. (http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/575&format=HTML&aged=0&language=FR&guiLanguage=en). The results of this consultation have not been published yet. Additionally, the CNIL has issued guidelines on cloud computing as mentioned above in Q11. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   No.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   No.

4. Are there applicable international standards relevant for cloud computing that are commonly used?
   No. The results of the EC public consultation and the strategic document promoting cloud computing services to companies and public administration are still to be published.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   No.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   No. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?

There are several obligations that must be respected in the financial sector:

According to the Data Protection Act, the data controller shall take precautions regarding the nature of the data and risks of the processing to preserve its security and prevent alteration and damage, or access by non-authorised third parties. In outsourcing, the processor shall offer adequate guarantees to ensure the implementation of security and confidentiality measures. Financial service firms should take into account the obligation of security in the contract signed with the cloud computing provider. However, they remain responsible for any loss, damage or disclosure of data in case of any breach of contract by the cloud computing provider. They should require the service provider to comply with high technical standards (such as ISO/CEI 27001 and ISO 27005 or PCI DSS).

Personal data transfer outside the EU or to a third country that does not ensure an adequate level of protection, is subject to a prior authorisation of the French data protection authority (CNIL). In order to file a request for authorisation, the data controller must name all countries concerned and list all processors and data centres. The service provider should provide a list of all data centres and contractors that will be used for the processing. If data centres/contractors having access to personal data are located outside the EEA, a data transfer agreement is required with each processor (including the processor's own contractors) as is prior authorisation from the CNIL.

Banks and financial institutions must, when outsourcing essential services, keep relevant expertise in order to ensure effective control of outsourced tasks or services and deal with associated risks. Firms should ensure (by technical, organisational and contractual means) that the implementation of cloud computing services respects regulation 97-02. In practice, this is likely to limit the number and location of data centres.

The French Monetary and Financial Code stipulates that employees, banks and financial service organisations are bound by professional secrecy. All measures (technical and contractual) must be taken to ensure respect of professional secrecy. ►

The sharing or transfer of data is strictly limited subject to a necessity test to cases listed by the Code or by authorisations obtained from clients under express and informed consent. Financial institutions must ensure they have obtained all authorisations required. Professional secrecy must be respected regardless of the data storage location. Access must be granted to the French banking regulating authorities regardless of the data storage location.

See the report of the Forum des compétences on obligations regarding information systems security: http://www.forum-des-competences.org/files/resourcesmodule/@random4f1327fd4c75b/1326655684_Obligation_en_S_curit__des_Syst_mes_d_Information.pdf ■

Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, depending on the terms of the licence.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   No.

3. Is it possible to use Open Source Software for cloud computing?
   Yes. For instance, the French government has shown interest in a cloud service projects that would use Open Source Software (the Nuage project and the Andromède project).

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   There are no sanctions specifically designed for cloud computing issues, but the French Intellectual Property Code provides civil sanctions regarding counterfeit in general.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   There are no sanctions specifically designed for cloud computing issues, but the French Intellectual Property Code provides that counterfeit is a criminal offence.

   The French Authority in charge of regulating the protection of copyrights on the internet, the HADOPI, can impose administrative sanctions.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   Yes. The Law regarding Confidence in the Digital Economy (LCEN) provides that Internet Service Providers are not liable unless they do not promptly delete the infringing material when aware of its illicit nature.

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?
   Yes. The LCEN provides for the notice-and-takedown procedure.

   The Internet Service Provider must be notified of the illicit nature of the material. The notification must respect strict requirements and include specific elements such as date ▸

of the facts and description of the illicit material. Once the ISP is aware of the illicit nature of the material, it must remove or delete it promptly. If it does not do so, it can be held liable for the infringing material. There is no obligation to inform authorities about the infringing act.

8. Are there any other special intellectual property law issues that may be relevant to cloud computing (e.g. unusual termination of the license provisions etc.)?

Although cloud computing contracts relate to provision of services rather than supply of software, appropriate software licences may need to be granted to the customer to enable them to legally and correctly use the necessary software without the risk of copyright infringement.

The customer will be required to grant to the service provider a licence to their content allowing the service providers to use any content stored on its servers. Licences cannot be perpetual and often last for the duration of the intellectual property rights themselves.

Aiming at protecting suppliers' intellectual property rights in their own software and the extent to which customers may take advantage of know how gained in a short term contractual relationship, the contract may be terminated at short notice by a customer. ■

International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   Personal data cannot be transferred outside of the EU/EEA without legal grounds (e.g. prior authorisation of the Data Protection Authority or in some cases consent of the data subject). The prior and complete information of the data subject on transfer and disclosure is mandatory. Those obligations clash with the procedures of the Patriot Act that require the recipient of the order not to disclose it and do not expect the recipient of the order to request any kind of authorisation from the local authorities.

From a litigation standpoint, according to French blocking statute, it is strictly forbidden to disclose economic, commercial, industrial, financial or technical information, in order to submit it as evidence in foreign judicial or administrative proceedings.

Those provisions have only been enforced once by the Cour de Cassation in 2007, where it clearly ruled that the disclosure of any document or information of an economic, commercial, industrial, financial or technical nature is forbidden, where it is intended to establish evidence in view of legal proceedings abroad, unless the procedures set out by the Hague Convention are complied with. ■

Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   This is set out in the relevant contractual instrument between the parties. It is influenced by the extent to which personal data is involved in the data loss and whether it is a B2B or B2C arrangement.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   No. General legal provisions and case law relating to unfair provisions (B2C) and prohibition of excessive limitation on essential obligations (B2B) apply.

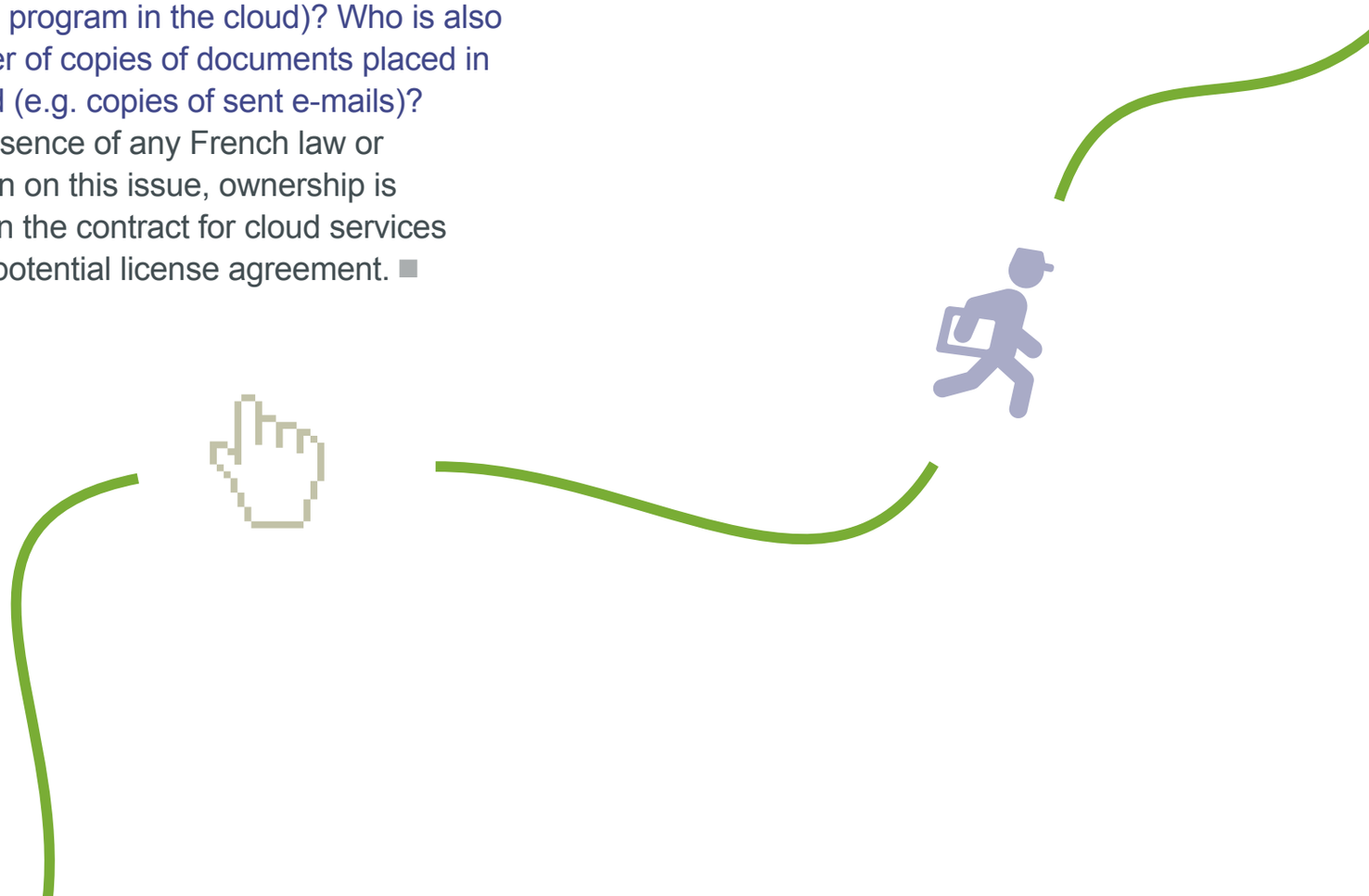
3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   No.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   This is no different to the insolvency/ bankruptcy of any other entity. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   In the absence of any French law or regulation on this issue, ownership is defined in the contract for cloud services and the potential license agreement.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud)? Who is also the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   In the absence of any French law or regulation on this issue, ownership is defined in the contract for cloud services and the potential license agreement. ■



Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes, the French government has shown interest in cloud solutions and is looking to develop a cloud service that would be available to French administrations and companies. This cloud service would be focused on the storage of sensitive data such as healthcare data, administrative data and economic information requiring maximum safety.

   Following the French government's "Call for manifestations of interest", two proposals were selected for developing the Andromède Project: Thalès / Orange and Bull / SFR. A special investment fund was attributed to both.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
   No, but the French government recently selected two cloud services projects in the course of the Andromède Cloud Project.

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   The French Network and Information Security Agency (ANSSI), has published a guideline on managing outsourcing risks. This underlines the risks regarding cloud computing services and makes recommendations such as implementing security measures in order to ensure data security and confidentiality. See: http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf.

   The French National Assembly's report, "Individual rights in the digital revolution" proposes a recommendation on how to evaluate the consequences of data transfer in the context of cloud computing. It recommends an evaluation report of data transfer outside the EU, see: http://www.assemblee-nationale.fr/13/rap-info/i3560.asp.

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   The French Data Protection Authority has published guidance on this issue; http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf. ▶

See also the recommendation of the CNIL which advises companies on cloud computing services issues. http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

Along with general recommendations concerning risk management, data backup, traceability, archiving and maintenance, the CNIL provides advice on cloud computing; especially recommending not using services where there is no guarantee regarding the effective geographical location of the data. It provides guidance as to the content of the cloud service agreement (sub-contracting agreement) such as ensuring provisions (security audits, installations visits, etc.) are included so that guarantees offered by the sub-contractor regarding data protection are effective, including:

- encrypting data according to its sensitivity, or at least ensuring that the sub-contractor has procedures guaranteeing it does not have access to the data;
- data link encryption (using HTTPS connections);
- guarantees regarding network protection, traceability (logs, audits), management of security clearances, authentication, etc.;
- conditions of restitution of data and its destruction in the event of termination or expiry of the contract – including confidentiality provisions in the sub-contracting agreement.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?

The French government has launched an investment fund. Since 2011, it has created 3 procurement models in order to develop cloud computing services: the first two aimed at developing infrastructures, the third focusing on exploiting data.

In 2011, five cloud computing projects were selected, including a cloud designated for universities, a “super computing on demand” operating in cloud computing mode, and a highly secured cloud for healthcare data and medical files. Those projects will benefit from 19 million Euros public support.

A few requests for proposals have been launched by the government in this respect and further information can be accessed via the links below.

- Concerning the call for proposal on Cloud Computing n°1 – http://www.industrie.gouv.fr/fsn/cloud-computing-1/index.php ►

- Concerning the call for proposal on cloud computing n°2 – http://www.industrie.gouv.fr/fsn/cloud-computing/index.php
- Concerning the call for proposal on big data – http://www.industrie.gouv.fr/fsn/cloud-computing-3/

6. Who is or would be the responsible regulator for cloud services?
The CNIL, since it has already published guidance and recommendations on this matter. ARCEP (the electronic communications regulator) is also likely to play a role.

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
No. ■

Security issues

1. Are cloud services providers free from content filtration or censorship obligations?
   There is no mandatory/general filtering or censorship of content. Therefore, cloud service providers are not subject to any such obligation.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   There are no specific laws requiring specific security measures from cloud computing service providers. The provisions of the French DP Act and other special regulations (e.g. for the financial sectors or the recommendations of the ANSSI) ensure a certain level of security. ■

Germany

In Germany, the use of commercial cloud computing services becomes more and more popular, mainly in the private sector. However, data protection and IT security are still major concerns and hinder an even more widespread use. Use of cloud computing services is mainly driven by cost efficiency and flexibility considerations, but reasons for relying on cloud computing services also include enhanced functionality compared to pre-existing tools. While all kinds of cloud services are being tested and operated, SaaS solutions are by far the most common. The public sector is, mainly driven by data security concerns, more hesitant and concentrates, if at all, on clouds managed by the authorities themselves.

German Data Protection Authorities gave up their initial unrealistic obstructive approach on cloud computing and accept the service in general now. However, they expressed serious – but, in our view, mostly unfounded – doubts on the legality of cloud services performed in countries outside the EEA from a data protection perspective. Further, effective control of the cloud provider by the cloud service user as the data controller and transparency concerns are on top of their agenda. It is still heavily debated how data protection requirements such as data control by the customer shall be realised in practice. ■

General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   Yes, only for the sake of completeness. Irrespective of the modality of agreement (click-wrap or other), special obligations apply to e-commerce agreements, including information obligations. For example, there is a very strict law concerning the labelling of acceptance buttons, and non-compliance results in nullity of the contract. ■

Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes. The Rome I Regulation and the Brussels I Regulation allow contracting parties to choose the law and jurisdiction in B2B contracts. There are limitations (e.g. purely domestic contractual situations where mandatory German law remains applicable). In B2C contracts, the choice of law must not deprive the consumer of any mandatory provisions of the consumer's habitual residence (i.e. such law remains applicable regardless of the choice of law).

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   According to Rome I, a contract for the provision of services shall be governed by the law of the country where the service provider has its habitual residence or central administration. The same applies to a rental contract. In the context of cloud services, this is generally the law of the place in which the cloud computing service provider locates its servers. There is no clear authority regarding the applicable law for claims arising out of torts committed over the internet. This depends on the facts of each case. If the tort is closely connected to a contract, a court may apply the applicable law for the contract. There is also a chance that a court will apply the law of the jurisdiction where the alleged damage was sustained.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   According to Rome I, B2C contracts shall be governed by the law of the country where the consumer has his habitual residence, provided the business pursues its commercial or professional activities in the country of the consumer's habitual residence, or directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities. See also Q2 regarding torts.

4. Are there any other relevant issues related to applicable law and cloud computing?
   No. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?

None particularly relating to cloud computing. German consumer protection law is very strict, especially with regard to T&Cs and online transactions – and therefore cloud services. Since summer 2012, special obligations apply to e-commerce agreements, including information obligations. For example, there is a very strict law concerning the labelling of "acceptance buttons" in place in Germany and non-compliance with the law results in nullity of the contract. There are extensive obligations on using customer information and limiting or excluding liability and warranties is only permitted to a limited extent. ■

Data protection

1. Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?
   The German Data Protection Act, Bundesdatenschutzgesetz (BDSG), implements the EU Data Protection Directive and is generally compatible. In Germany stricter requirements apply to data processing, data transfer to non-EEA states (this is not regarded as data processing), and Safe Harbor justification of data transfer to the US (at least in the view of the German Data Protection Authorities).

2. Which law is applicable in the case of a dispute concerning data protection and cloud computing?
   If the cloud data controller is located in an EEA state other than Germany, but is collecting, processing or using personal data at a branch inside Germany, German data protection law is applicable. German data protection law applies if the cloud data controller is located outside the EEA and collects, processes or uses personal data inside Germany (e.g. by using servers, cookies, or desktop clients in Germany).

   When determining which group entity has actual control over the personal data and is therefore the data controller, German Data Protection Authorities can be very strict. For example, they take the view that Google Ireland is not the data controller with respect to German users. Instead, they regard Google Inc. in the US as the data controller because they think that the relevant decisions are taken by Google US.

3. Who is the data controller in a cloud computing service?
   A data controller is the person/entity who determines the purpose and manner in which data is processed. Whether this is the user of cloud computing services or the cloud services provider depends on the particulars of each case (i.e. the actual level of control parties have over the data). Normally, the user is seen as the controller. With private end users, the German Data Protection Authorities' approach is that they do not require the conclusion of a data processing agreement with the cloud provider (although the wording of the law does not distinguish between private end users and other controllers). ►

4. Who is the data processor in a cloud computing service?
A data processor is the person who processes data on behalf of the controller. Whether this is the user of cloud computing services or the cloud services provider depends on the facts of each case (i.e. the actual level of control parties have over the data). Normally, the cloud provider is seen as the processor. In case of private end users, the German Data Protection Authorities' approach is that they do not require the conclusion of a data processing agreement with the cloud provider (although the wording of the law does not distinguish between private end users and other controllers).

5. If the cloud provider is a data processor, what are its obligations under data protection law?
A data processor must take appropriate technical and organisational security measures. Such measures need to be specified in sufficient detail in a written form data processing agreement. The processor must comply with the orders of the data controller regarding the collection, processing, and use of the data and with other obligations that are laid down in the commissioned data processing agreement. If the processor believes that an instruction by the controller violates the BDSG or other data protection provisions, the processor shall inform the controller of this immediately. Since most cloud services are standardised, the user may find it difficult to enforce such rights in practice.

6. Is there a requirement to notify end users about the use of cloud services?
Yes, if the cloud service is outside the EEA or the cloud provider is the data controller. If the cloud provider is a data processor inside the EEA, no.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?
Generally no, if the data controller appointed an in-house data protection officer (mandatory in most cases).

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?
Data transfer in cloud services must comply with the general rules that apply to data transfers outside the EEA. Besides the normal justification for data transfer (e.g. necessity to perform a legal obligation or with the data subject's consent), a special justification for transfer data outside the ▶

EEA is required. This includes:

- transfer to certain white listed countries;
- Safe Harbour certification in case of transfer to the US;
- agreement on Binding Corporate Rules;
- use of EU standard contractual clauses.

9. Are cloud providers permitted to use sub-processors?
Yes, insofar as it is allowed in the data processing agreement between the data controller and the data processor. Sub-processing agreements must mirror the obligations in the head agreement.

10. What are the security requirements connected with processing data?
Technical and organisational measures must be implemented in order to comply with the requirements of the BDSG. This comprises:

- logical and physical access control;
- disclosure control;
- input control;
- job/order control;
- availability control;
- the separate processing of collected address data for different purposes.

It is up to the data processor by which means he ensures security as long as it is effective. There are no specific requirements for cloud computing. Data controllers are obliged to control the data processor. It is subject to debate as to how this can be achieved in cloud computing – one option is auditing/ control by a qualified third party.

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?
Under German data protection law, the transfer of sensitive data such as health data, trade union affiliation or religious beliefs cannot be justified by a normal balance of interest. The transfer of sensitive data can only be justified with the data subject's consent or in other very specific circumstances (e.g. the protection of vital interests).

With respect to non-EEA clouds, the German Data Protection Authorities argue that processing sensitive data in clouds is generally not permissible (from their written opinion, it is not clear whether they would accept consent). We think that consent or, in rather exceptional cases, a balancing of interests can justify the processing of ▶

sensitive data in non-EEA clouds. The German Banking Act (Kreditwesengesetz) the German Securities Trading Law (Wertpapierhandelsgesetz), the German Investment Act (Investmentgesetz) and the German Insurance Supervision Act (Versicherungsaufsichtsgesetz) contain strict regulations for outsourcing which are often impossible to meet in a public cloud context.

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?

The existing normal data protection legislation (BDSG, German Telemedia Act (Telemediengesetz), German Telecommunications Act (Telekommunikationsgesetz)) applies. There is no specific data protection legislation existing or planned for cloud computing. With regard to normal data protection, the EU General Data Protection Regulation (which applies to all of Europe) is expected to enter into force in 2014 at the earliest if agreed. With regard to employee data, a new law on employee data protection is expected to come into force in 2013/2014. The far-reaching ban on the transfer of personal data to entities outside the EEA that telecommunication providers are currently subject has been lifted. This means that the general provisions on data transfer abroad will apply to telecommunications providers. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   Standardisation of cloud computing is strongly supported by the German Federal Ministry for Economics (BMWi). The Federal Office of Information Security (BSI) is responsible for standardisation in IT environments. The German Institute for Standardisation, Din, (www.din.de), which is not a public institution, also sets standards.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   The white paper "Security Recommendations for Cloud Computing Providers" published by the Federal Office of Information Security (BSI) provides governmental advice concerning interoperability in cloud computing platforms and recommends a number of industry standards for limiting interoperability and portability issues which can apply to cloud computing, some of which are already being used. These include the Open Cloud Computing Interface (OCCI) of the Open Grid Forum, the vCloud API from VMware and the Open Virtualization Format (OVF).

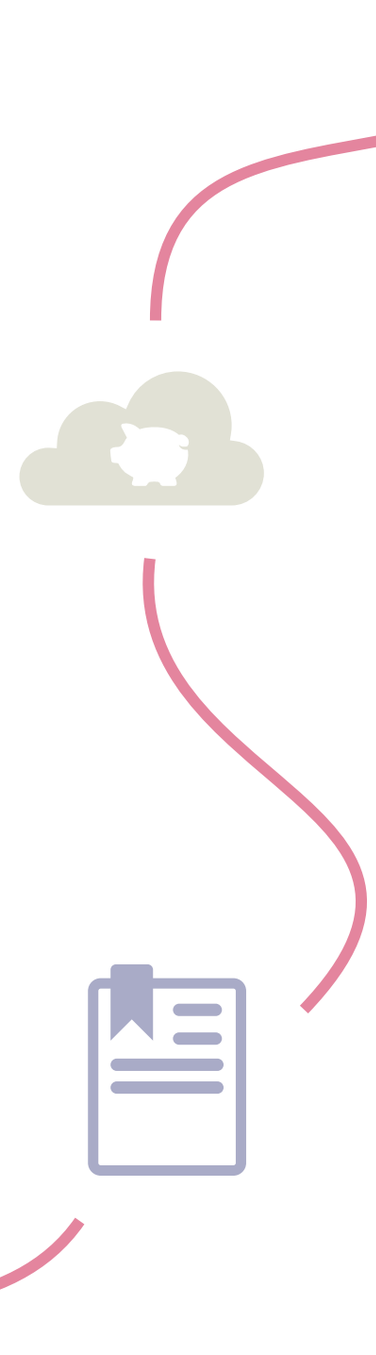
4. Are there applicable international standards relevant for cloud computing that are commonly used?
   The study "Das Normungs- und Standardisierungsumfeld von Cloud Computing" sets out the relevant international standards and can be found at http://www.bmwi.de/BMWi/Navigation/Service/publikationen,did=476730.html

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   Standard SLAs are commonly used and mainly dictated by the cloud provider, at least in bulk cloud business.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   In general and to a certain degree, the cloud provider is obliged to provide support for migration as an ancillary contractual duty and according to the principle of good faith. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?
   The German Banking Act (Kreditwesengesetz) contains special duties for financial institutions concerning outsourcing activities and processes to external companies, which are essential for the performance of banking transactions, financial services or other services typically performed by these institutions. Similar regulations apply for financial institutions dealing with securities, funds and insurances according to the German Securities Trading Law (Wertpapierhandelsgesetz), the German Investment Act (Investmentgesetz) and the Insurance Supervision Act (Versicherungsaufsichtsgesetz). ■



Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, provided that the license is sub-licensable. Another issue is whether the customer actually needs a sub-license – this may depend on the technical infrastructure and the license of the provider.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   No. The use of standard terms and conditions is common, but every provider has its own standard terms.

3. Is it possible to use Open Source Software for cloud computing?
   Yes.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   Yes. For example, according to the German Copyright Act (Urheberrechtsgesetz), a person who infringes a copyright faces an action for injunctive relief requiring the wrongdoer to remedy the impairment and to cease and desist if there is a danger of repetition of the acts of infringement, as well as an action for damages if the infringement was intentional or the result of negligence. Similar provisions exist for patents, trademarks, utility models, etc.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   Yes, infringers may be subject to a fine or, in serious cases, imprisonment.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   German law knows the “concept of liability of the interferer” (Störerhaftung) which means that an internet provider can be subject to civil (not criminal) liability even if it did not act negligently. Criminal liability requires fault. However, Germany implemented the E-Commerce Directive which contains provider liability privileges. With regard to host providing, cloud providers are generally not liable for third party content hosted on their service provided that they do not know about the third party infringing content hosted on their platform, or they delete the content without undue delay after gaining knowledge. If the service is not purely host providing, but the cloud provider also takes advantage of ▶

the stored data (e.g. by generating advertising revenue), there is a risk that the liability privilege does not apply. In any case, the host-providing privilege does not apply to injunctive relief. Possible sanctions comprise of cease-and-desist orders, injunctions, damages, and criminal liability in serious cases.

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?

Yes. In addition to the notice-and-takedown obligation, the implementation of a filter mechanism by the host provider in order to prevent similar infringements in the future may be necessary depending on the facts of the case. ISPs are generally obliged to respond to queries by police/prosecution service/court authorities. A proactive information obligation exists for certain serious crimes (not for normal copyright violation). In the implementation of the EU Enforcement Directive 2004/48/EC, the German Copyright Act (Urheberrechtsgesetz) now contains information rights for rights holders in certain cases. This is not a proactive information obligation.

8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?

No. ■

International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   There is no specific law for clouds, but the general international agreements like the SWIFT/TFTP Agreement apply to cloud services. In practice, US/US owned cloud providers operating in Germany disclose data to US authorities on requests justified (only) by US law, although this may conflict with German data protection law. ■

Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   This depends on contractual arrangements. Without specific arrangements, the cloud provider is liable for damages if negligent. Depending on the individual circumstances, there may be contributory negligence of the cloud user (e.g. in cases where it was reasonable to back up data and no backup was made).

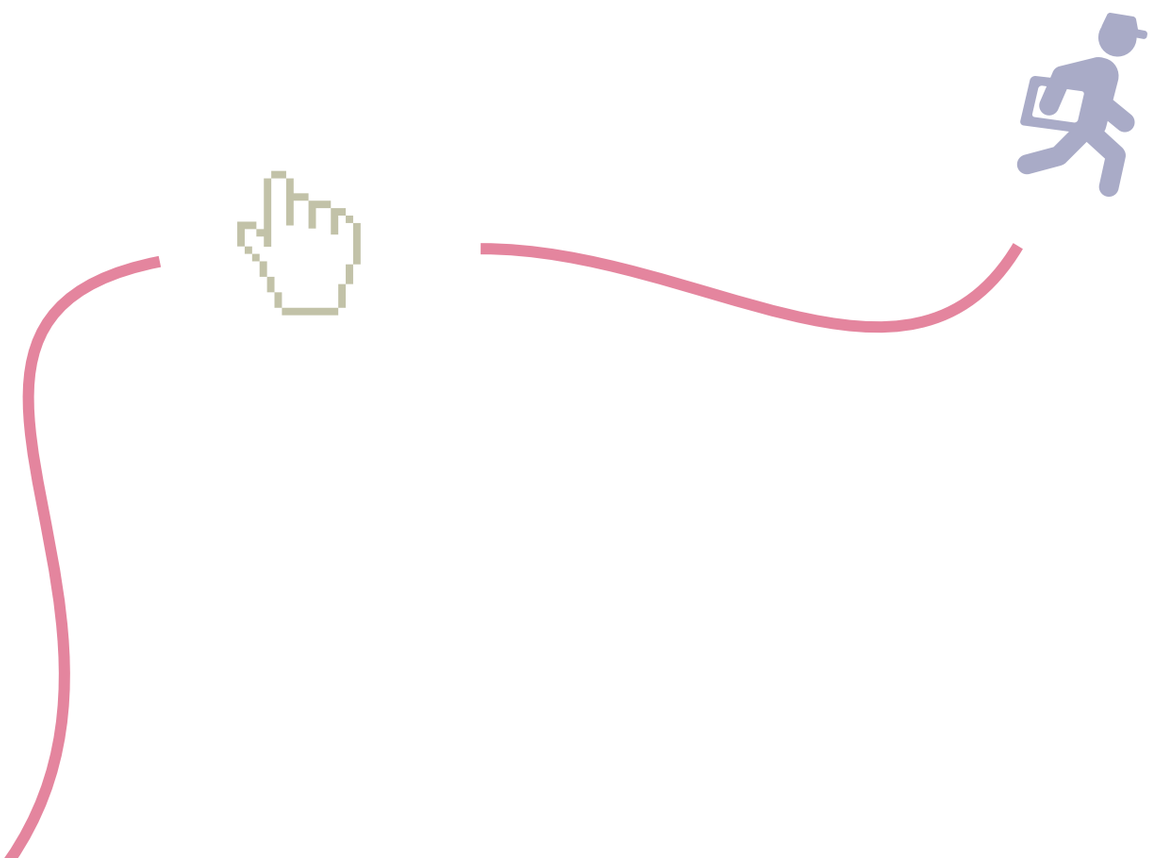
2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   General terms and conditions are heavily regulated, even in B2B situations. As a rule of thumb (there are exceptions), liability can only be excluded for simple negligent breach of non-cardinal obligations. For example, in case of storage of data in a cloud, the storage obligation is a cardinal obligation. In case of an inadmissible clause, the court will apply the standard of law, which means uncapped liability. Careful drafting is necessary. In individually negotiated contracts, liability can be excluded except for intent.

3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   Yes, if T&Cs are used, both in B2C and B2B (less strict) situations. In general, it is not possible to exclude warranty obligations as a whole, even in B2B situations. The scope of the allowed limitations depends on the nature of the services to be provided under the cloud contract.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   From a practical point of view, there is a high risk that cloud data will become (at least temporarily) inaccessible. From a legal perspective, in case of insolvency, the cloud service user is generally entitled to claim the return of his data from the insolvency administrator, but as soon as a cloud provider is offline the enforcement may take a long time. It is advisable to technically ensure portability of data in order to facilitate the transfer in case of insolvency. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   There is no concept of absolute "ownership" of data in German law. If intellectual property rights (e.g. copyright) apply to the data, there will be a person who has these rights. In all cases, the "ownership" will (also) be determined by the contract between the cloud provider and the user. Usually, the cloud provider asks for limited rights that are necessary to provide the service in the cloud contract offer.
2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud)? Who is also the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   This depends on the license under which the data was placed in the cloud service and the type of modification. ■



Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
German public institutions are highly interested in cloud computing as possible means of cutting costs. German authorities, especially at state (Bundesland) level are giving serious consideration to establishing private clouds. At present, we are not aware of any public authority public clouds in operation. With regard to cloud computing in the private sector, the German Federal Ministry for Economics (BMWi) has launched a cloud computing action program which includes a promotional/support program, the Trusted Clouds program. This has received €50 million of public sector funding and another €50 million from the private sector.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
German public institutions are highly interested in cloud computing, as a possible means of cutting costs. German authorities, especially at state (Bundesland) level are seriously considering the establishment of cloud strategies (private clouds). There are concrete projects that aim at the introduction of private clouds for the public sector (e.g. in Berlin and in Rhineland-Palatinate). As far as we can see, no public clouds are in operation yet.

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
Recently published guidelines by public institutions include:

- a white paper published by the Federal Office of Information Security (BSI) dealing with the minimum information security requirements of cloud computing, aimed at the private and public sectors (2011);
- a white paper on Guidelines on Cloud Computing by the Working Group Technology and Media of the German Data Protection Authorities (2021).

Although these papers are not directly legally binding, the published views indicate the manner in which German authorities will view and examine cloud computing arrangements. ►

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
The Data Protection Authorities and the BSI try to raise awareness (e.g. on their websites).

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
We are not aware of any models.

6. Who is or would be the responsible regulator for cloud services?
Regarding data protection, the 16 Data Protection Authorities at state level and the Federal Data Protection Commissioner would be responsible (however, the cloud provider has the option to escalate data protection conflicts to the courts for a final decision). From a technical and organisational point of view, the German Federal Office for Information Security (BSI) publishes minimum security standards.

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
No, but it is likely that public authorities will require strict adherence to the security standards set out by the Federal Office of Information Security (BSI). ■

Security issues

1. Are cloud services providers free from content filtration or censorship obligations?
   Depending on the circumstances, a cloud provider may be subject to an obligation to content filtration with regard to content marked as infringing by the rights holder. Plans to introduce mandatory internet filtering (aimed at targeting online child pornography) were abandoned in 2011.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   There is no law specifically aimed at cloud providers. Providers must comply with the general data security requirements (e.g. they must implement the technical and organisational measures outlined in Q10 in the Data Protection section). Although not directly legally binding, cloud providers should follow the BSI's technical and organisational guidelines, since it is likely that a court would apply them when determining the necessary standard of care. ■

Hungary

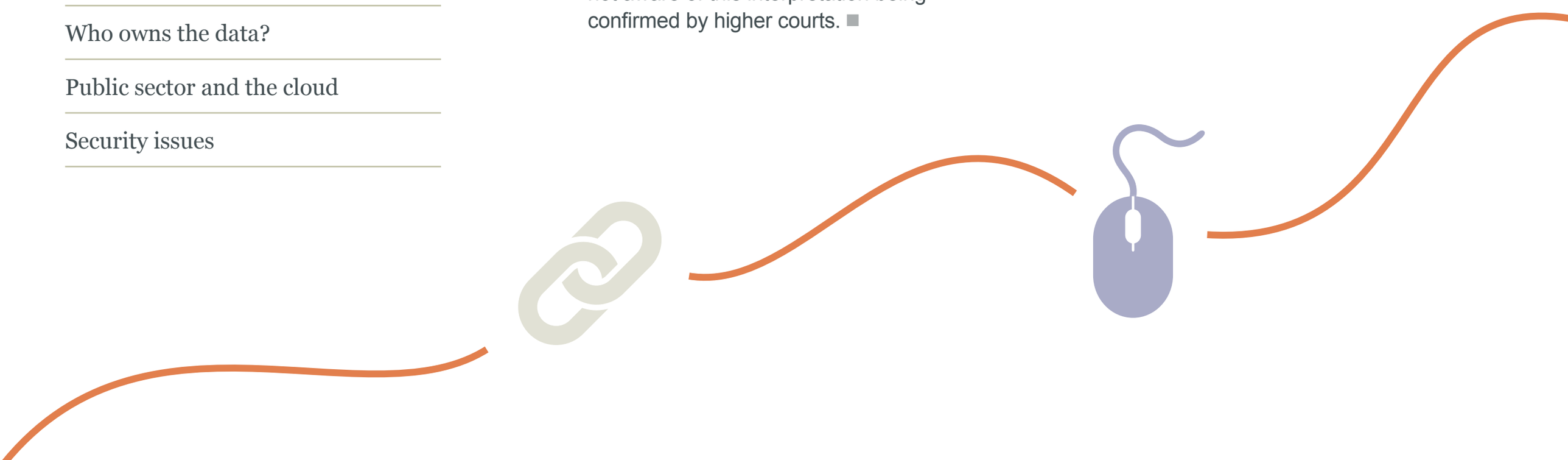
Hungarian companies are keen to move to the cloud, particularly given the cost efficiencies it offers. Some enterprises have already deployed their own clouds, while others, including SMEs, are using third party services. The public sector seems to be reluctant to use external vendors, nevertheless there is growing interest from the government for a pan-government cloud or to find trusted vendors who are ready to provide the required level of service for public bodies.

The Hungarian Data Protection Authority has not issued any guidelines or recommendations on cloud computing. The Hungarian Financial Supervisory Authority (PSZÁF) however issued a general circular for Hungarian financial institutions on the use of cloud computing technologies (in Hungarian: http://www.pszaf.hu:80/data/cms2364896/vezkorlev_4_2012.pdf); a remarkable first step in analysing the legal issues of cloud computing.

In Hungary data protection has been considered a burden of deploying cloud services since the Privacy Act still contains an outdated provision which expressly precludes sub-contracting (outsourcing of data processing functions by a processor to a sub-processor). This odd requirement clearly conflicts with the needs of the cloud computing industry, not to mention EU law. While the head of the Data Protection Authority recently also acknowledged the need for sub-contracting he also stressed that until the Privacy Act is amended accordingly the agency cannot disregard statutory law. However, the head of the Agency also admitted the conflict between Hungarian and EU law and stressed that sub-contracting shall be possible if certain criteria are met. It is expected that the Privacy Act will be amended and the outdated prohibition of sub-contracting will be lifted. ■

General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   The use of click-wrap agreements is widespread in Hungary. Whether they are lawful is a controversial issue since the Hungarian Copyright Act requires license agreements to be in written form. There is an exception for software products, though it remains unclear whether this can be applied to online licenses. Some courts consider click-wrap agreements as “implied consent/ agreement” and consider this lawful. We are not aware of this interpretation being confirmed by higher courts. ■



Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes, in accordance with Rome I Regulation on the law applicable to contractual obligations and Law Decree no. 13 of 1979 on international private law.

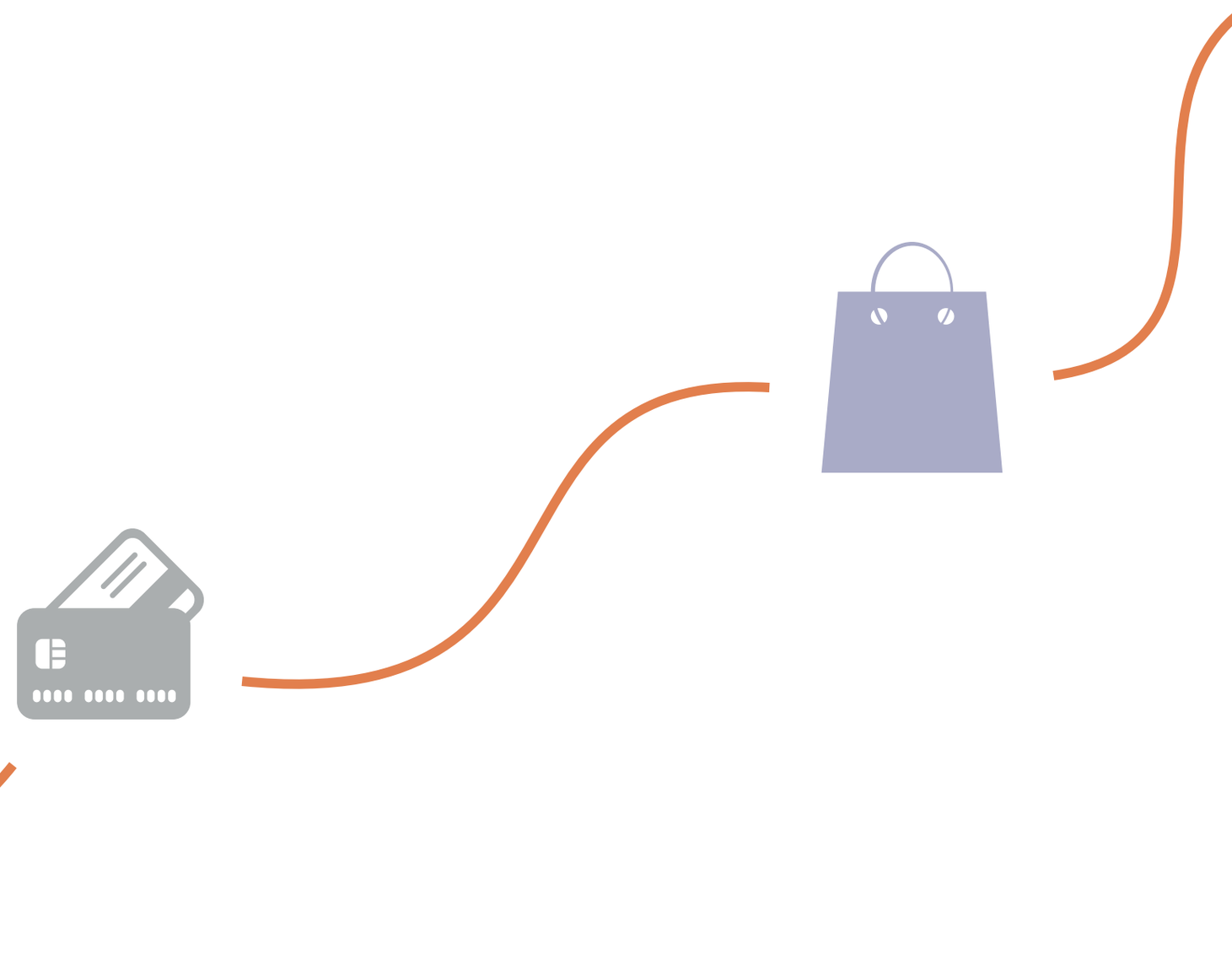
2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   The applicable law is determined in accordance with Rome I. In legal disputes, Hungarian courts may rule if the registered seat of the plaintiff is located within the territory of Hungary.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   The applicable law is determined in accordance with Rome I Regulation. According to Decree Act 13 on international private law, Hungarian courts may rule on a legal dispute initiated by or against a Hungarian consumer even if the governing law has been stipulated in the contract.

4. Are there any other relevant issues related to applicable law and cloud computing?
   No. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?
   In all e-commerce related matters the provisions of Act CVIII on E-commerce are applicable. ■



Data protection

1. **Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?**
   The Hungarian Privacy Act on informational self-determination and freedom of information is intended to implement the EU Data Protection Directive. There are issues where the implementation of the Directive is controversial, such as legal grounds of data processing, transfer to third countries and use of sub-processors.

2. **Which law is applicable in the case of a dispute concerning data protection and cloud computing?**
   The applicable law is determined by the provisions of the Rome I Regulation and the Decree. However, the scope of the Hungarian Privacy Act covers all data processing activities carried out within the territory of Hungary.

3. **Who is the data controller in a cloud computing service?**
   The Hungarian Data Protection Authority has not issued any guidelines or recommendations. The answer depends on the details of the service. Hungarian data protection law has been strict as to the definition of the data controller. If an entity is able to take an autonomous decision in relation to its processing activities then it is likely that it will be considered data controller.

4. **Who is the data processor in a cloud computing service?**
   Hungarian law is quite strict as to definition of data controller and data processor. Data processors must perform only technical operations according to the instructions of a data controller and cannot take autonomous decisions on the data processed.

5. **If the cloud provider is a data processor, what are its obligations under data protection law?**
   Data processors are obliged to ensure data security and implement technical and operational measures determined by the Privacy Act and other data protection related legislation (e.g. preventing data breach, unauthorised access, unlawful data transfer, accidental destruction and connection of data kept in different databases). When deciding about measures to ensure data security, both data controllers and data processors must choose technology providing high security, unless this would result in disproportionate difficulties on the side of the data controller (the Act does not mention difficulties of data ►

processors). A data processor cannot make processing related decisions and must perform its tasks in accordance with the instructions of the data controller.

6. Is there a requirement to notify end users about the use of cloud services?

The Privacy Act contains a general requirement to notify data subjects about all circumstances regarding processing of their personal data (i.e. purpose, legal basis, duration of data processing, retention periods and data processors). While there are no legal provisions addressing notification in case of use of cloud services, the above general requirement may trigger a notification requirement.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?

The Privacy Act does not contain any special notification or registration requirement addressing cloud services and/or cloud providers. The Privacy Act contains a general registration requirement according to which any data processing activities must be notified by the data controller to the authority. While data controllers are required to register their data processing activities, data processors are not required to do so. The Hungarian DPA is required to approve or reject a data processing request within 8 days of receipt. Data processing may only begin on receipt of the DPA's approval. If the DPA does not respond within 8 days, data processing can begin without approval. Data controllers need to pay a fee for registration. The amount has not been disclosed yet. According to government leaks, it is likely to be minimal (approximately €10). Until this fee is confirmed, new registration requests can be filed for free. The Privacy Act provides for certain exceptions to the authorisation requirements. Processing of certain types of data, such as employee or customer data, is exempt. In relation to customer data, financial institutions, community service providers and electronic communication service providers have no exemption.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?

Data can be transferred to a country located outside the EEA, if one of the following criteria is met:

- the data subject has expressly consented to the transfer;
- the data subject previously consented to local processing or other valid legal basis apply (e.g. legitimate interest, legal obligation) and an adequate level of ▶

protection is ensured in the non-EEA country;
- the transfer is based on an international treaty.

Adequate level of protection is ensured if it is so determined by a binding EU legislation or an international agreement concluded between the non-EEA country and Hungary (e.g. participants in the Safe Harbour Agreement). The Privacy Act does not contain clear provisions regarding the use of SCCs and BCRs. The Authority recently confirmed that SCCs must be accepted, but seems to be reluctant to accept BCRs claiming that these are not mentioned in statutory law.

The Hungarian data protection regime has been traditionally very strict as to the legal grounds for data processing. The Privacy Act, which has been in force since 1 January 2012, essentially retains the general consent requirement but also enacted a limited implementation of Article 7(c) and (f) of the EU DP Directive (95/46/EC) by adding further requirements not included in the Directive to legal obligation and legitimate interest. This limitation is controversial given the recent case law of the Court of Justice of the European Union (CJEU), which ruled in November 2011 that a similar provision in the Spanish legislation was incompatible with EU law (CJEU C-468/10 and C-469/10). CJEU also ruled that Art 7(f) of the Directive shall have direct effect in Member States. Therefore a data controller can rely on the Directive if a Member State has implemented this provision incorrectly. The Hungarian DPA confirmed that this is an acceptable position, provided that the general proportionality requirements are also met. It is expected that the legislator will solve this controversy by removing the additional requirements from the Privacy Act.

Data transfer within the EEA is considered as transfer within the territory of Hungary. The data controller is obliged to keep a data transfer register which includes the date, legal basis, recipient and scope of data of the data transfer. The data kept in the data transfer register must be kept for at least 5 years (20 years for special or sensitive data).

9. Are cloud providers permitted to use sub-processors?

The Privacy Act contains an outdated provision which expressly precludes sub-contracting (outsourcing of data processing functions by a processor to a sub-processor). This odd requirement clearly conflicts with the needs of the cloud computing industry, not to mention ▶

EU law. While the head of the Data Protection Authority recently also acknowledged the need for sub-contracting he also stressed that until the Privacy Act is not amended accordingly the agency cannot disregard statutory law. However, the head of the agency also admitted the conflict between Hungarian and EU law and stressed that sub-contracting shall be possible if certain criteria are met, for example, if a processor is established outside of EEA and the C2P SCCs are based on Commission Decision 2010/87/EU. It is expected that the Privacy Act will be amended and the outdated prohibition of sub-contracting will be lifted. NAIH also recognises that it is a controversial situation where a data processor established in Hungary cannot outsource to a sub-processor. However, according to the NAIH, even if this is odd, they cannot ignore the law. Only the legislator can solve this by removing the prohibition of outsourcing form the DP Act.

Despite of the current controversial legislation businesses usually take a business-minded approach in this regard and use sub-processors.

10. What are the security requirements connected with processing data?

Both data controllers and data processors, within their scope of activities, are obliged to ensure data security, implement such technical and organisational measures and establish procedural rules to maintain security over data. Personal data must be protected with appropriate measures especially against:

- unauthorised access;
- unauthorised alteration;
- unauthorised transfer;
- unauthorised disclosure;
- unauthorised deletion or destruction;
- accidental destruction or damage.

There must be adequate technical solutions for the protection of electronically processed sets of data kept in various registers that ensures the data cannot be directly connected with the data subjects. In case of automated processing of personal data, additional measures must be implemented by the data controller and the technical data processor. When determining measures to ensure data security, both data controllers and data processors must choose the technology providing higher security, unless this would result in disproportionate ►

difficulties on the side of the data controller (the Act does not mention difficulties of data processors).

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?
Sensitive data can only be processed if one of the following applies:

- the data subject has consented in writing;
- processing of the data is necessary for the execution of an international treaty or the enforcement of a right determined by the Fundamental Act of Hungary (the Constitution) or national security, crime prevention and law enforcement purposes;
- it is ordered by law.

The data controller is obliged to keep a data transfer register that includes the date, legal basis, recipient and the scope of data included in the data transfer. The data kept in the data transfer register must be kept for at least 5 years (20 years for special or sensitive data). Any data processed by a financial institution which relates to the customer qualifies as bank secret, thus stricter rules apply according to the Financial Institutions Act. Financial institutions are required to register their processing activities on customer data with the DPA and must also appoint a data protection officer.

The Hungarian Data Protection Authority has not issued any guidelines or recommendations on cloud computing. The Hungarian Financial Supervisory Authority (PSZÁF) however issued a circular for Hungarian financial institutions on the use of cloud computing technologies. While the latter contains general recommendations this is a remarkable first step in analysing the legal issues of cloud computing by a Hungarian authority.

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?
Industry groups are lobbying for the removal of the outdated provisions from the Privacy Act, including the exclusion of sub-processors and the limited legal basis of data processing. According to non official information the head of the Hungarian DPA requested the Minister of Justice to submit a legislative amendment to the parliament. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   Yes, the Hungarian Standards Institution.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   We are not aware of guidance or standards.

4. Are there applicable international standards relevant for cloud computing that are commonly used?
   We are not aware of guidance or standards. International standards are not directly applicable in Hungary. They only apply when the Hungarian Standardisation Institute validates them as Hungarian standards.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   We are not aware of model agreements.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   We are not aware of any issues. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?

Hungarian law enables a financial institution or insurance company to outsource data processing activities. Outsourcing must comply with the general requirements contained in the Privacy Act. The outsourcing service provider must ensure, to a degree corresponding to the risk, the same personnel, material and security measures that are applicable to a financial institution. A financial institution must notify the Hungarian Finance Supervisory Authority (HFSA) about the outsourcing within two days after signing the outsourcing service agreement. The applicable law also contains certain provisions as to outsourcing (i.e. the content of the agreement and the possibility of investigations by the HFSA and the Hungarian Central Bank).

The Hungarian Financial Supervisory Authority (PSZÁF) issued a circular for Hungarian financial institutions on the use of cloud computing technologies. While the latter contains general recommendations this is a remarkable first step in analysing the legal issues of cloud computing by a Hungarian authority. ■

Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, it is possible.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   We are not aware of such standard terms and conditions.

3. Is it possible to use Open Source Software for cloud computing?
   Yes, it is possible.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   Yes, provided that none of the statutory exemptions apply to the cloud provider. Hungarian law implemented the EU IP Enforcement Directive (2004/48/EC).

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   Yes, but there is no case law on criminal sanctions in the field of cloud computing. Criminal sanctions are widely applied in the offline environment (e.g. in combating piracy). In the online environment it is difficult to conclude a criminal proceeding. From time to time police and prosecutors start proceedings against P2P networks.

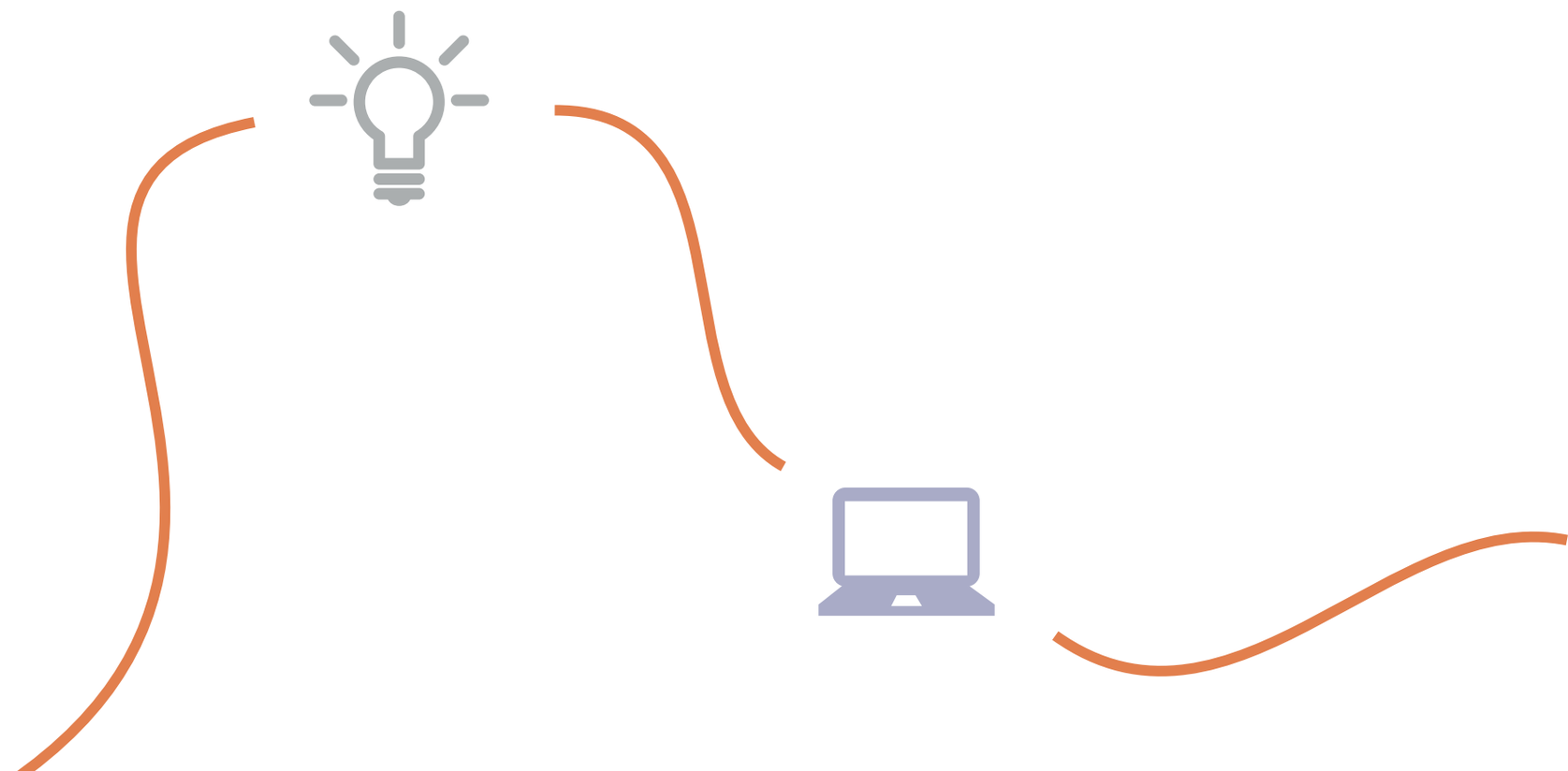
6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   Hungary implemented the EU E-Commerce Directive (2000/31/EC) so same or similar exceptions apply for the ISP. If, despite the exceptions in the Hungarian E-Commerce Act, an ISP is liable of any illegal activities, it may face civil and criminal sanctions. Criminal sanctions are rarely applied. Civil sanctions include cease and desist injunctions, declaration of infringement, compensation of damages etc. Hungary also implemented the EU IP Enforcement Directive (2004/48/EC). It is expected that Hungarian courts would follow the relevant rulings of CJEU, including SABAM v. Netlog (C-360/10). ►

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?

Yes. Hungary implemented the notice-and-takedown procedure as set out in the EU E-Commerce Directive (2000/31/EC). The service provider needs to inform the content provider of any measures taken in connection with the notice-and-takedown procedure. However, the ISP is not obliged to inform any authorities about any measures taken.

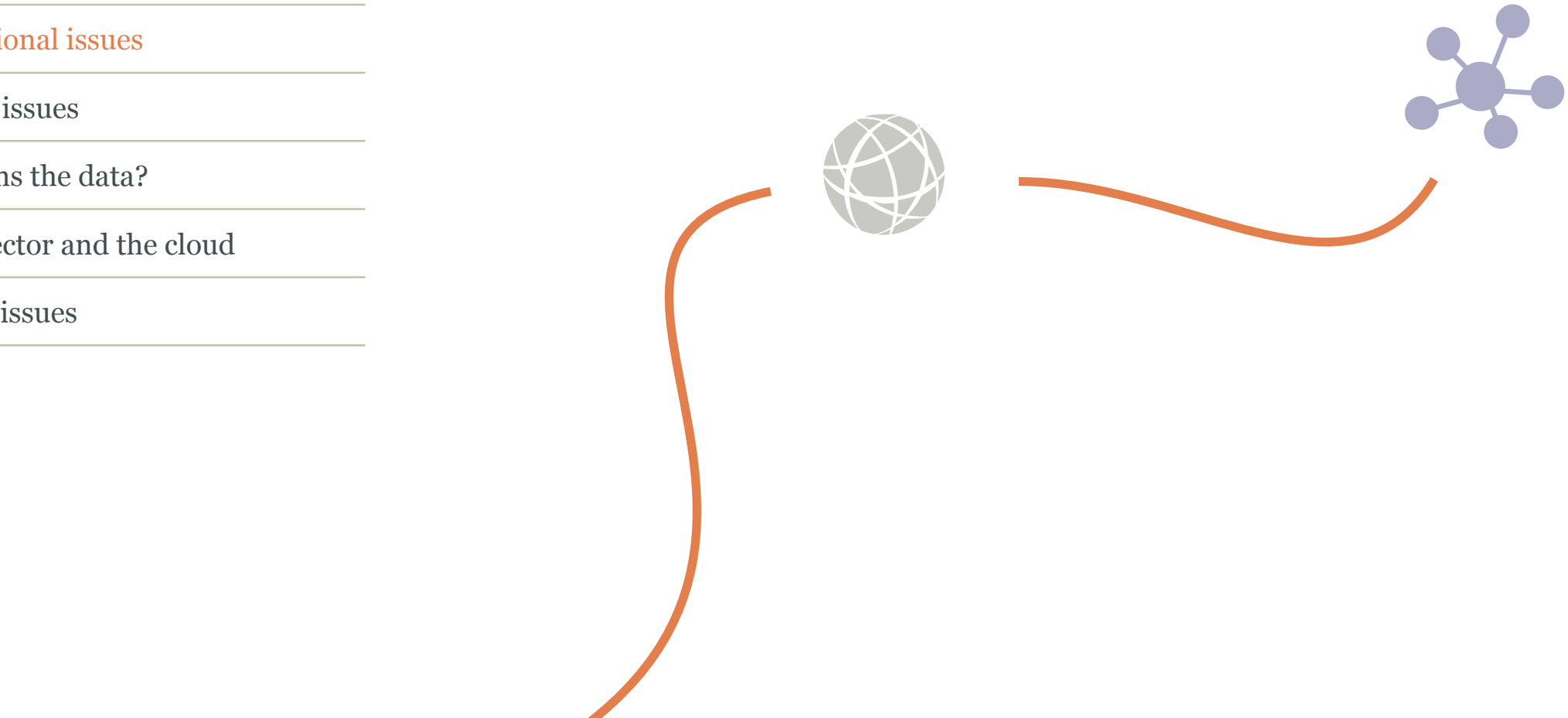
8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?

No. ■



International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   Yes. For example the agreement between Hungary and the USA on enhancing co-operation in preventing and combating crime, which amongst other things, allows the transfer of fingerprint data. ■



Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   Under the Privacy Act, the data controller will be held liable for the damages caused by the data processor and will have to reimburse the damages caused. The agreement concluded between the data controller and the data processor can include provisions settling liability.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   Although the data controller and the data processor may have a separate agreement for the provision of data processing, under the Privacy Act, a data controller will be held liable for and pay all damages arising from a data loss. According to general provisions on liability, as set forth in the Hungarian civil Code, liability for breach of contract as a result of deliberate or gross negligent action or felony cannot be excluded. Nor can liability excluded for breach of contract resulting in death, personal injury or adverse health effects. Save this prohibition liability for breach of contract can be excluded or limited, if the disadvantages of exclusion/limitation are offset by the adequate reduction of the consideration or by other advantage.

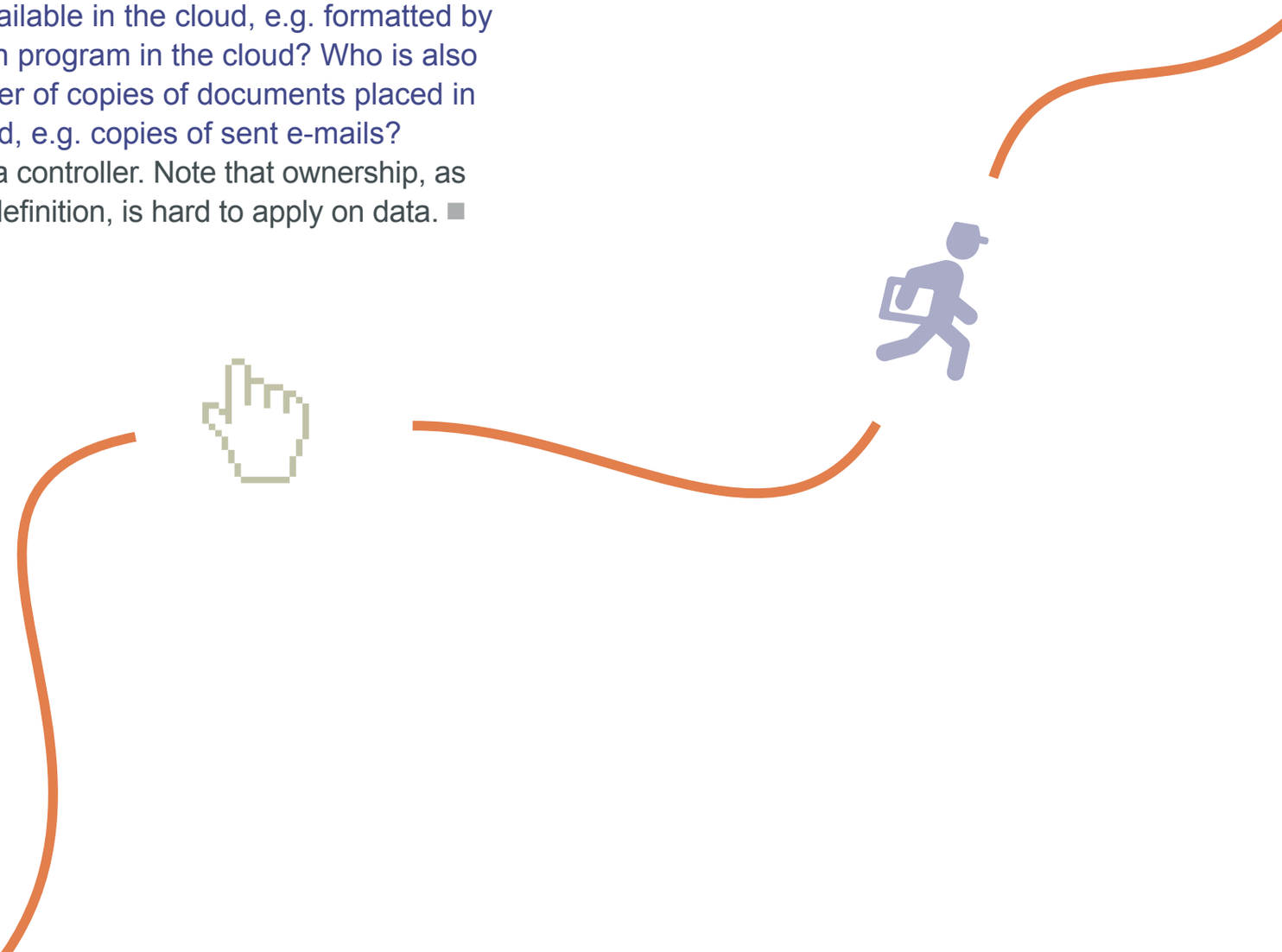
3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   No.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   The data controller is liable towards the data subjects and bears the liability if the cloud service provider becomes insolvent. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   The data controller. Note that ownership, as a legal definition, is hard to apply on data.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud, e.g. formatted by the open program in the cloud? Who is also the owner of copies of documents placed in the cloud, e.g. copies of sent e-mails?
   The data controller. Note that ownership, as a legal definition, is hard to apply on data. ■



Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   In Hungary public institutions seem to have concerns in relation to transfering their data to the cloud due to technical, security and political reasons. However, there is growing interest from the government for a pan-government cloud or to find trusted vendors who are ready to provide the required level of service for public bodies.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
   No, but the government is interested in G-Cloud.

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   The Hungarian Financial Supervisory Authority (PSZÁF) issued a circular for Hungarian financial institutions on the use of cloud computing technologies. While the latter contains general recommendations this is a remarkable first step in analysing the legal issues of cloud computing by a Hungarian authority.

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   We are not aware of public processes in relation to cloud services for the public sector. For financial institutions the Hungarian Financial Supervisory Authority (PSZÁF) issued a circular on the use of cloud computing technologies, which is a remarkable first step in analysing the legal issues of cloud computing by a Hungarian authority.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
   We are not aware of models.

6. Who is or would be the responsible regulator for cloud services?
   The legislation regulating cloud computing would be prepared by the Government and the Data Protection Authority would submit recommendations. We are not aware of such draft legislation or plans. ►

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
Certain general obligations and recommendations apply for suppliers of the public sector, but according to our best knowledge there are no specific obligations on cloud providers. ■

Security issues

1. Are cloud services providers free from content filtration or censorship obligations?
   Yes. Hungary implemented the EU E-Commerce Directive (2000/31/EC) so the general rules set out in this apply in Hungary. It is expected that Hungarian courts would follow the relevant rulings of CJEU, including SABAM v. Netlog (C-360/10).

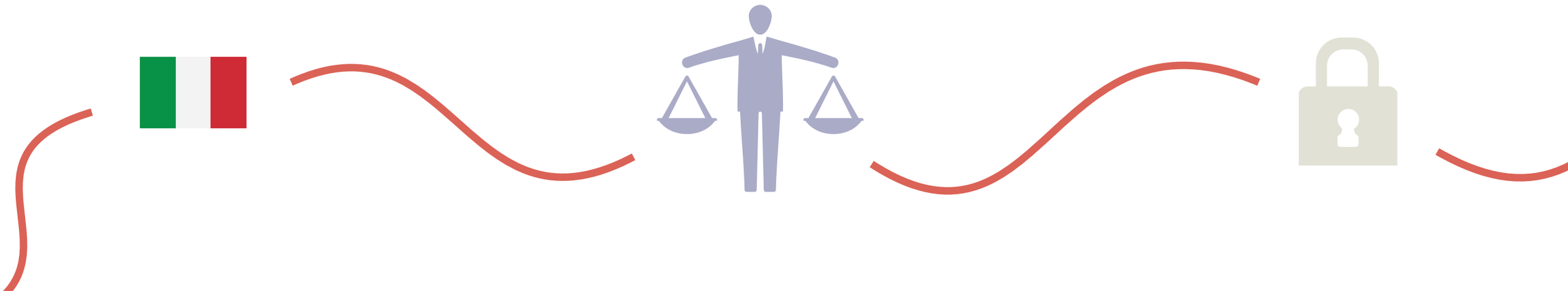
2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   The Privacy Act contains general obligations to ensure security of data. Both data controllers and data processors, within their scope of activities, are obliged to ensure data security, implement such technical and organisational measures and establish procedural rules which are deemed necessary to maintain security over data. Personal data must be protected with appropriate measures especially against: (i) unauthorised access; (ii) unauthorised alteration; (iii) unauthorised transfer; (iv) unauthorised disclosure; (v) unauthorised deletion or destruction; and (vi) accidental destruction or damage. It must be ensured with adequate technical solutions for the protection of electronically processed sets of data kept in various registers that the data kept in these registers cannot be directly connected with the data subjects. In case of automated processing of personal data additional measures must be implemented by the data controller and the technical data processor. When determining measures to ensure data security both data controllers and data processors must consider state of the art technology and choose the one providing higher security, unless this would result in disproportionate difficulties on the side of the data controller (the Privacy Act does not mention difficulties of data processors here). ■

Italy

There is growing interest in cloud computing services in Italy, and according to some studies 69% of medium to large companies have already adopted cloud solutions for their business. Smaller companies are follower in their larger counterparts footsteps but at a slower rate.

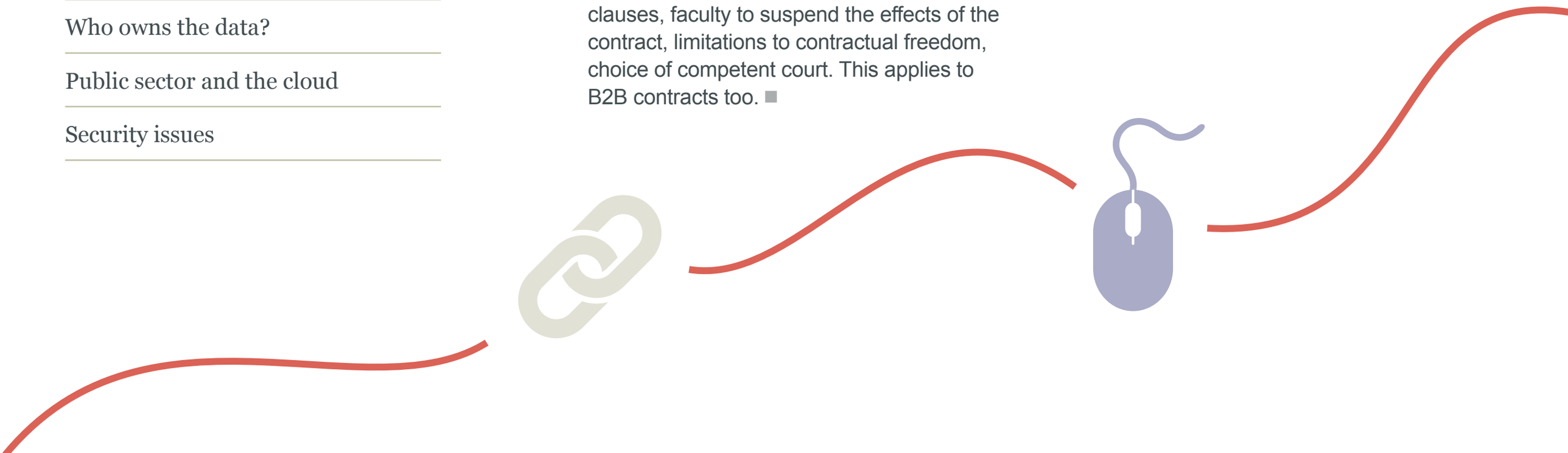
For those that haven't taken up the cloud, the main concerns seem to be the lack of a clear legal regulation, the difficulties in integrating cloud with their existing IT infrastructure, the lack of clarity and immaturity of the offers and the complex quantification of costs and benefits. This being said, the new Italian Digital Agency has issued some basic rules for the adoption of cloud services by the PA, but a wider and more detailed regulation is expected to be implemented by the end of 2013 within the framework of the Italian Government Digital Agenda. The Italian Data Protection Authority has also issued basic guidelines and suggestions on how to use cloud services respecting privacy principles (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906181).

Once guidelines and regulations become clearer and the market provides better examples of how best to integrate, we expect the adoption of cloud services to accelerate considerably. ■



General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   Partially. The agreement can be executed through a click-wrap method but some terms are only valid if accepted through handwritten signature or advanced electronic signature (firma elettronica digitale, firma elettronica qualificata, firma elettronica avanzata). In particular, certain types of clause considered burdensome for the contracting party need specific acceptance (i.e. an extra signature). Examples include limitations of liability, withdrawal clauses, automatic renewal clauses, faculty to suspend the effects of the contract, limitations to contractual freedom, choice of competent court. This applies to B2B contracts too. ■



Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes.
   According to Rome Convention and Rome I Regulation, the parties can choose the law regulating the agreement. They can also decide that different parts of the agreement are regulated by different laws.

   According to Bruxelles I Regulation, the parties (except in some specific cases) are free to choose the jurisdiction of disputes deriving from their agreement.

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   According to Rome I Regulation, a contract for the provision of services is governed by the law of the country where the service provider has its habitual residence, which means the place of the company's central administration.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   According to Rome I Regulation, B2C contracts are governed by the law of the country where the consumer has his habitual residence, provided that the professional:

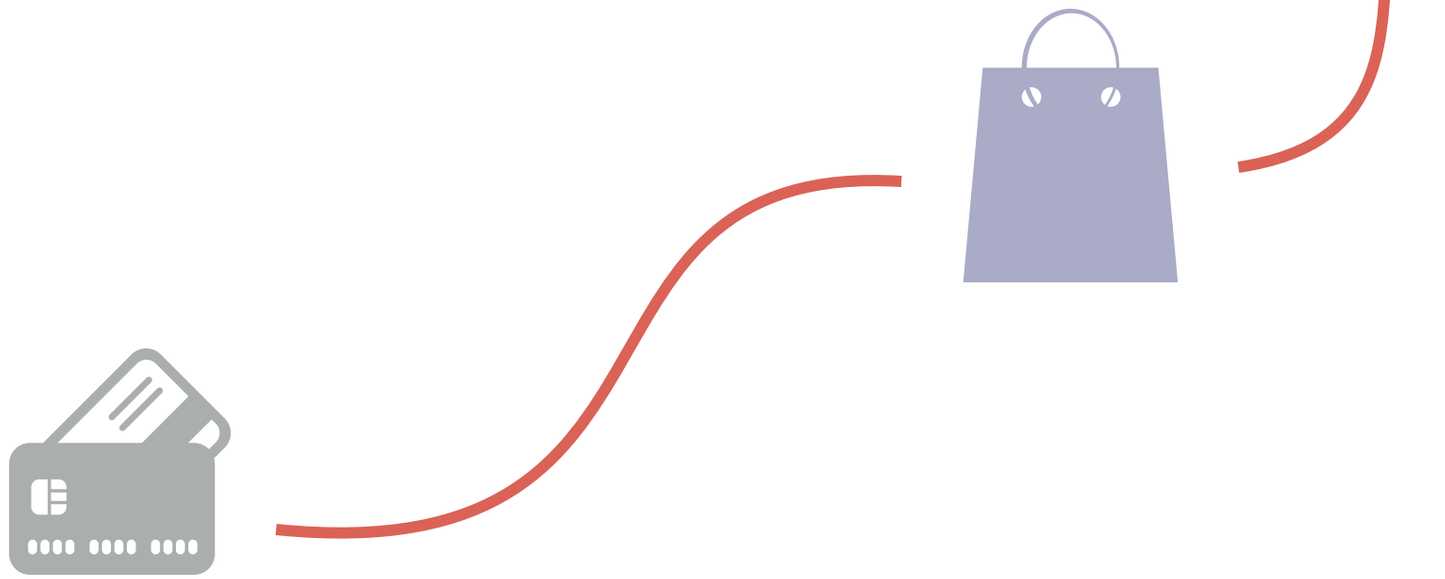
   - pursues its activities in that country; or
   - directs its activities to that country or several countries including that country

   The contract must fall within the scope of these activities.

4. Are there any other relevant issues related to applicable law and cloud computing?
   No. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?
   The rules of the Italian Consumer Code apply wherever cloud computing services are offered to persons acting for purposes outside their trade, craft, business or profession. These rules concern matters such as unfair commercial practices and unfair terms. ■



Data protection

1. Is the data protection law compatible with the EU Data Protection Directive on cloud computing issues?
   Italian data protection legislation transposed the principles of the EU Data Protection Directive. Even where the legislation is applicable to all kinds of processing, it is not specifically tailored to deal with cloud services.

2. Which law is applicable in the case of a dispute concerning data protection and cloud computing?
   The Italian data protection legislation applies if the controller is:

   - an Italian or EU company with a branch/ stable organisation in Italy;
   - a non-EU controller processing data through a branch/stable organisation in Italy;
   - a non EU controller using technical (e.g. cookies, servers) or physical means in Italy except where the equipment is used for transit only.

   Italian law does not apply to a subsidiary or separate legal entity that is not involved in the processing.

3. Who is the data controller in a cloud computing service?
   The controller is the person/entity that determines (sometimes jointly with another controller) the purposes, means and security measures of the processing. The Italian data protection authority (Garante) has issued guidance for the use of cloud computing services and the related risks. The Garante suggested that the user/client of the cloud service is the controller.

   The Garante does not give formal guidance where cloud services are used for household purposes. Since the user is subject to Italian data protection law (except in implementing security measures) unless he systematically discloses or disseminates data, it is likely that the controller is the cloud provider.

4. Who is the data processor in a cloud computing service?
   Guidance from the Garante (Italian Data Protection Authority) identifies the data processor as the cloud provider, provided this is the person/entity who processes data on behalf of the controller. ►

5. If the cloud provider is a data processor, what are its obligations under data protection law?
The processor must abide by the instructions given by the controller and carry out the processing operations in line with the tasks that the controller has assigned to the processor. Where the processor is in charge of taking appropriate security measures and the controller is subject to the Italian data protection law, the processor must implement the security measures it requires.

The controller usually delegates to the processor the implementation of the mandatory security measures to comply with Italian rules on system administrators.

6. Is there a requirement to notify end users about the use of cloud services?
No. However, users must be informed about details of processing of their data, including information about controllers or processors who may have access to their information and any data transferred outside the EU.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?
No.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?
Transfer of data outside the EU is subject to the general rules applying to any data transfer. Unless an alternative legitimate basis (e.g. consent of the data subjects, necessity to transfer data to execute contractual obligations, to comply with the Italian or European laws) applies, the transfer to countries without an adequate level of protection is allowed in case of:

- use of EU standard contractual clauses;
- agreement on Binding Corporate Rules;
- Safe Harbour certification in case of transfer to the US;

The controller cannot rely on exemption through legitimate interests, as this is subject to authorisation by the Garante.

The Garante advises controllers contracting with cloud service providers to take into account the location where data will be stored and the processing that will be carried out abroad. ►

9. Are cloud providers permitted to use sub-processors?

Sub-processing is subject to the discretion of the controller who is directly responsible for selection and supervision of the processors. The processor is not automatically entitled to sub-delegate processing of data. Where there is multi-level processing, the controller can:

- appoint each of the processors and sub-processors directly (even if there is no direct contractual relationship);
- give the processor a mandate to appoint the sub-processors specifying criteria for selection of the sub-processor.

The sub-processing agreement should mirror the obligations of the contract between the cloud provider and the controller.

10. What are the security requirements connected with processing data?

A data processor must take the minimum physical, technical and organisational security measures to minimise the risk of data being:

- destroyed or lost;
- accessed by unauthorised entities;
- processed unlawfully or in a way that is not compatible with the purposes for which it was collected;
- modified because of unauthorised or unlawful actions.

For instance, a client should make sure data remains available and accessible only to authorised persons. How data is stored and how it is transmitted are crucial.

Guidelines can be found in the Italian Data Protection Code and the mandatory provisions of the Garante (Italian Data Protection Authority) concerning technical and organisational security measures.

Periodical third party auditing and control of the processing carried out by the cloud providers is essential.

The following aspects of the Garante's recommended security measures are crucial:

- availability of data;
- portability of data;
- emergency and disaster recovery plans;
- appropriate training of the users and provider personnel. ▶

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?

Processing of judicial, sensitive (especially medical) data is subject to strict procedures and requirements (e.g. restrictions on the circumstances in which data can be processed, accessed and disclosed and security measures for the transfer of data). Financial data, even if not classed as sensitive according to the Italian Data Protection Code, is particularly sensible (e.g. secret and confidential information). The Garante advises the proper evaluation and selection of the data the controller puts on cloud, also based on more risky circumstances for some of them.

12. Is there existing or planned legislation relating to data protection and cloud computing that may be relevant?

There is draft legislation aimed to promote the development of digital services, including cloud computing. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   No. The Agency Digital Italy (former DigitPa) carries out public administration. The Agency has issued recommendations for a general framework for the use of cloud computing in public administration. http://www.digitpa.gov.it/sites/default/files/notizie/Raccomandazioni%20Cloud%20e%20PA%20-%202.0_0.pdf

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   No.

4. Are there applicable international standards relevant for cloud computing that are commonly used?
   We are not aware of any international standards.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   No.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   No. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?
   No. Agreements need to comply with regulations applicable to IT outsourcing. Any solution adopted must ensure that data is safely kept, remain under the control of the financial institutions and can be freely accessed by them at any time. Cloud computing must not jeopardise regulators' ability to carry out supervision; appropriate measures can be required depending the kind of data being processed. ■

Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   The right of sub-license has to be provided for within the agreement between the parties.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   Since the services offered can vary, there are no standard terms and conditions. Providers use different terms and conditions depending on the kind of services offered and their customers' circumstances.

3. Is it possible to use Open Source Software for cloud computing?
   Yes.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   No. General principles and civil and criminal sanctions connected with putting material protected by Intellectual Property Rights into the cloud without proper authorisation apply. With civil sanctions, where there are threats of or actual violation of an exploitation right on a work, it is possible to obtain a preliminary injunction to stop the violation.

   A party presenting reasonable evidence that his/her intellectual property rights have been infringed or are about to be infringed, can request the judge to:

   - order the exhibition or requests information to the counterpart;
   - order the counterpart to provide evidence to help identify persons and entities involved in the production and distribution of products and services infringing his/her rights.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   Not specific to cloud computing. According to general principles, infringers of Intellectual Property Rights may be subject to a fine or, in serious cases, imprisonment.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   Yes, in some cases.

   Cloud providers are generally not liable for third party contents hosted on their service provided either of the following applies: ▶

- they do not know about the illegal activity or infringing content;
- they delete (or disable access) to it without delay when they gain knowledge of it.

From a civil law perspective, the internet service provider may be deemed responsible if:

- it does not disable access to the content after a request from the judiciary authority or competent administrative authority, or
- it does not inform the competent authority having learned that the content is illicit or may damage third parties.

The service provider is not subject to general obligation to monitor information that it transmits or stores, or to actively seek evidence of illegal activities. The service provider is obliged to:

- promptly inform the judiciary authority or the competent administrative authority with surveillance duty, if it learns about illicit activities or information relating to its customer;
- promptly respond to a request from the competent authorities for any information useful in identifying its customer so that preventative measures can be taken.

The ISP may be subject to both civil and criminal consequences and sanctions.

7. Is there any notice-and-takedown procedure that can oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?

There is no notice-and-takedown procedure comparable with those in other jurisdictions. The judiciary authority or the competent administrative authority with surveillance duty (for example, the Authority for Guarantees in Communication, the Data Protection Authority, the Italian Competition Authority) can request, through provisional injunctions, that the hosting providers prevent or stop illicit activities.

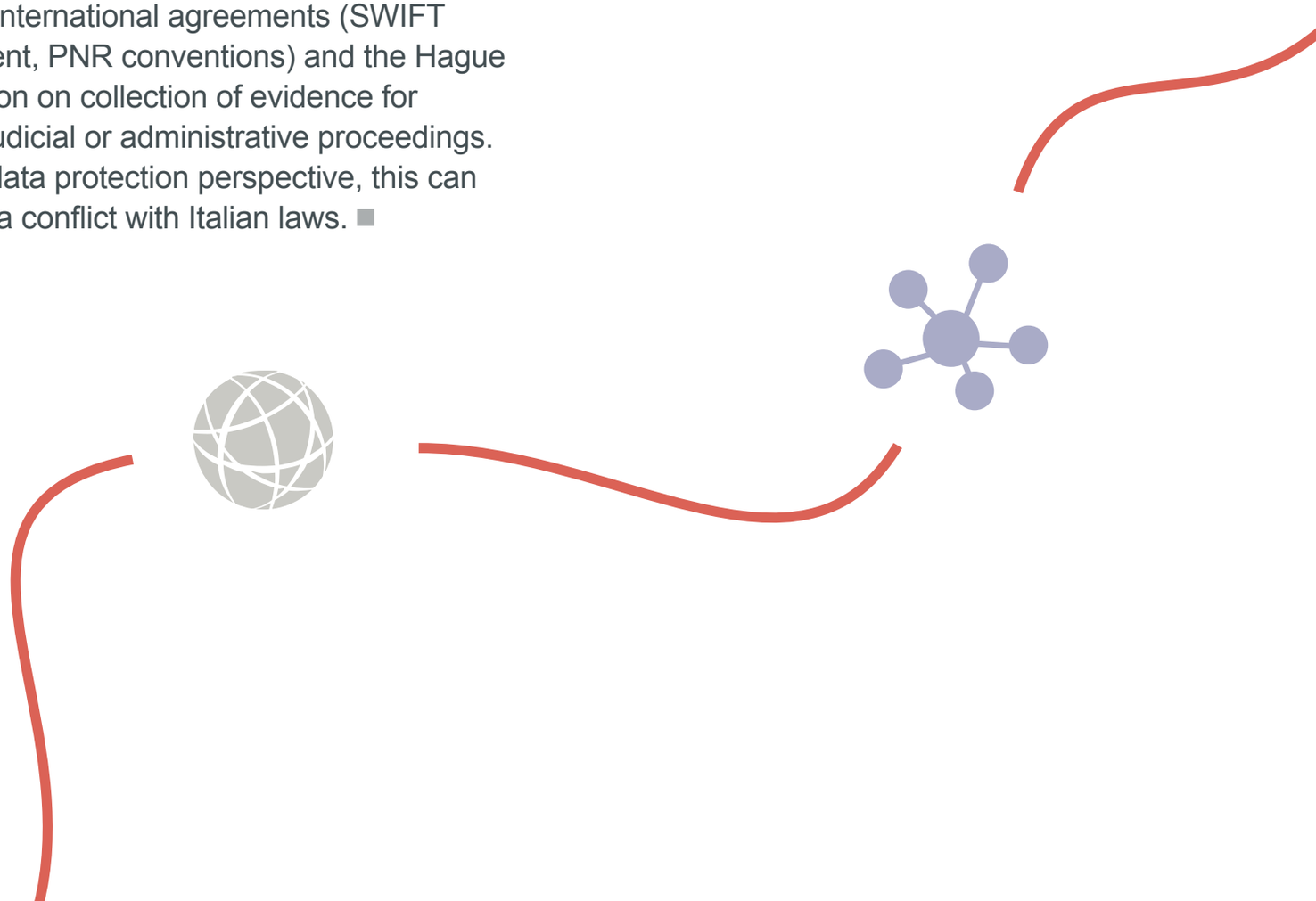
According to some decisions of the Italian courts, in case of notice of the party claiming for the infringement of its rights, the ISP can be deemed to be aware and therefore responsible for the infringement.

8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?

No. ■

International issues

1. Are there specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   No. Principles applicable to the disclosure of data in response to an enforcement action by a foreign authority are used to evaluate if and how data can be disclosed. Examples include existing international agreements (SWIFT Agreement, PNR conventions) and the Hague convention on collection of evidence for foreign judicial or administrative proceedings. From a data protection perspective, this can result in a conflict with Italian laws. ■



Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   This is normally regulated under the terms and conditions of the service where the agreement specifies the exact content of the obligations and the extent of the service provider's responsibility. The service provider tends to limit its liability as much as possible and to disclaim any liability in case of loss of data. If no limitation has been validly agreed, a cloud provider could face liability for damages (both direct and indirect) with no limitation.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   Limits to liability are not valid in the case of fraud or gross misconduct. Any limit to liability fixed under the standard terms and conditions of the provider are not valid unless approved by handwritten or advanced electronic signature by the customer.

   With consumers, the Italian Consumer Code states that all clauses that limit or exclude the rights of the consumers in the case on non-fulfilment or late fulfilment of its obligations are void.

   The controller remains liable for the loss of data unless it can prove that it has:

   - properly instructed the cloud provider to implement all measures to prevent the loss of data;
   - ensured adequate supervision of its activity.

   This can result in a civil liability for damages arising from the loss, administrative fines and criminal liability if the loss is the result of inadequate implementation of minimum security measures.

   The Garante recommends that controllers (especially small companies) have insurance to address potential liabilities for damages relating to loss of data or data breaches.

3. Are there any binding norms in context of warranties that may be relevant for cloud computing?
   Warranties for defects are subject to the rules of the Italian Civil Code relating to service agreements. ▶

For B2B, the issue can be regulated by the contracting parties. If the contract is regulated by Italian law, it may need an additional signature for the relevant clause.

For B2C contracts, provisions limiting the rights of consumers relating to warranty for defects can be considered void.

Under the Italian Data Protection Code the liability for unlawful processing or loss of data is an automatic liability. The offender is liable for pecuniary and moral damages unless it can prove it has implemented all necessary security measures to prevent unlawful processing (i.e. the offender is liable, except in case of an Act of God). The Garante advises choosing providers who guarantee appropriate warranties.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?

This is no different to the insolvency/ bankruptcy of any other entity. The court appoints a bankruptcy administrator who decides whether to continue or terminate the contract. In practice, there is a risk of data being inaccessible or the obligation arising from the contract not being fulfilled. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   If intellectual property rights are applicable to data, the entity creating the data and putting them in the cloud is the owner. These issues should be regulated within the agreement with the service provider. Data (as copyright work) created by an employee executing employment activities belongs to the employer.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud? Who is the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   Modifying the data with tools available in the cloud (e.g. formatting the data) should not imply any change in the property of the data provided that the changes do not substantially modify the work or add a creative contribution. It is important to evaluate the extent of the changes from a quantity and quality point of view. From a contractual point of view, it is important to regulate the issue within the terms and conditions of the services in order to avoid possible dispute on the property of the final work. ■

Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes public bodies in Italy are actively looking at cloud solutions. A Government body, the Italian Digital Agency, is promoting surveys and guidelines on cloud computing and its adoption by public entities. This includes participation in the EU Cloud Partnership. The agency has completed a series of public surveys on cloud adoption principles and safety measures and is monitoring the implementation of specific cloud public adoption projects. Some local entities and authorities have already implemented cloud systems within their IT infrastructure and service to the public.

2. Is there any kind of government cloud operating? Do you know if any public institution is operating using cloud computing services?
   There is no government cloud in Italy but many local authorities have already adopted cloud solutions.

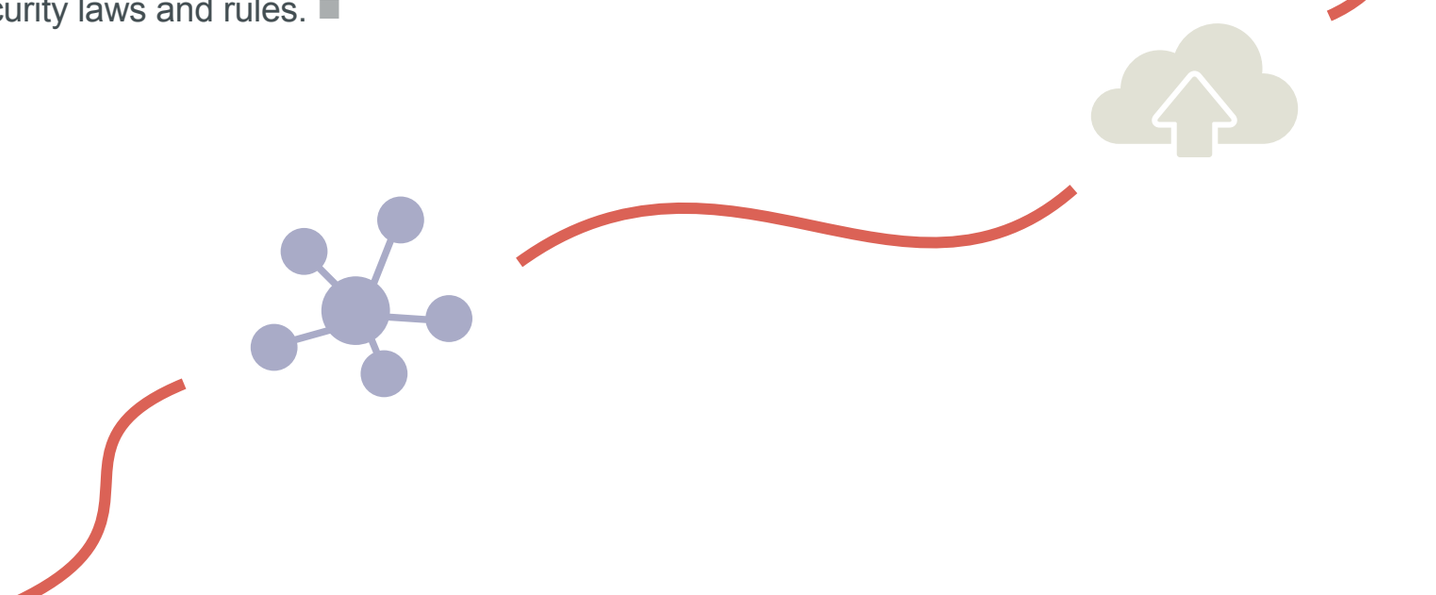
3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   Yes. The Italian Digital Agency issued a series of best practice guides on public entities' adoption of cloud computing solutions. The Italian Data Protection Authority also issued a document on cloud computing and privacy.

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   Yes, see points 2 and 3 above on Public Sector and cloud.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
   The Italian Digital Agency issued public consultations on cloud in various economic and business sectors, and maintains a best practice monitoring service for public IT procurement and adoption solutions. The health sector is under close study – the benefit of cloud technologies is perceived as having potential to reduce the high public spending in this area. ►

6. Who is or would be the responsible regulator for cloud services?
There is no cloud services regulator. The Italian Digital Agency is considered as a reference agency for public entities in all IT matters. The Data Protection Authority is the authority with sanctioning powers on privacy matters. Both areas are indirectly relevant to cloud computing.

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
No. General principles concerning state secrets and national security matters apply to cloud services. Various public authorities, the police, the military and Italian courts have the right to order access, seizure and destruction of data in case of breach of applicable safety/security laws and rules. ■



Security issues

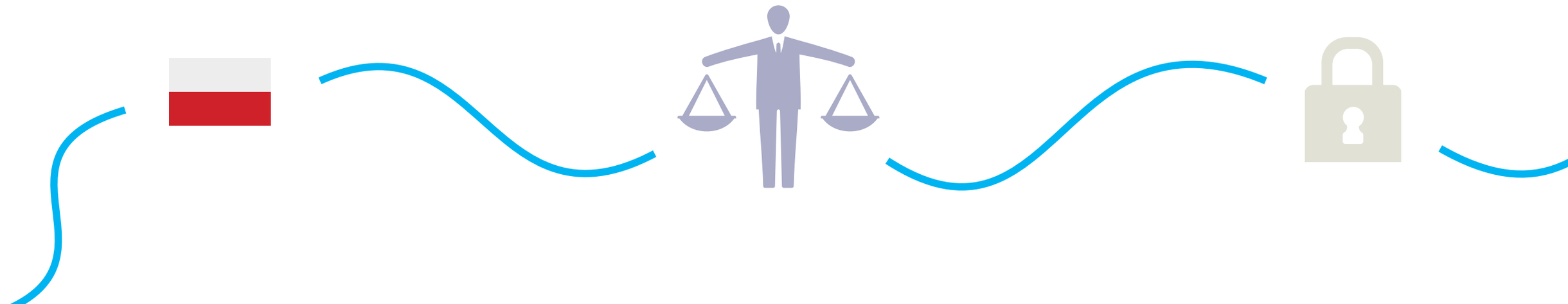
1. Are cloud services providers free from content filtration or censorship obligations?
   Cloud service providers who do not have any influence on data collection and review can find protection under the hosting umbrella principle of the E-commerce directive. Separate rules apply to broadcasting.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   No obligatory law exists although minimum security requirements for data treatment and conservation are provided for under the Italian Data Protection Code and must be applied by cloud providers to their customer's data if their users, as controllers of the data, are subject to the Italian Data Protection law. ■

Poland

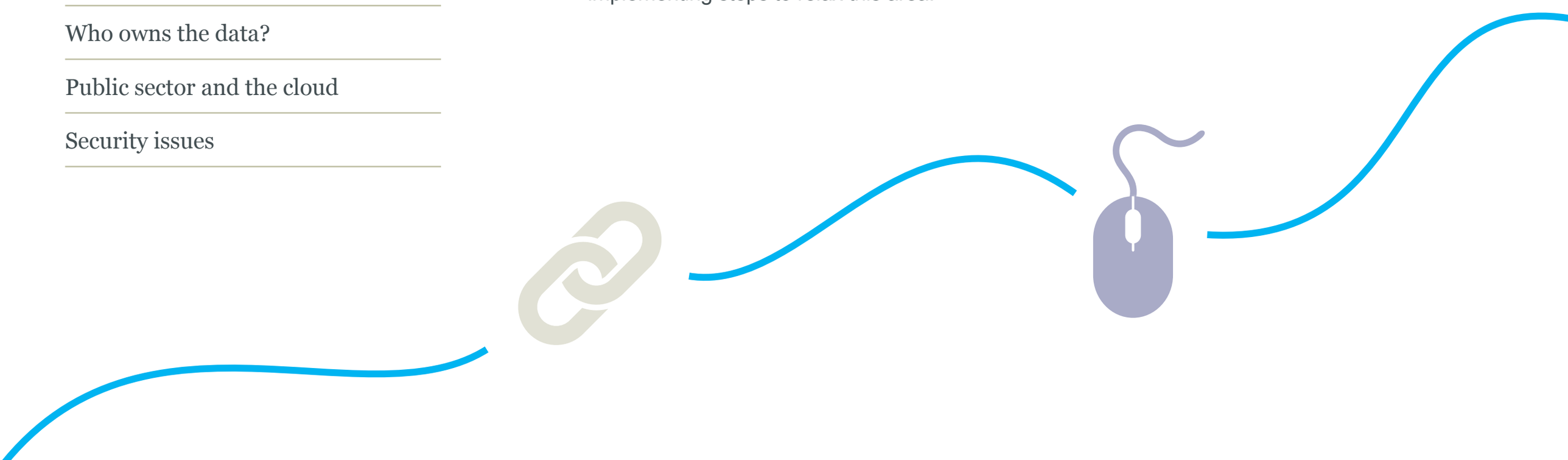
Forecasts for cloud computing in Poland in 2013 are optimistic. According to the IDC the estimated value of the Polish cloud computing market (both private and public) is more than USD 36m. Cloud computing is the most dynamically growing part of the Polish ICT market with a predicted annual growth ratio of 33% by 2015 (which we believe could be an underestimation).

There have been several new cloud developments recently: in particular OKTAWAVE which is growing domestically and internationally. The public sector is also looking at the cloud with growing interest and the Polish Data Protection Authority (GIODO) has been supportive of cloud computing given its positive impact on business. Cloud computing has also become attractive to the financial sector: the new Recommendation D of the Polish Financial Supervision Authority concerning IT and security mentions cloud computing in the context of processing critical data, which seems a strong positive message to the market. ■



General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   Yes. Some agreements or declarations of will (e.g. a data processing agreement or consent to transfer data to a third country not ensuring adequate protection) require a written form either as a hard copy or document with an e-signature with qualified certificate. The latter is not operational and is rarely used in practice so written form cannot be concluded or made electronically. The Ministry of Administration and Digitalisation is implementing steps to relax this area. ■



Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes. The Rome I Regulation and the Brussels I Regulation apply. In B2B, a free contractual choice of law and jurisdiction is possible. In B2C, the choice of law must not deprive the consumer of certain mandatory rights of the consumer's habitual residence (i.e. the consumer law applies regardless of the choice of law). The choice of jurisdiction must not deprive the consumer of the right to bring a case before a court in his/her domicile (such a clause is considered abusive and invalid).

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   According to Rome I Regulation, a contract for the provision of services is governed by the law of the country where the service provider has its habitual residence or central administration. This will generally be the law of the registered office of the cloud provider. There is no clear authority regarding the applicable law for claims resulting out of torts committed over the internet. This will depend on the facts of the case. If a tort is closely connected to an (internet) contract, a court will possibly apply the applicable law for the contract. However, there is also a chance that a court will apply the law of the jurisdiction where the alleged damage was suffered.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   If the consumer service is addressed to a particular jurisdiction, the law of that jurisdiction applies. Depending on the circumstances, it may be similar to a B2B litigation or it may be that the applicable law is the law of the country in which the consumer has a habitual residence. The Rome Convention and Rome I provide that it is not possible to contract out certain protection provisions of the law of the country in which the consumer has a habitual residence.

4. Are there any other relevant issues related to applicable law and cloud computing?
   The nature of cloud computing may encourage cloud providers to do a forum shopping. This means the providers are likely to choose the law or jurisdiction that will offer them the most advantageous substantial procedural law and case law. ■

Consumer protection

1 Are there any consumer protection issues that may be relevant for cloud computing services?

In Poland consumer protection laws apply to the use of cloud computing services in the same way as other services.

Polish consumer protection legislation does not specifically target cloud computing. It is very strict, especially on:

- clauses in agreements or terms & conditions that may be considered abusive (e.g. limitation of liability);
- scope of information that should be provided to consumers;
- the form of documents in B2C relations (e.g. information should be provided to the consumer on paper or consent should be obtained in hard copy).

The issue of conducting business over the internet was considered by the Polish Ministry of Administration and Digitalisation. Their report, prepared in co-operation with experts (including Bird & Bird) and stakeholders indentified the following as the main barriers for conducting business over the internet:

- overregulated internet market;
- restrictions on free flow of information;
- lack of clarity of the internet law and problems with interpretation;
- out of proportion penalisation of some internet activities;
- lack of some legal solutions.

Furthermore, a cloud computing offer addressed to Polish consumers may have a problem with the “Big Bang of the Register of Abusive Clauses”. In Poland the B2C sector faces a serious problem of erupting register of abusive clauses. Currently there are 4095 of registered abusive clauses and this number is growing by almost 100 per month. ►

In Poland only the Court of Competition and Consumer Protection can recognise a specific clause as abusive - but after a specific clause is recognised as abusive - each common court applies that decision in an individual case. Any consumer business can be sued for its terms and conditions by any association or other non-profit organisation established to protect consumer rights. Thanks to this ease to sue a new legal business model has evolved. Lawyers inspire or set up different associations and then those associations sue business for each clause separately.

Because of the above the register of abusive clauses becomes virtually useless as it contains far too many different clauses (many of them considered legitimate outside of Poland), still or even more constituting a threat to consumer businesses. ■

Data protection

1. Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?
   The Polish Personal Data Protection Act (PDPA) implements the EU Data Protection Directive 95/46/EC. The PDPA is mostly compliant with the Directive and in some cases provides higher standards.

   The PDPA is not adjusted to the electronic environment (e.g. it requires an individual's hard copy consent signed by hand to transfer data outside the EEA and a hard copy data processing agreement signed by hand).

2. Which law is applicable in the case of a dispute concerning data protection and cloud computing?
   The PDPA applies to:

   - entities with their registered office in Poland;
   - entities conducting permanent and separate operations in Poland (e.g. a branch);
   - entities with their registered office outside the EEA, but using technical means located in Poland to process personal data. This includes:
     - the data controller's servers in the EEA;
     - the technical means of a data processor within the EEA to whom the data controller outside the EEA outsourced the processing of personal data;
   - cookie text files placed on a data terminal of a user located in Poland (e.g. on a computer, tablet or smart phone) in order to store personal data.

3. Who is the data controller in a cloud computing service?
   The data controller is a person/entity that determines the purpose and manner in which any data is processed. Whether this is the cloud services user or the cloud services provider depends on the particularities of an individual case (i.e. the actual level of control parties have over the data). In Poland, the user is normally seen as the controller.

4. Who is the data processor in a cloud computing service?
   The data processor is the person/entity that processes data on behalf of the data controller. In contrast to the data controller, the data processor only has to comply with security obligations and not with other data protection obligations under the Data Protection Directive.

5. If the cloud provider is a data processor, what are its obligations under data protection law?

The processor is obliged to take appropriate technical and organisational security measures. The applicable technical and organisational security measures are determined by either the data protection law of the country of the processor's registered office, if the processor is located in the EEA or the Polish data protection regulations, if the processor is located outside the EEA. Polish regulations are among the few in the EEA that describe in such detail the mandatory appropriate technical and organisational safeguards that should be applied to adequately protect personal data.

The data controller is obliged to conclude a data processing agreement with the data processor that specifies at least the scope and purpose of entrusting the data to the processor. The agreement should be in writing (a hard copy signed by hand by both parties). If the hard copy of the agreement is not signed, the agreement is still valid but the personal data security rules are breached.

6. Is there a requirement to notify end users about the use of cloud services?

No. The end-user/data subject does not need to be notified about the use of cloud services.

The data controller (cloud user) must provide certain information in accordance with the PDPA regardless of how the personal data is processed. This includes information on the purpose of the processing, what personal data is processed and whether the data may be disclosed to a third party.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?

No.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?

Yes. It is possible to send data outside the EU/EEA without special requirements, where:

- the destination country has been pre-approved as having adequate data protection laws and standards;
- the data importer is self certified in Safe Harbour, in case of a transfer to the US;
- some limited exceptions apply. ►

In other cases, the DPA's (the Polish Inspector General for the Protection of Personal Data or GIODO) consent is needed before data is exported. The data exporter needs to prove to the GIODO that the data importer will apply adequate safeguards to the exported data. Standard contractual clauses or binding corporate rules are used most often to prove whether the safeguards are adequate.

9. Are cloud providers permitted to use sub-processors?

Yes. Cloud providers are permitted to use sub-processors, although the PDPA does not provide for this explicitly.

According to the GIODO, sub-processing is compliant with the PDPA where the agreement between the data controller and the data processor contains an explicit authorisation to entrust personal data to the sub-processor. The authorisation should contain the sub-processor details (name and address). It should meet the same requirements as the agreement with processors (i.e. it should be in writing, and indicate the purpose and the scope of data processing).

10. What are the security requirements connected with processing data?

The data controller and data processor with registered offices in Poland need to implement adequate security measures that cover the minimum standard of applicable technical and organisational measures described in the PDPA and the Ordinance on the personal data processing documentation, and technical and organisational conditions which should be fulfilled by devices and computer systems used for personal data processing. All cloud providers and cloud users need to apply a high level of security (security level required when the IT system of the controller and processor is connected to the internet).

This comprises, in particular, logical and physical access control, disclosure control, input control, job/order control and availability control.

The Polish data controller and the Polish data processor should implement and adopt a hard copy security policy signed by hand and an IT system management instruction, as well as keeping records of IT system users. These documents should include: ►

- places in which the data are processed (i.e. physical places in which the processing of personal data takes place),
- functionality of the IT system (e.g. whether the system ensures the recording of who enters data into the system and when, to whom they are disclosed and when).

There are no specific security requirements for cloud computing. Data controllers are obliged to control their data processors. It is subject to debate how this can be achieved in cloud computing – one option is an audit/control by a qualified third party.

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?

Special rules apply to transfers of sensitive data from one controller to another controller. This is understood under the PDPA as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued in court or administrative proceedings.

Such special rules would be relevant for cloud computing where the cloud provider becomes a data controller of the entrusted data. They would require a special justification for a transfer and processing of sensitive data by the cloud provider, like a data subject's written consent.

Financial information is often subject to professional secrecy (e.g. banking secrecy; secrecy under the Payments Services Act) that prohibits disclosure of financial information unless certain requirements are met, (e.g. the client gave written consent or information is disclosed to an outsourcee that meets the relevant outsourcing obligations).

There is also an issue over the prohibition of limited liability of the service provider towards the bank for client damage as a result of a non-performance or improper performance of the outsourcing agreement.

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?

There is no specific data protection legislation existing or planned for cloud computing. The existing general data protection law applies, i.e. the PDPA and the Ordinance. The Act on Providing Services via Electronic Means ▶

(implementation of the E-commerce Directive) covers special rules on processing personal data when providing electronic services (information society services in the meaning of the E-commerce Directive).

The following planned legislation is likely to be relevant for cloud computing:

- The review of the data protection regulations: in early 2012 the GIODO announced that it is likely that the PDPA and the Ordinance is scheduled to be revised in early 2013 in terms of the requirement for mandatory security rules and abolishing the hard copy consent and agreement signed by hand.
- The EU General Data Protection Regulation (which is not particular to Poland, but to all of Europe) is expected to come into force in 2016 at the earliest. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   Officially there is no public institution responsible for standardisation. However, in 2011 the Ministry of Administration and Digitalisation was established. It is likely that the Ministry, officially or unofficially, will influence the standardisation.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   No.

4. Are there applicable international standards relevant for cloud computing that are commonly used?
   No.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   Some cloud providers have developed their own standard service level arrangements, there is nothing used centrally.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   Yes. Recommendation D 2013 on IT by the Polish Financial Services Authority requires that banks wishing to use cloud services ensure data portability contractually. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?

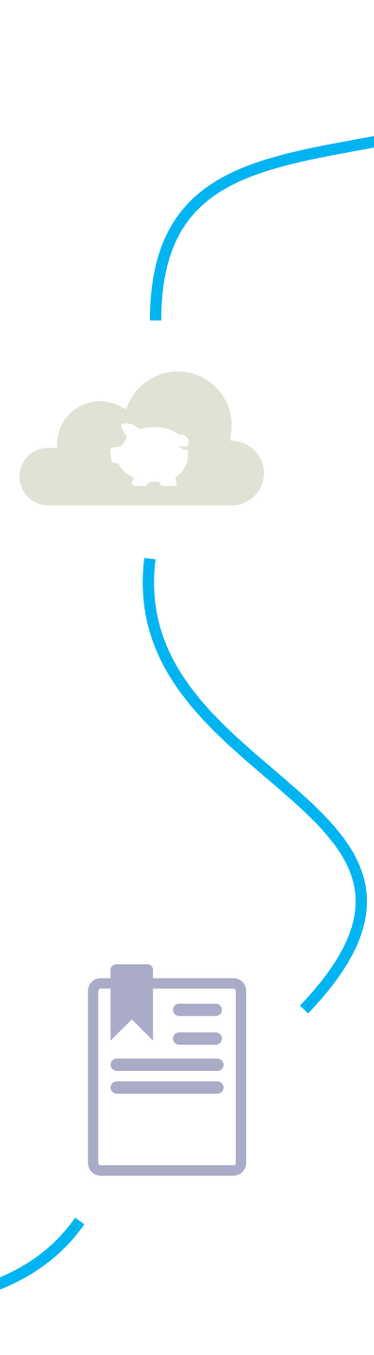
In principle, regulations concerning the financial sector focus on operations or processes critical to the organisation, leaving non-critical operations outside the area regulated by administrative law (i.e. within the domain of civil law and the freedom of contract principle).

The main problem in the financial sector is the prohibition of limited liability of the service provider towards the bank for client damage as a result of a non-performance or improper performance of the outsourcing agreement – according to the Banking Law. An identical regulation is established in the Payments Services Act or Financial Instruments Act. These provisions present a serious barrier to developing cloud computing in the financial sector (incorporating new business models, such as mobile payments). The prohibited limited liability is Poland specific.

On the 9 January 2013 The Polish Financial Supervision Authority issued a Recommendation D concerning managing areas of information technology and the security of information and communication environment in banks. The new Recommendation D supersedes the previous Recommendation D of 2002. The new Recommendation D contains 22 large points and around 200 small points, not including bullets, so it is reasonably detailed. The Recommendation D addresses inter alia cloud computing. The Recommendation D refers to the NIST definition of cloud computing and requires banks to implement additional security measures such as encryption when using cloud computing to process sensitive information (e.g. information protected by banking secrecy).

The Polish Bank Association has issued two reports on cloud computing. The first regulatory report was prepared by the Bird & Bird Polish Office and issued in 2011. Polish and English versions of the Cloud Computing Regulatory Report 2011 are available via the ►

Polish Bank Association's website (http://www.zbp.pl). In 2013 the Polish Bank Association issued another comprehensive cloud computing report, which included a legal chapter written by head of Bird & Bird Poland, Maciej Gawronski. This report is also available in Polish at http://www.zbp.pl). The Polish Insurance Chamber issued another 2013 report on cloud computing, focusing mainly on contractual aspects of cloud computing in B2B relations. Those publications constitute another source of knowledge regarding cloud computing in the Polish financial sector. ■



Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes. It is possible to sub-license the software for the customer by the cloud provider, provided that the licence is sub-licensable. Another issue is whether the customer actually needs a sub-licence. This may depend on the technical infrastructure and the provider's licence.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   No.

3. Is it possible to use Open Source Software for cloud computing?
   Yes.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   Yes. The civil sanctions depend on whether or not the cloud user was authorised to use the materials protected by Intellectual Property Rights. If not, the user may be liable for a breach of intellectual protection rights, in particular copyrights under the Copyright and Related Rights Act and the Industrial Property Law. The infringer may be liable to cessation of the infringement, remedy the situation, damages or compensation.

   There is no separate body of intellectual property law relating to cloud computing.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   Yes. There are criminal sanctions for unauthorised use of copyright protected materials and counterfeiting registered trademark, that may be committed by putting material protected by Intellectual Property Rights into the cloud. The Copyright and Related Rights Act and the Industrial Property Law apply respectively.

   There is no separate body of intellectual property law relating to cloud computing.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   Cloud service providers can be held liable for infringing material placed in the cloud by its users when the cloud service provider knows or has reason to believe that the material in question is infringing. In that case the ▶

exceptions regarding limitation of liability of host providers under the Act on Providing Services via Electronic Means does not apply. If the service is not only pure host providing, but the cloud provider also takes advantage of the stored data (e.g. by generating advertising revenue), there is a risk that the liability privilege does not apply.

According to the Act on Providing Services via Electronic Means, the data host is liable if, when receiving reliable information about the infringing character of the materials, it does not block it immediately.

Possible sanctions include cease-and-desist orders, injunctions, damages and criminal liability in serious cases.

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?
Yes. In the case of receiving reliable information about the infringing character of the materials, the cloud service providers should block it immediately. The cloud service provider is not liable for the damage caused by blocking of such materials to the user.

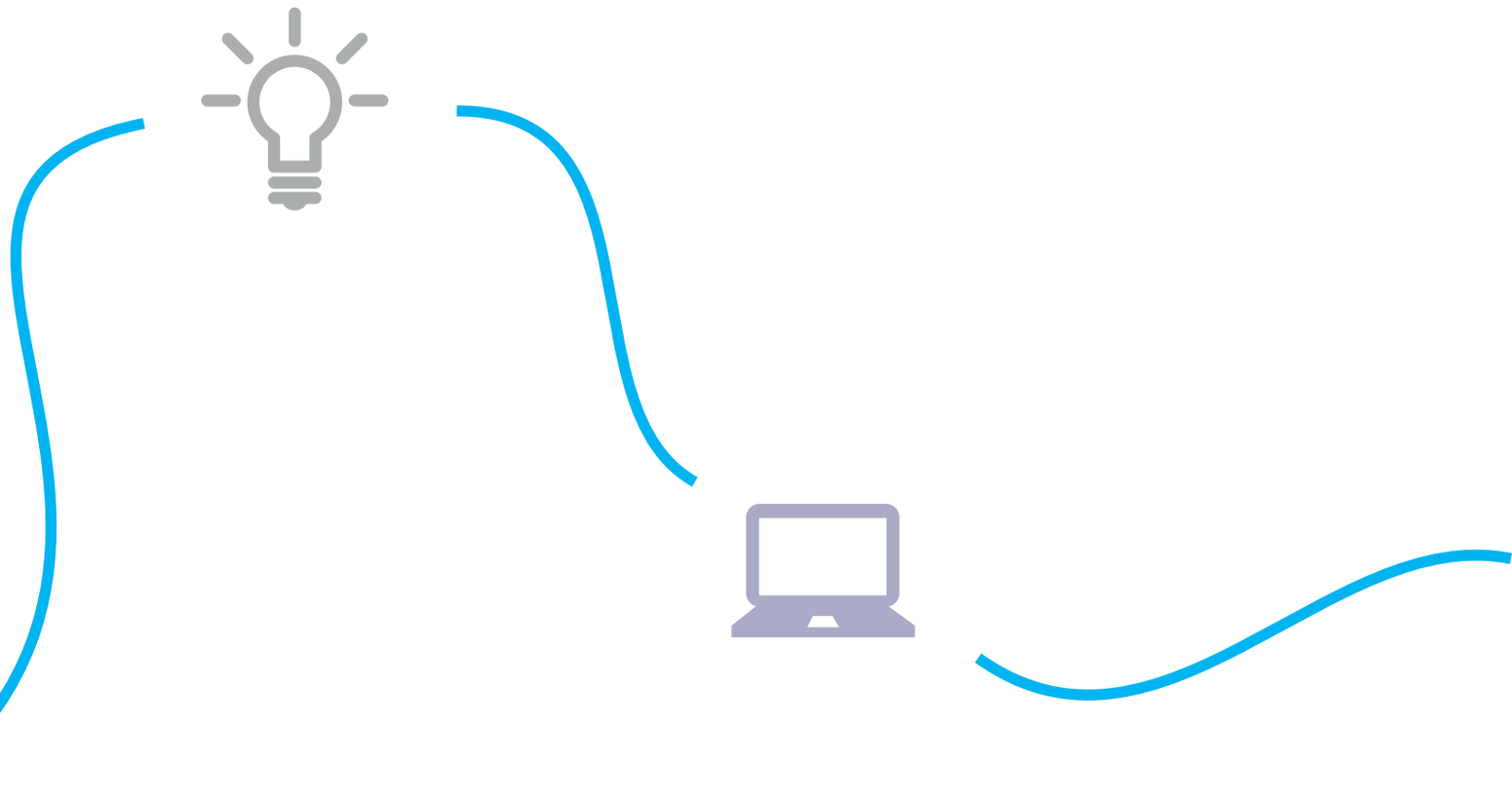
The cloud service provider is not obliged to inform any authorities about the infringing act of the end user. The Polish Government published a draft amendment to the Act on Providing Services via Electronic Means that provides for a three-step notice-and-takedown procedure. The amendment has not been sent to the Parliament yet so it is difficult to predict when it will come into force, especially taking into consideration the controversies it generated.

8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?
In B2C relations it is important that all Intellectual Property Rights can only be transferred based on a hard copy document signed by hand.

There a discussion about the possibility of granting a perpetual copyright licence, in which Bird & Bird Poland is taking part. According to the Copyright and Related Rights Act, unless stated otherwise in the licence, the licence can be granted for up to 5 years. If a licence is granted for longer, after 5 years it is deemed concluded for an indefinite period of time, and can be terminated by the termination notice as ▶

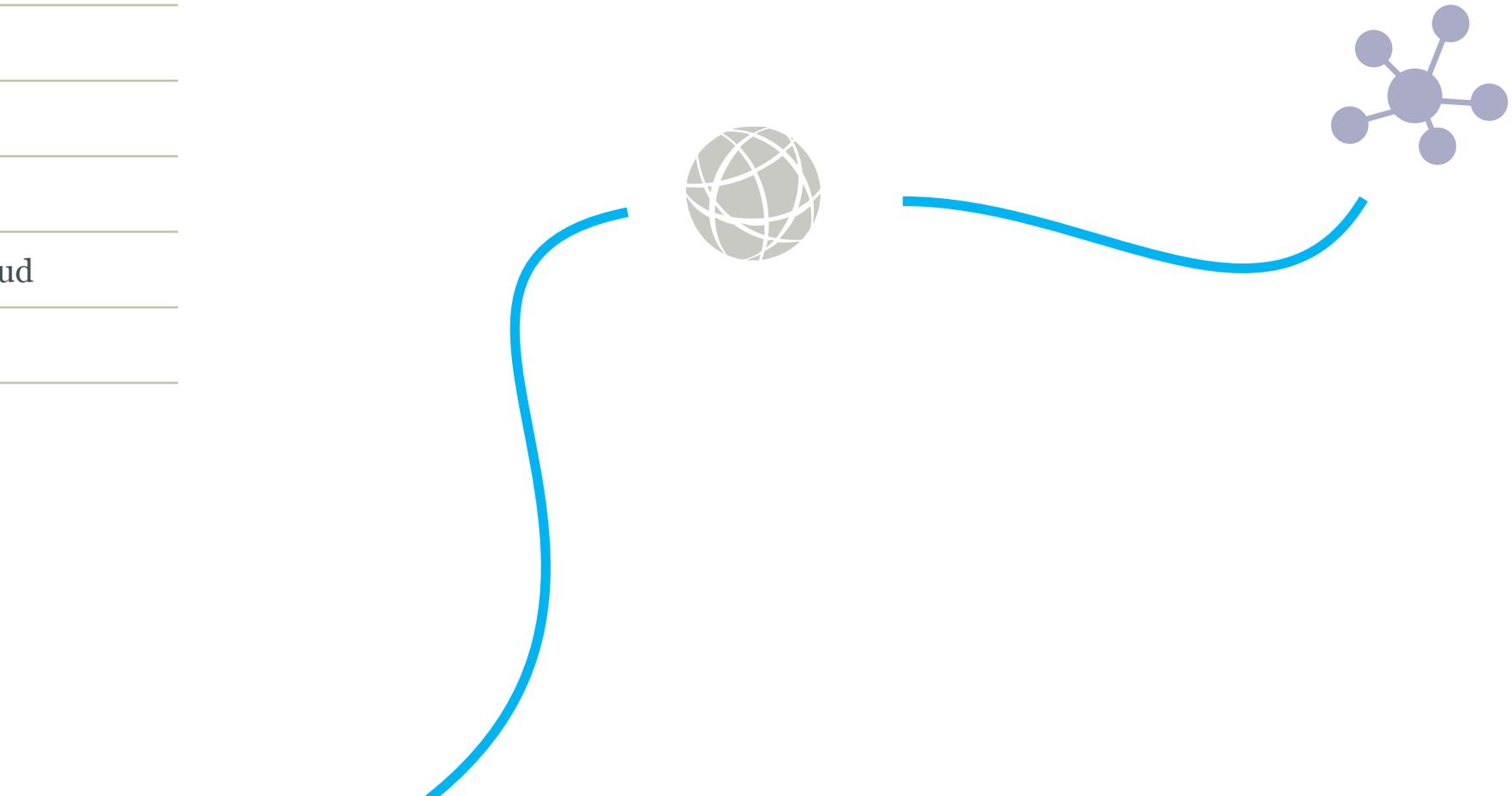
defined in the licence. If the termination notice is not defined, it is deemed concluded with a one year termination notice (counted from the end of the year).

Although cloud computing contracts relate to the provision of services rather than to the supply of software to customers, appropriate software licences may still need to be granted to customers to enable them to legally and correctly use the necessary software without the risk of a copyright infringement. ■



International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   We are not aware of any such specific provisions. ■



Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   The PDPA applies to liability for data loss. Under the PDPA, the data controller has administrative and civil liability for loss of data and its employees and management can have criminal liability. The service provider (data processor) has administrative liability in the case of a security measure breach resulting in data loss and its employees and management can have criminal liability. Where service providers are located in Poland, they are liable for ensuring back-up solutions relating to personal data. In addition, the service provider can be liable on a contractual basis.

   Without a specific arrangement, the cloud provider is liable for any damage arising from negligence.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   Yes. In general the provider cannot exclude the liability for wilful and intentional actions or inactions.

   In the case of outsourcing in regulated sectors (e.g. banking, payment service), Polish law often does not permit the provider of the critical service to restrict its liability. Limiting liability in B2C is disregarded and treated as ineffective. It could also be treated as an abuse of common consumers' interest and result in administrative fines. The Polish implementation of the Payment Services Directive (the Payment Services Act) allows for limiting liability of providers of IT services and solutions serving payment services, thus creating a disproportion between requirements imposed on the banking sector (where the Polish Banking Law prevails) and requirements applying to other participants of the payment services market. ►

3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   Yes. If the warranty is granted to the consumer, it should be free of charge. It is important in the context of B2C cloud computing services.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   This is no different to the insolvency/bankruptcy of any other entity under Polish law. From a practical point of view, bankruptcy of a cloud provider may bring material risks to the data availability and the service continuity. In relation to B2B, the Polish cloud service provider and its management could be held liable in case of a data loss and no back-up solution. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   There is no concept of ownership of data in Polish law. Different types of rights will be applicable as:

   - confidential business information,
   - data protection,
   - Intellectual Property Rights. If Intellectual Property Rights (e.g. copyright) apply to the data, there will be a person who has these rights.

   In all cases, the ownership will also be determined by the contract between the cloud provider and the user. Usually, the cloud provider asks for as limited rights as possible while still being able to provide the service in the cloud contract offer.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud)? Who is also the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   This depends on the licence under which the data was placed in the cloud service and the type of modification. As a rule, the right of access to information will decide. In our opinion, independently of the sequential format of data, the owner of the data is the person who placed the data in the cloud. ■

Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes. Representatives of public institutions look at cloud computing services. Although some use cloud computing services in their IT departments, cloud computing is still behind-the-scenes knowledge. There is no official Government opinion. The Polish Parliament uses the term iCloud.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
   According to our knowledge there is no official existing or even planned 'Government Cloud' operating but there are some public institutions (like National Bank of Poland) that are using cloud services. We do not know the scale of this operation. From the practical view, different Ministries use cloud services (as Google groups, wiki, iCloud, Sharepoint) for various types of their group work.

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   No.

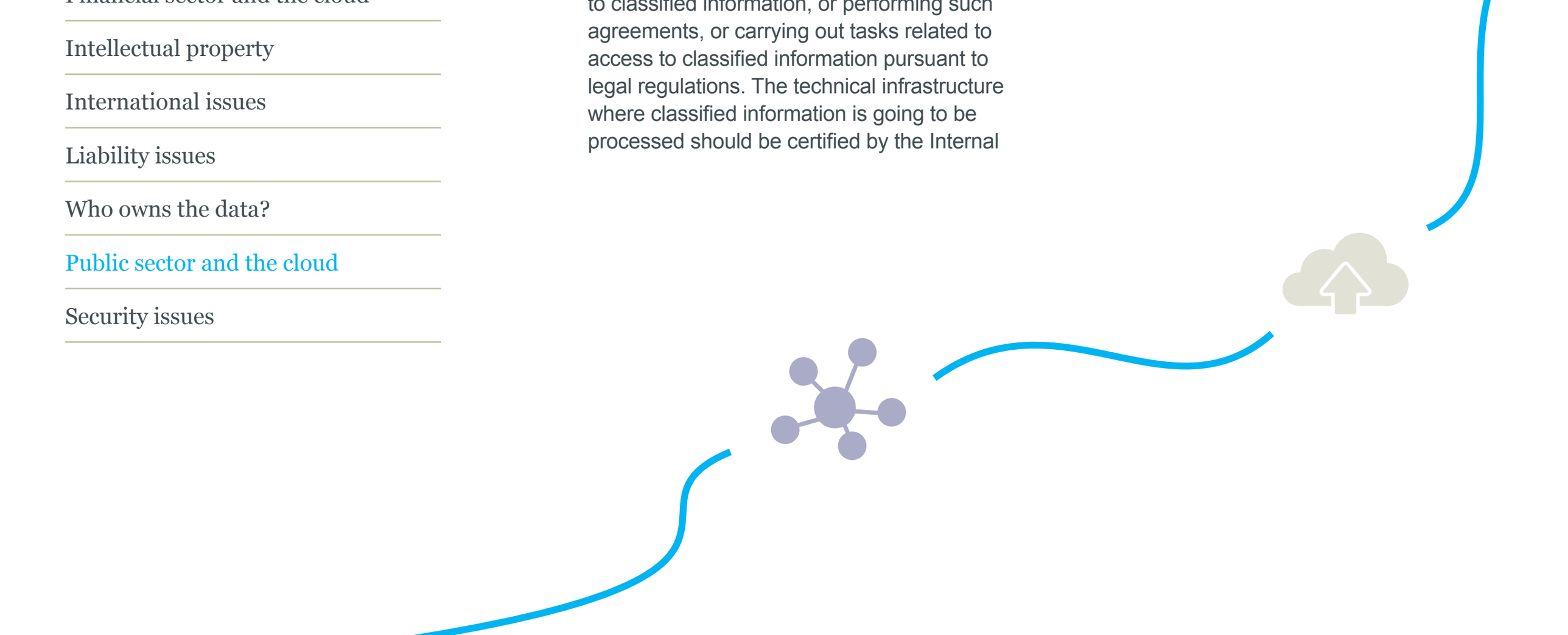
4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   No. However, the Forum of Bank Technology of the Polish Banks Association (a non-governmental and well reputed organisation of which Bird & Bird Poland is a member) created a cloud computing group. The main purpose of this group was to prepare a report on the application of cloud computing in the global and Polish banking sector. This report described the phenomenon of cloud computing, a model of cloud processing, legal aspects, possibilities of cloud applications, barriers and restrictions as well as benefits. The legal part of the report was prepared by Bird & Bird Poland and is available online http://www.zbp.pl/site.php?s=MjIzODYxMA.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
   No.

6. Who is or would be the responsible regulator for cloud services?
   The GIODO and the Polish Financial Supervision Authority are the only regulators currently publishing comments on cloud computing. ▶

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?

The Act on Protection of Secret Information specifies the basic rules for protecting classified information. From the cloud computing point of view, it is relevant that the Act applies to undertakings intending to pursue or pursuing agreements on access to classified information, or performing such agreements, or carrying out tasks related to access to classified information pursuant to legal regulations. The technical infrastructure where classified information is going to be processed should be certified by the Internal Security Agency. The service provider of the cloud, in which this kind of information will be stored, may also be controlled by Polish state security agencies such as the Supreme Audit Office, the Internal Security Agency and the Military Counterintelligence Service. ■



Security issues

1. Are cloud services providers free from content filtration or censorship obligations?
   As there is no mandatory/general filtering or censorship of content, cloud service providers are not subject to any such obligation.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   Please see the data protection section and sector regulation. There are no generic regulations in relation to data more generally. ■

Spain

In Spain, the use of cloud computing is rapidly increasing among private businesses and public administrations. Recent studies state that the use of cloud computing in Spain increased 93% in 2012. Cloud computing has also grown in the public sector where it is used by 33% of public bodies. The move to the 'cloud' is due to cost savings and the efficient use of IT capabilities it provides by simplifying resources.

On the legal side, although a multiplicity of approaches and models are emerging and it is difficult to generalise, cloud contracts still remain at an early stage and, except in large deals, are rarely negotiated (provider's standard terms and conditions are generally set to be accepted or rejected as a whole). There are some first attempts of users to try to make the terms more suitable to their requirements – with cloud integrators playing a key role – but there is still a long way to go. From a regulatory perspective, the most challenging aspect of the cloud relates to the data protection legislation, of which the requirements in respect of security, sub-contracting and international transfers do not seem to fit the reality of the cloud. Although the Spanish Data Protection Agency (AEPD) and public bodies such as INTECO (The National Institute of Communication Technologies) are making efforts to provide guidance and solutions to the legal challenges of the cloud, the truth is that there is still a long road ahead until cloud adoption can be said to be driven by legal certainty. ■

General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   Yes. The formation of contracts is traditionally based on consent and does not require any specific form. It is enough for end-users to tick an "I have read and agree the Terms of Use" box. ■

Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes. The Rome I Regulation and the Brussels I Regulation apply. In B2B contracts a free contractual choice of law and jurisdiction is possible. In B2C contracts the choice of law must not deprive the consumer of certain mandatory rights of the consumer's habitual residence (i.e. the consumer mandatory law applies regardless of the choice of law). The choice of jurisdiction must not deprive the consumer of the right to bring a case before a court of the consumer's domicile (a clause that would deprive a consumer of that right is considered abusive and invalid).

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   According to Rome I, a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence.

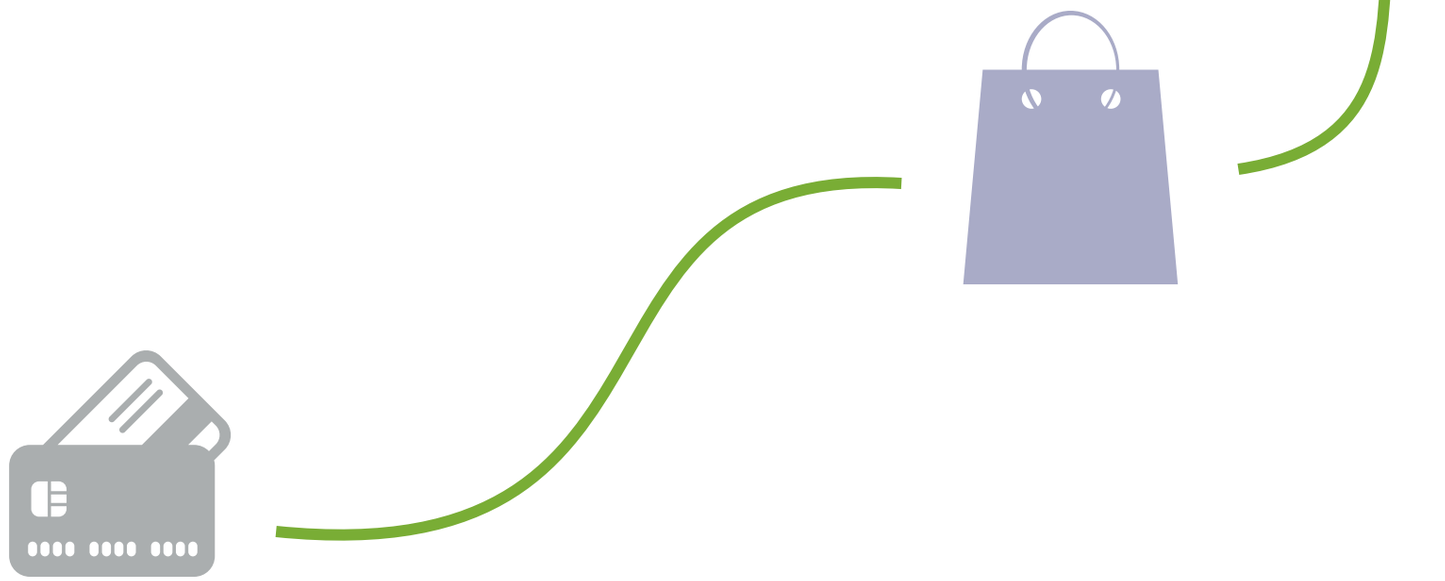
3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   According to Rome I, the governing law will be that of the country of residence of the consumer provided this is the country where the professional carries out his/her activities or to which his/her activities are directed.

4. Are there any other relevant issues related to applicable law and cloud computing?
   No. The atypical nature of cloud computing may make the application of jurisdictional rules unclear. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?

The Spanish consumer protection laws apply to cloud services to the same extent as to other online services (mainly Spanish rules on standard terms and conditions and on protection of consumers). The Spanish consumer protection laws are strict, especially in terms of interpretation of clauses in agreements and terms and conditions that may be considered abusive. ■



Data protection

1. Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?

The Spanish Data Protection Act (LOPD) and its Regulations (RLOPD) implements the EU Data Protection Directive and is generally compatible. The LOPD and RLOPD do not deal with cloud computing specifically. The Spanish Data Protection Agency (AEPD) ran a consultation on cloud computing in order to finally define the AEPD's views on the matter but it has not yet published these views. Nonetheless, it has published a report on aspects of cloud computing relevant to law firms. It has also published a legal report (0157/2012) that establishes a possible way to obtain authorisation from the AEPD to make international transfers in the context of a cloud service (based on contractual safeguards adapted to cloud computing business models).

There are strict requirements in certain respects (for instance detailed compliance with a set of security measures) and the legislation is strictly applied (with significant fines in cases of breach).

2. Which law is applicable in the case of a dispute concerning data protection and cloud computing?

The LOPD governs all processing of personal data:

- where the processing is carried out in Spanish territory in the context of the activities of an establishment of the controller;
- where the controller, though not established in Spanish territory, is subject to the application of Spanish law by virtue of international public law
- where the controller is not established in the territory of the European Union and for purposes of data processing makes use of equipment situated in Spanish territory, unless the equipment is used solely for purposes of transit.

Briefly, if the controller of the data is located in the Spanish territory (or is located outside the EU but uses equipment in Spain for the processing of the data – e.g. cookies) the LOPD will apply (it does not matter where the cloud provider is located). ►

3. Who is the data controller in a cloud computing service?
This depends on the service concerned. The AEPD has not issued any guidelines or recommendations yet (except those concerning the activities of law firms) but in principle, according to the usual characteristics of a cloud computing service, the client is likely to be the controller (and the provider of cloud services a processor).

4. Who is the data processor in a cloud computing service?
The provider of cloud services (see Q3 of this section), but each case needs to be studied in the light of its specific circumstances as the provider could be considered joint controller of the processing if it holds control over the data.

5. If the cloud provider is a data processor, what are its obligations under data protection law?
The performance of processing operations for the account of third parties shall be governed by a contract that is in writing or another form that allows its conclusion and contents to be evidenced. It needs to expressly stipulate that the processor shall only process the data in accordance with the instructions of the controller. Also that he shall not apply or use them for a purpose other than as established in the contract, nor disclose them, even for storage purposes, to other persons.

The contract shall also stipulate the specific security measures referred to in the LOPD and in the RLOPD, which the processor is required to implement.

Once the contractual obligation has been performed, the personal data must be destroyed or returned to the controller, together with any medium or document in which any personal data on the subject of processing are recorded. The report of the AEPD addressed to law firms for their own activity states the need for:

- permanent availability and portability of information;
- encryption of the data;
- authentication mechanisms to access data;
- accessibility of data;
- backup management;
- disaster recovery;
- continuity of service;
- compliance with legislation relating to sub-contracting.

Once the AEPD issues a clear position on all aspects on cloud computing (not only ▶

addressed to law firms for their own activity and/or international transfers) the above general requirements might be adapted to fit the provision of cloud services.

6. Is there a requirement to notify end users about the use of cloud services?
There are no legal provisions addressing notification in case of use of cloud services. Under the LOPD, the data controller must provide the data subject with;

- clear and complete information on the processing;
- the recipients or categories of recipients of the data;
- the intended transfer of personal data to non-EU states (this international transfer needs to be consented to by the data subject unless an exemption applies).

Each case needs to be assessed in the light of its specific context, and in some cases the data subject will need to be informed of the use of cloud services (at least to a certain extent, for instance to inform and gather consent for the international transfer if necessary).

7. Is there a requirement to notify local data protection authorities about the use of cloud services?
There are no specific requirements that apply to use of cloud services. The standard notification regarding any processing of personal data is mandatory.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?
Yes, under the usual requirements for international transfers of data. That is, if the country of destination does not offer an equivalent level of security, generally, the international transfer requires one of the following:

- the express and specific consent of the data subject (including the relevant information on country of destination, the fact that it does not offer an equivalent level of security etc);
- authorisation from the data protection agency (where the controller needs to adduce adequate safeguards with respect to protection of the privacy and fundamental rights and freedoms of individuals, and as regards the exercise of the corresponding rights). The AEPD's legal report 0157/2012 opens the door to a new way of authorising data transfers outside the EEA by ►

adapting the EU Standard Contractual Clauses to the cloud computing service and allowing for a general authorisation to be obtained to cover all data flows between a cloud provider and its clients – not requiring an authorisation/client;
- if the country of destination is the US and the relevant entity is recognised for Safe Harbour protection.

9. Are cloud providers permitted to use sub-processors?

Yes, provided that the provisions related to sub-contracting of the RLOPD are complied with.

The RLOPD states that, to sub-contract services, the data processor needs the authorisation of the data controller and that:

- the contract between the controller and the processor needs to specify what services may be subject to sub-contracting and, where possible, the company to which they shall be sub-contracted. When the sub-contracted company is not identified in the contract, the data processor shall inform the data controller of its identifying data before proceeding with the sub-contracting;
- the processing of the personal data by the sub-contractor follows the instructions of the data controller;
- the data processor and the sub-contracted company formalise a data processing contract with the requirements of the LOPD and RLOPD.

The recent report 0157/2012 deals with sub-contracting in cloud computing and specifies that a single framework agreement between the cloud provider and the sub-processor is possible (to cover the processing of the data controlled by each of the clients of the cloud provider). Also, that when the sub-contracted company is not specified in the processing contract between the client and the cloud provider, it suffices that the contract specifies a website where all the necessary information on the sub-contractors is given.

10. What are the security requirements connected with processing data?

There are extensive security requirements that a data processor needs to comply with (and that need to be included in the contract between the controller and the processor). Such requirements are stated in the TITLE VIII of the RLOPD. ►

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?

Yes. Personal data revealing ideology, trade union membership, religion and beliefs may only be processed with the express, written consent of the data subject. Personal data relating to racial origin, health or sex life may only be obtained, processed and disclosed when permitted by a law on the grounds of general interest, or with the data subject's express consent. Such data is sensitive and implies the data processor implementing high level security measures (as opposed to the basic or medium level).

Financial information will probably require the implementation of medium level security measures.

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?

The Spanish Data Protection Agency (AEPD) ran a consultation on cloud computing in order to finally define the AEPD's views. It has not yet published these views. It has only published a report on aspects of cloud computing to be taken into account by law firms. Also a legal report (0157/2012) regarding the way of obtaining authorisation from the AEPD to make international transfers in the context of a cloud service. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   AENOR (the Spanish Association for Standardisation and Certification). As far as we know, within AENOR, the sub-committee CTN71/SC38 is in charge of normalisation of services and platforms in the area of Architectures Oriented to Services (SOA) and Services in the cloud. The sub-committee mirrors the ISO JTC1/SC 38 Distributed Application Platforms and Services (DAPS).

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   The references are:

   - Cloud Data Management Interface (CDMI); SNIA
   - SNIA Open Virtualisation Format (OVF); DMTF
   - DMTF IEEE P2301, Draft Guide for Cloud Portability and Interoperability Profiles (CPIP); IEEE

   To the best of our knowledge the most commonly used is Open Virtualisation Format (OVF); DMTF.

4. Are there applicable international standards relevant for cloud computing that are commonly used?
   The references are the same as for the rest of the jurisdictions (standards on security, portability, interoperability etc.) but we are not aware of the use that is given to such international standards.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   No.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   No. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?

In Spain there were no particular provisions related to the outsourcing by financial entities of financial services or other services typically performed by these institutions, including cloud computing services, until recently. The main development has been carried out by Royal Decree 216/2008, 15 February, on equity of the financial entities. This allows financial entities to outsource to a third party the development of their main services and activities The exceptions are those activities/ services reserved to financial entities, if the service or activity is not left without content and if the delegation does not reduce the internal control of the financial entity and the supervision carried out by Bank of Spain.
The requirements that have to be met include:

- the delegation does not imply the transfer of liability of the financial entity;
- the delegation will not modify the relations between the financial entity with their clients and authorities;
- the outsourcing agreement must be in written form.

This has been further developed by a Resolution of the Bank of Spain.

While using cloud computing services, financial institutions must comply with general security obligations and requirements established MiFID and in the Spanish regulation relating to internal control of credit institutions and investment firms. Although not compulsory, Spanish financial entities are complying with high technical standards.

Furthermore, the Spanish Data Protection Act must be considered. According to this, the provider is required to regulate the access to the personal data of clients of the financial entity. The agreement between the financial entity and the cloud computing provider must include a clause in accordance with the Spanish Data Protection Act in relation to the obligations of the data processor. ■

Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, but it depends on the license terms.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   No.

3. Is it possible to use Open Source Software for cloud computing?
   Yes.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   No special sanction in relation to cloud. The standard legal regulation on IPR applies.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   No special sanction in relation to cloud. The standard legal regulation on IPR applies.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   ISP shall not be liable for the information placed in the cloud at the request of the recipient, provided that they do not have actual knowledge that the activity or the information stored is unlawful, or that it causes actionable damage in respect of the goods or rights of a third party. They are also not liable if they do have knowledge, and act diligently to remove the data or to disable the access.

   The exemption of liability shall not apply when the recipient of the service is acting under the direction, the authority or the control of his provider.

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?
   Yes, a competent body might declare that the data is unlawful and order its removal or the disablement of access. ▶

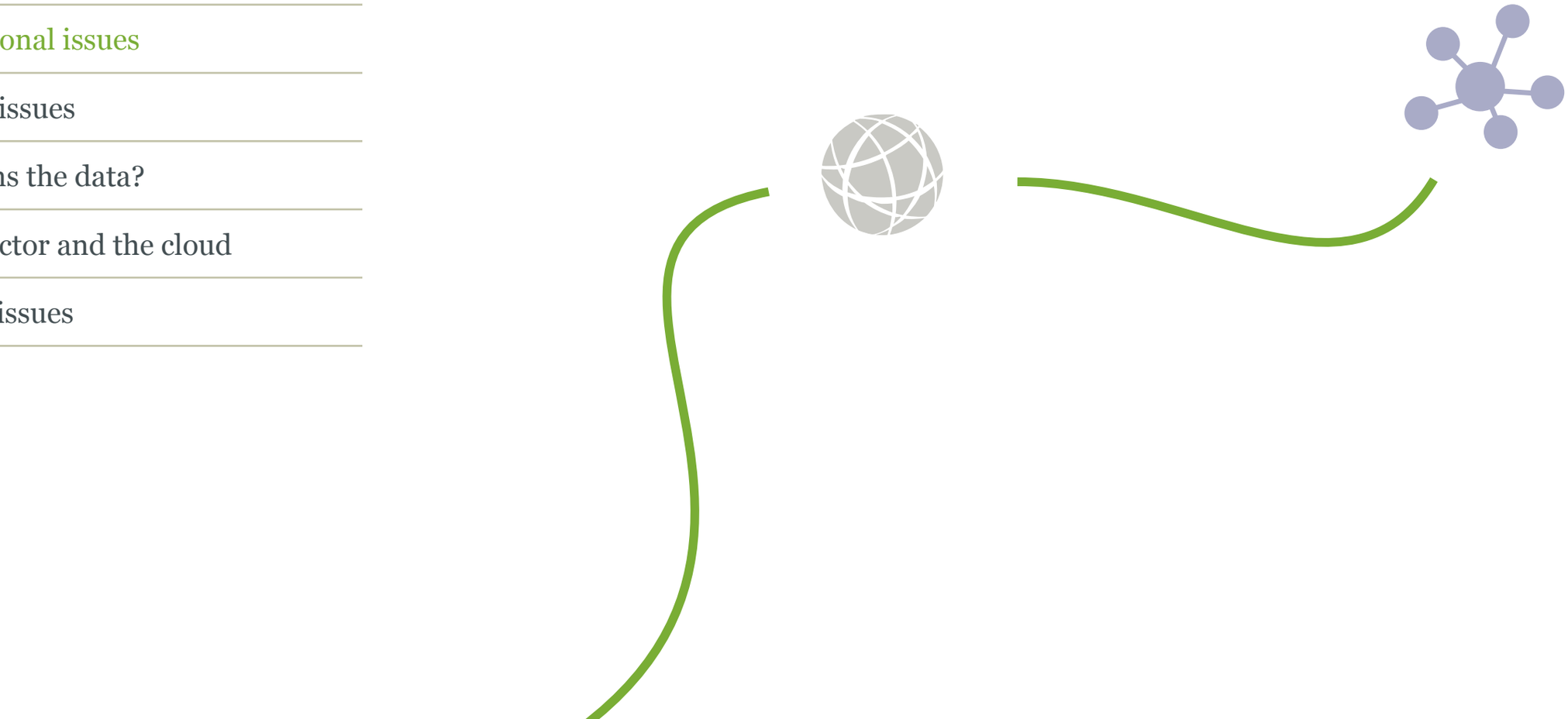
There is not an information duty. If the ISP has knowledge of the infringing act, it needs to act diligently to remove the data or to disable access in order not to incur potential liabilities.

8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?

The principle set out in the Consolidated Intellectual Property Law, is that intellectual property rights are freely assigned or transferred and will have the scope agreed by the parties in the agreement. The assignment is limited to the right or rights assigned, the forms of operation expressly provided for and at the time and in the territory established. Where the time and territory are not established, the time limit of the assignment will be 5 years and the territory will be the country where the assignment is carried out. ■

International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   No. ■



Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   From a contractual perspective it depends on contractual arrangements. The general principles of civil law would apply (i.e. breach of obligation, damage/loss of profit and causal link between the breach of obligation and damage/loss of profit).

   Regulator liability may exist towards the AEPD if there is a loss of personal data and the Spanish Data Protection legislation applies.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   There are no prohibitions on limitation of liability specifically relevant to cloud computing. The general legal provisions and case law relating to unfair provisions (B2C) and prohibition of limitation of liability in case of wilful intent or gross negligence (B2B) apply.

3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   Not specific to cloud services.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   This is no different to the insolvency/ bankruptcy of any other entity under Spanish law. From a practical point of view, bankruptcy of cloud provider might imply risks to the data availability and the service continuity. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   No specific regulation. Standard rules on ownership and title apply and the contractual provisions need to be checked. In the case of personal data the controller will in principle (subject to the circumstances) be the client.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud)? Who is also the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   No specific regulation. Standard rules on ownership and title apply and the contractual provisions need to be checked. ■

Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes, public bodies are showing an increasing interest in cloud computing. The technology only reached the public sector recently but statistics published by the National Institute Of Communication Technologies, show 33.4% of public entities are users. 14.2% adopted it within the last 12 months and 51.2% within the last 3 years.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
   There is not yet a 'Government Cloud' but the authorities have established that they would like to tend towards a model of "community cloud" for all public administration (integrating national, regional and local administration). The budgetary situation and spending and deficit adjustments needed have led public authorities to view cloud computing as a potential instrument to save costs and optimise technology.

The spread of cloud computing among Spanish public sector entities is limited, and is more common among local authorities than central government or autonomous community bodies. According to statistics published by the National Institute Of Communication Technologies, 33.4% of the public entities are users of a cloud computing-type service. The remaining 66.6% have not opted to include a cloud service. An example of public administration project in this area is the Correos – SISNOT electronic notification platform.

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   No, apart from Royal Decree 3/2010, on the National Security Scheme, and Royal Decree 4/2010 on the National Scheme for interoperability. These have a number of provisions on security and technological standards to be considered by public authorities. ▶

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
Yes, for instance a study on cloud computing in the Spanish public sector drafted by the National Institute Of Communication Technologies (a Government body attached to the Ministry of Industry, Energy and Tourism) and funded as part of the SERPLAGO project.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
Consolidated Public Sector Procurement Law regulates the procurement procedures of the Spanish public authorities, which cloud-based contracts will have to adhere to.

It includes the minimum content of the agreement between the authority and the cloud service provider. It also covers the other conditions required, the prohibitions on contracting, and restrictions in terms of aptitude, solvency, duration and other applicable circumstances.

6. Who is or would be the responsible regulator for cloud services?
The AEPD for data protection matters.

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
The National Security Framework in the field of e-Government (Royal Decree 3/2010) and the National Interoperability Framework (Royal Decree 4/2010), are applicable in the field of public authorities. Both include provisions relating to the standards and procedures applicable in the field of security and interoperability. Cloud computing providers are required to provide and, in many cases, implement and manage these when providing services to public bodies. ■

Security issues

1. Are cloud services providers free from content filtration or censorship obligations?
   Yes, there is no mandatory/general filtering or censorship of content in Spain.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   There is no specific law aimed at cloud services. Cloud service providers must comply with the regulations related to the protection of personal data (LOPD and RLOPD). ■

Sweden

In Sweden, an increasing number of municipalities, authorities and businesses are considering the use of cloud services, where public sector organisations also have started to procure cloud services. Data privacy and security issues are the two subjects that are most frequently discussed when customers consider the use of cloud services. The Swedish Data Inspection Board and Cloud Sweden (a subgroup within the Swedish Computer Association) have issued guidelines for cloud computing http://www.datainspektionen.se/in-english/cloud-services/.

The Swedish Data Inspection Board is heavily involved in data privacy issues connected with cloud computing since organisations must carry out a risk and impact assessment in order to assess if it is possible to appoint a certain cloud service provider, what security level that is appropriate and what measures that have to be taken. There are also a lot of discussions regarding the issue of where personal data may be stored and processed, i.e. only within Sweden, EU/EEA or in third countries and what measures are necessary in order to secure the data. ■

General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   Yes. However, limitations may apply to its content, especially regarding B2C contractual relationships. ■

Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes, but there may be mandatory rules on applicable law and jurisdiction which apply irrespective of contractual provisions (e.g. in relation to data protection and consumer protection).

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   Contractual obligations – According to the Rome I Regulation, a B2B contract for the provision of services shall be governed by the law of the country where the service provider has its habitual residence or central administration. The same applies to a rental contract. In these circumstances, this is usually the law of the place in which the CSP locates its servers. The service provider can be defined as the party required to affect the characteristic performance of the contract – in this case the CSP.

   Non-contractual obligations – According to the Rome II Regulation, and subject to a number of exceptions, the law of the country in which the damage occurs or is likely to occur is applicable.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   Contractual obligations – According to the Rome I Regulation, B2C contracts shall be governed by the law of the country where the consumer has his habitual residence, provided that either the business (the CSP) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or directs such activities to that country or to several countries including that country and the contract falls within the scope of these activities.

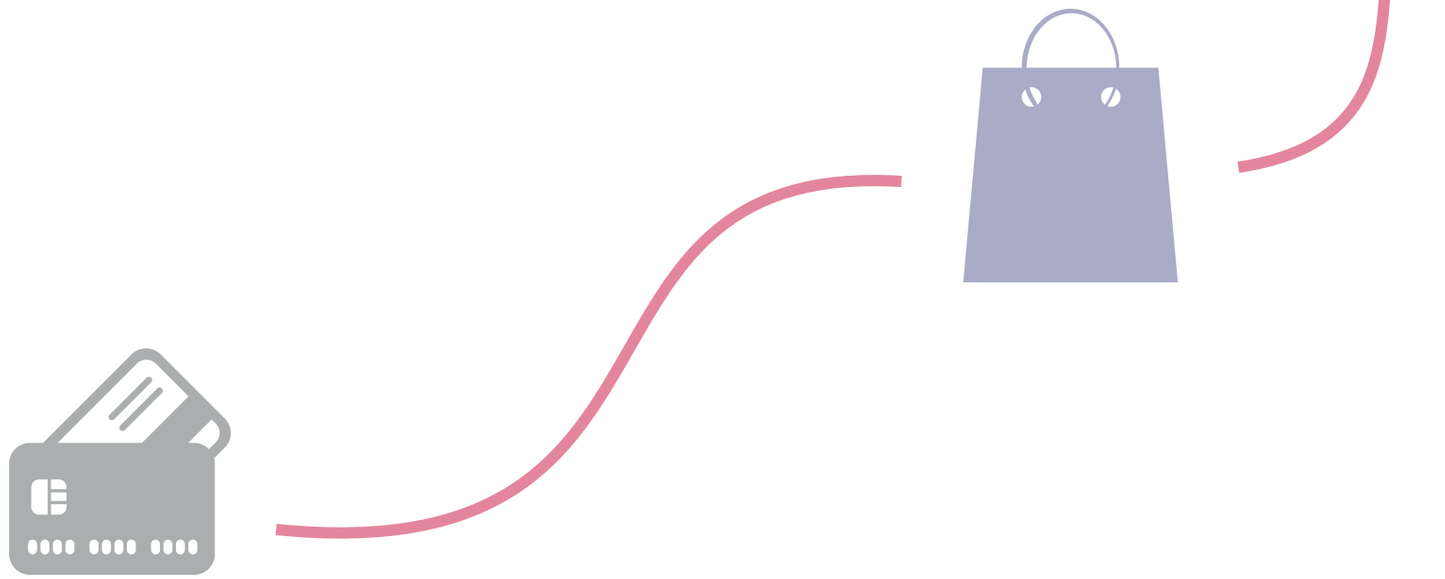
   Non-contractual obligations – According to the Rome II Regulation, and subject to a number of exceptions, the law of the country in which the damage occurs or is likely to occur is applicable.

4. Are there any other relevant issues related to applicable law and cloud computing?
   No. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?

   In Sweden there is no consumer protection legislation that specifically applies to cloud computing. However, special obligations apply to e-commerce agreements (e.g. the Distance and Doorstep Sales Act and the Electronic Commerce Act). ■



Data protection

1. Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?
   The Swedish Personal Data Act implements the EU Directive 95/46/EC and is generally the same as of the Directive. Neither of these address cloud scenarios specifically.

2. Which law is applicable in the case of a dispute concerning data protection and cloud computing?
   The Swedish Personal Data Act is applicable if the data controller (e.g. a user of cloud computing services) is established in Sweden or if the data controller is established outside the EU/EEA but uses equipment in Sweden for processing. The Swedish Personal Data Act applies unless the data controller's operations are governed by other enactments (e.g. within the health and hospital care area).

3. Who is the data controller in a cloud computing service?
   The data controller is the person or entity, alone or together with others, deciding the purposes and means of the processing. Normally, this is the customer.

4. Who is the data processor in a cloud computing service?
   The data processor is the person or entity processing personal data on behalf of the data controller. Normally this is the CSP.

5. If the cloud provider is a data processor, what are its obligations under data protection law?
   The data controller is liable for data processing under the Swedish Personal Data Act regardless of whether a data processor is involved. The Swedish Personal Data Act requires the data controller to ensure that the data processor, through a processor agreement, processes the data only in accordance with the data controller's instructions and takes appropriate technical and organisational security measures.

6. Is there a requirement to notify end users about the use of cloud services?
   No, the data subject need not be informed that cloud services are used to process the data. In accordance with the Swedish Personal Data Act, the data controller must provide certain information, regardless of by which means the personal data is processed. This includes the purposes of the processing, what personal data is processed, what security measures are being taken, whether ▶

the personal data may be transferred to a third country and whether the data may be disclosed to a third party.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?
No, not specifically relating to the use of cloud services. Processing of personal data shall be notified to the Swedish Data Inspection Board, unless a personal data officer is appointed or other exceptions apply.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?
Yes, provided that one of the following criteria is satisfied:

- the laws of the non-EU/EEA country provide sufficient data protection (a case by case assessment is necessary and the data controller has the burden of proof);
- the receiver is part of a Safe Harbour scheme;
- standard contractual clauses are used to safeguard an external transfer;
- binding corporate rules, approved by competent authorities on an EU level, are used to safeguard an internal transfer;
- the data subject's consent to the transfer is obtained;
- the transfer is necessary for one of the following reasons:
  - the performance of a contract between the data controller and the data subject, or the implementation of pre-contractual measures taken in response to the request of the registered party;
  - the conclusion or performance of a contract between the data controller and a third country which is in the interest of the data subject;
  - the establishment, exercise or defence of legal claims;
  - the protection of vital interests of the data subject.

9. Are cloud providers permitted to use sub-processors?
Yes, provided the sub-processors are bound by a processor agreement with the data controller. This can be entered into by the first data processor with a mandate from the data processor. Also provided that the data controller is aware of any sub-processor so that the sub-processor's processing may be controlled as regards security measures, etc. ►

10. What are the security requirements connected with processing data?
Appropriate technical and organisational security measures. What is appropriate in a given situation depends on:

- the technical possibilities available;
- what it would cost to implement the measures;
- the risks related to the processing of personal data;
- the sensitivity of the personal data.

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?
Under the Swedish Personal Data Act, sensitive data is defined as data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership to a work union, or information relating to health or sex life. Processing of these types of data is subject to further requirements and, generally, more substantive security measures need to be taken. Some types of data that are not officially classed as sensitive may require more substantive security measures than others; it depends on how sensitive the data is and other factors concerning the processing. See Q10 of this section.

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?
Not in Sweden as far as we are aware. The draft regulation on a European Union level is of high relevance. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   The Swedish Standards Institute (SIS) have ongoing standardisation projects, which include establishing national standard terms and definitions.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   We are not aware of any standards.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   We are not aware of any guidance or standards.

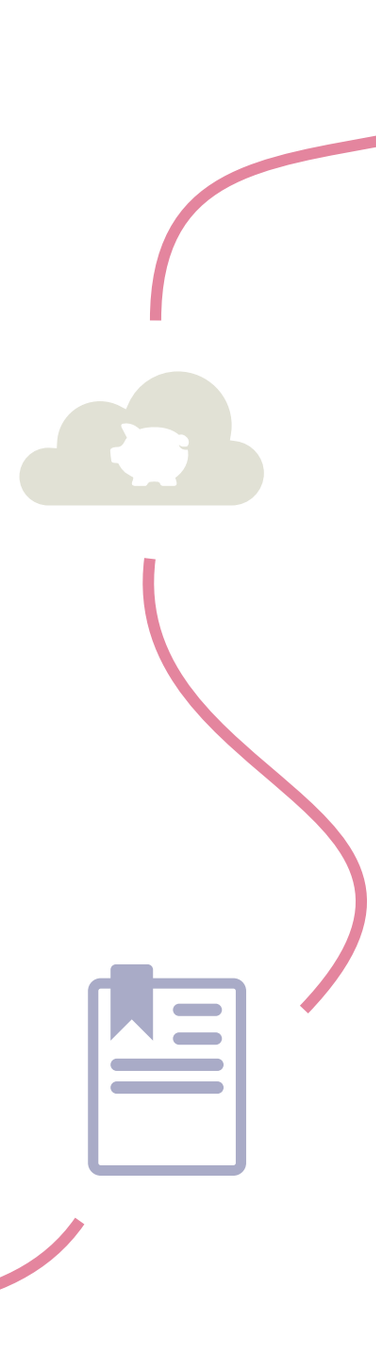
4. Are there applicable international standards relevant for cloud computing that are commonly used?
   We are not aware of any guidance or standards.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   The Swedish membership organisation Swedish IT & Telecom Industries (Swe: IT & Telekomföretagen) has published general terms and conditions titled “Cloud Computing version 2010”, “Cloud Computing Special Conditions” and “Service Levels for Cloud Computing”.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   We are not aware of any other issues. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?
   No, regulations connected to the financial sector tend to focus on the services provided rather than the means through which those services are rendered (e.g. through cloud computing). Even if there are no regulations specifically targeting cloud computing, regulations may indirectly affect how the services are rendered (e.g. regulations may stipulate certain requirements that will have to be integrated into the system/service for compliance with the applicable regulations). Different regulations may apply depending on the financial services provided. If financial services are provided to Swedish entities and/or individuals, it may be required to obtain relevant approvals and permits from the Swedish Financial Supervisory Authority for the services. ■



Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, if this is set out in the terms of the agreement.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   The Swedish membership organisation Swedish IT & Telecom Industries (Swe: IT & Telekomföretagen) has published general terms and conditions titled “Cloud Computing version 2010”, “Cloud Computing Special Conditions” and “Service Levels for Cloud Computing”.

3. Is it possible to use Open Source Software for cloud computing?
   Yes.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   There is no distinct intellectual property law specifically targeting cloud services. The civil sanctions laid down in intellectual property law may apply if material is put into the cloud in breach of intellectual property law.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   There is no distinct intellectual property law specifically targeting cloud services. The criminal sanctions laid down in intellectual property law may apply if material is put into the cloud in breach of intellectual property law.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   Yes. If the ISP is acting in breach of intellectual property law, it can be held liable for direct infringement. This could potentially be the case if the ISP makes unauthorised copies of copyrighted material that is being uploaded into the cloud by its users. The ISP can possibly be held liable for indirect/contributory infringement in case its users act in breach of intellectual property law when putting material into the cloud. In cases concerning indirect/contributory infringement, the ISP’s awareness of the infringing activities, whether the ISP has acted to prevent further distribution of infringing material after gaining knowledge, and whether the overall purpose of the service is legitimate or not has been taken into ▶

account in court assessments. However, there are few cases where cloud services have been specifically targeted. Civil and criminal sanctions are applicable in case of a direct or indirect/contributory infringement.

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?

There is no provision specifically targeting enforcement of notice-and-takedown procedure in Swedish intellectual property law. In infringement cases where the court has held ISPs liable for indirect/contributory infringement, it has stated that the ISP did not prevent further distribution of infringing material after being notified of the infringement by the rights holder (and such action would not imply unreasonable sacrifices on part of the ISP). There is no obligation to inform any authorities of the user's infringing actions.

8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?

One relevant copyright law issue is that it is uncertain whether the users can benefit from the private copying exemption when using cloud services that include a time-shifting function. There is a limitation to the private copying exemption in Swedish law that prohibits third parties making copies on a private person's behalf. ■

International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   We are not aware of any such specific provisions. ■

Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   In Sweden there are no specific regulations relating to cloud computing. Any loss of personal data would be subject to the Swedish Personal Data Act under which the data controller will be liable to pay damages to a data subject who has had his or her personal integrity violated due to the loss.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   There are no specific prohibitions relating to cloud computing. Any limitations that would be applicable if the service was provided by other means would also be applicable to the agreement between the user and the CSP.

3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   There are no specific prohibitions for cloud computing. However, any binding norms that would be applicable if the service was provided by other means would also be relevant to cloud computing.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   This is no different than the insolvency/ bankruptcy of any other entity under Swedish law. From a practical point of view, bankruptcy of a cloud provider might imply risks to the data availability and the service continuity. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   Swedish law does not define the owner of the data placed in the cloud. This should be determined by the contract between the service provider and the user.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud)? Who is also the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   Swedish law does define the owner of modified data in the cloud. The same applies to the ownership of copies being made in the cloud. This should be determined by the contract between the service provider and the user. ■

Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes. Certain Swedish municipalities use cloud services and have been criticised by the Swedish Data Inspection Board for not complying with the Swedish Personal Data Act while doing so.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
   Certain Swedish municipalities use cloud services and have been criticised by the Swedish Data Inspection Board for not complying with the Swedish Personal Data Act while doing so.

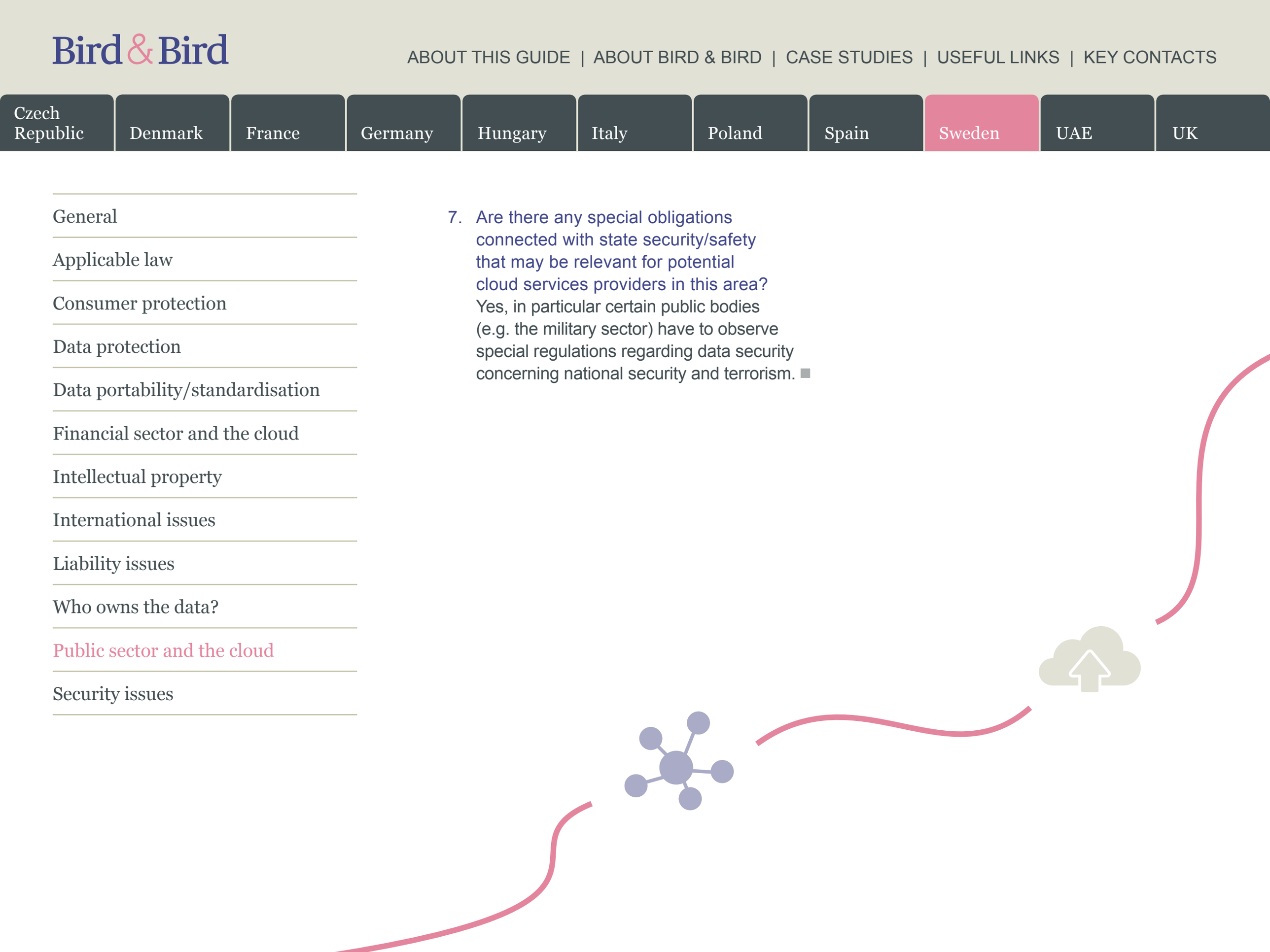
3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   The Swedish Data Inspection Board has issued guidelines on data protection and the use of cloud services.

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   The Swedish Data Inspection Board has issued guidelines on the use of cloud services and data protection issues. Cloud Sweden has published checklists relating to the use of cloud services.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
   No.

6. Who is or would be the responsible regulator for cloud services?
   The Swedish Data Inspection Board is the supervisory authority in relation to data protection. It would supervise any processing of personal data, including those relating to cloud computing. Given that the use of cloud computing is not specially regulated, any supervisory authority responsible for the service provided is also responsible for the same service provided by means of cloud computing. ►

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
   Yes, in particular certain public bodies (e.g. the military sector) have to observe special regulations regarding data security concerning national security and terrorism. ■



Security issues

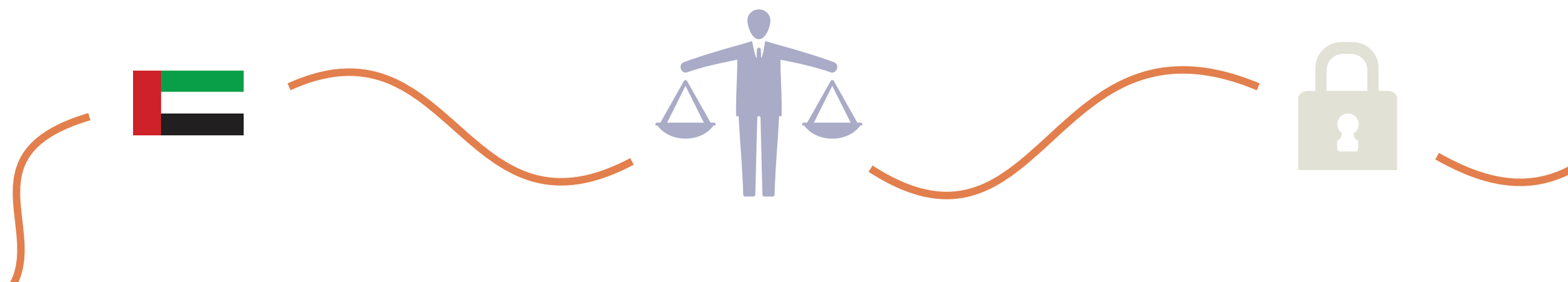
1. Are cloud services providers free from content filtration or censorship obligations?
   We are not aware of any such obligations.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   Only indirect, see answer to Q5 regarding Data Protection. Given that the use of cloud computing is not specially regulated, any regulations requiring certain security measures to be taken relating to the service provided would generally be applicable to the same service provided by means of cloud computing. ■

United Arab Emirates

Cloud computing is becoming increasingly popular despite the lack of a prescriptive legislative framework or official standards specifically relating to the provision of these services in the UAE. General laws apply and provide a degree of regulation but, given the lack of a comprehensive legal framework, parties are still entering into a relationship based largely on trust with a view to benefitting from the financial advantages of remote access computing services.

New laws aimed at tackling cyber crime and the mishandling of personal and sensitive information online could indicate a move towards addressing privacy issues and the protection of confidential/personal information online. As of mid January 2012, the UAE Federal Cabinet has approved new federal laws on commercial fraud which may further impact cloud computing. At this stage however, the claims which a cloud user could bring against a provider are still limited outside the scope of contractual rights and may not be effective, especially where the provider is located outside of the UAE. Issues relating to information security, privacy, record retention and data ownership are some of the key legal considerations currently associated with cloud computing. SMEs entering into these relationships are therefore strongly advised to undertake thorough due diligence and contingency planning exercises in order to minimise their exposure to these legal risks where possible. ■



General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   In general click-wrap agreements are lawful but cannot be used for all types of contracts (e.g. family, land and other agreements requiring notarisation). The terms of the click-wrap agreement will be subject to other general civil and commercial legislation governing contracts. ■

Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Freedom of contract is recognised in the UAE (except for certain types of contract), and therefore choice of law and jurisdiction provisions should, in principle, be enforceable. However, this does not always apply in practice.

   The UAE courts reserve the right to disregard contractual jurisdiction provisions and hear cases filed against UAE nationals, resident/ domiciled expatriates, and in some circumstances, non-resident foreign nationals. If the contract provides for disputes to be referred to arbitration in a foreign jurisdiction and a party raises the arbitration clause at the first hearing of the claim, a court will usually uphold the arbitration provision and refuse jurisdiction to hear the matter. The UAE is a signatory to the New York Convention and as such should enforce foreign arbitral awards.

   The courts are unlikely to uphold a choice of foreign law provision where there are public policy grounds for not doing so. This is a broad ranging and undefined right that the courts can rely on when the parties have agreed in their contract to another governing law with UAE jurisdiction. Even if the court chooses to accept the foreign law provision, there may be practical difficulties. For example, hearings are in Arabic and judges are often not well versed in foreign laws (especially those from non-civil legal systems), and cultural issues that make the application of a foreign law difficult to predict.

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   In the absence of contractual provisions regarding governing law/jurisdiction, the UAE courts may claim jurisdiction and apply UAE law to any claim that is brought before them. The position may be different if the contract includes a provision for arbitration in a foreign jurisdiction and a party raises the arbitration clause at the first hearing of the claim.

3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   In the absence of contractual provisions regarding governing law/jurisdiction, the UAE courts may claim jurisdiction and apply UAE law to any claim that is brought before them. The position may be different if the contract includes a provision for arbitration in a ►

foreign jurisdiction and a party raises the arbitration clause at the first hearing of the claim.

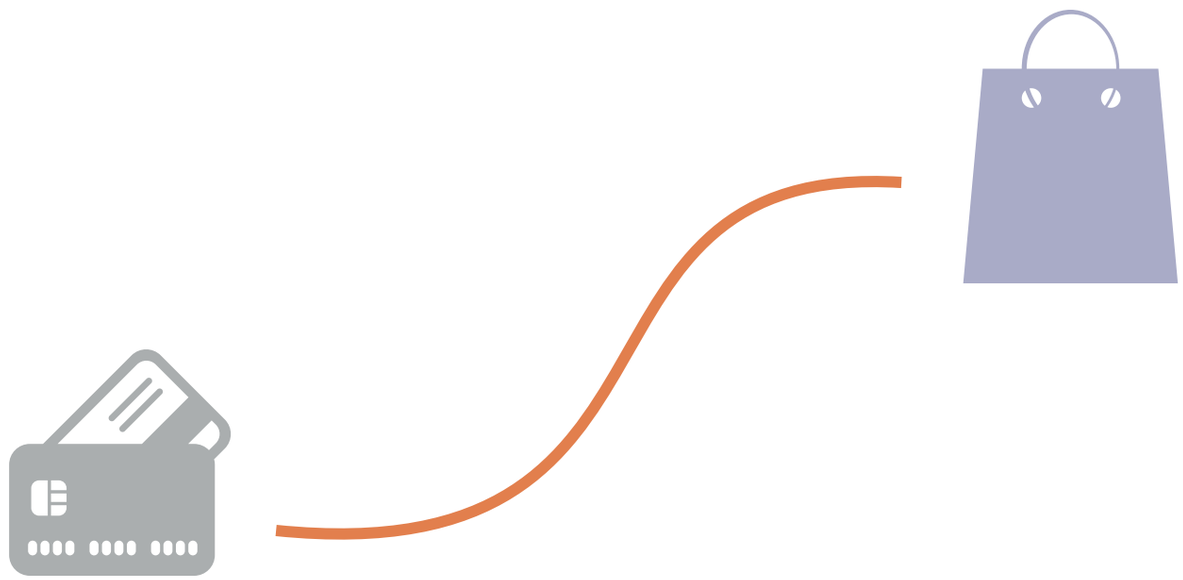
4. Are there any other relevant issues related to applicable law and cloud computing?
If the cloud service provider is based in, or the cloud services are provided from, another jurisdiction, the laws of that jurisdiction may also apply, notwithstanding a choice of law/ jurisdiction provision in their contract. ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?

The federal Consumer Protection Law contains a number of provisions designed to protect consumers purchasing both goods and services. From our experience, most enforcement action under this legislation has been taken against the providers of goods rather than ICT services. The federal Consumer Protection Law protects consumers against:

- abnormal price hikes (e.g. through implementation of price caps);
- misleading and confusing marketing;
- non-conformity to Accredited Standards of ESMA (we are not aware of any mandatory standards in respect of cloud computing);
- attempts to restrict or limit a consumer's right to damages in line with current rules. ■



Data protection

1. Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?
   No, the EU Data Protection Directive does not apply in the UAE. No single federal law in the UAE specifically governs the protection of personal data in a similar manner to the EU Data Protection Directive.

   Certain rights of privacy are protected in the Penal Code and through a patchwork of other pieces of federal and emirate legislation including the UAE Constitution, Civil Code, Labour Law, the updated Cyber Crimes Law (amended at the end of 2012) and the Electronic Transactions and E-Commerce Law.

   The Dubai International Financial Centre (DIFC) freezone has implemented its own data protection regime based on OECD guidelines and relevant EU Directives. The DIFC regime does not apply outside the DIFC. The Penal Code does apply in the DIFC.

2. Which law is applicable in the case of a dispute concerning data protection and cloud computing?
   This will depend upon a number of factors including what information is under dispute and under what specific UAE legislation the claim is made. For example, the Penal Code, which deals with criminal sanctions, applies to all acts done within the state and to acts done outside the state but where the effect of the act is intended to take effect within the state. Civil remedies are likely to be subject to the governing law and jurisdiction clauses of the contract.

3. Who is the data controller in a cloud computing service?
   The law of the UAE does not recognise and therefore does not make a distinction between a data controller and a data processor.

4. Who is the data processor in a cloud computing service?
   The law of the UAE does not recognise and therefore does not make a distinction between a data controller and a data processor. ►

5. If the cloud provider is a data processor, what are its obligations under data protection law?
The law of the UAE does not recognise the concept of a data processor and therefore the law does not make special provision for it.

6. Is there a requirement to notify end users about the use of cloud services?
There is no specific requirement to notify end users about the use of cloud services. It is advisable to obtain the end user's/data owner's consent to the specific processing activities contemplated in respect of his/her personal confidential information, particularly in light of the updated Cyber Crime Law. The Cyber Crime Law provides increased legal protection for the privacy of information that is published online. Conduct which amounts to a violation of the privacy of others is widely defined in the updated legislation, which also formally criminalises numerous cyber crimes.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?
No. There is no specific data protection law in the UAE and therefore no specific regulator.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?
Not applicable, although see Q6 of this section regarding the consent of the subject to the contemplated processing activities where personal confidential information is sent across a border.

9. Are cloud providers permitted to use sub-processors?
The UAE law does not deal with this point specifically, although see Q6 of this section regarding the consent of the subject to the contemplated processing activities.

10. What are the security requirements connected with processing data?
There are no specific security obligations placed on parties processing personal confidential information (except for specific industries – see Q11 of this section). A recurrent theme in the relevant legislation is to maintain the privacy and security of personal confidential information. This has been reinforced in the updated Cyber Crime Law and could be further discussed in proposed new federal laws on commercial fraud. It is therefore advisable for those in possession of another's personal confidential information to adopt suitable security regimes. ►

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?

Yes. There are specific requirements in respect of different types of data, including:

- medical data – practitioners may not disclose medical secrets except in very limited circumstances, although it is unclear whether patient consent to certain types of processing may permit use of cloud services in this context.
- credit information – credit information gathering agencies must be licensed to collect relevant financial and credit data. This data must be realistic, accurate and up to date and cannot relate to the private life, health condition, opinions or beliefs of the individuals concerned. The credit company has obligations to protect the data against unauthorised use and access and should have systems in place in respect of disaster recovery. Prior written consent is required prior to the disclosure of credit information to third parties. Any credit report may only be used for its intended purpose.
- ISPs – ISPs have specific obligations placed on them by the Telecommunications Regulatory Authority (TRA) in respect of the protection and use of information relating to consumers, including an anti-spam policy.
- the updated Cyber Crime Law provides increased protection of personal and confidential information published online, particularly in relation to credit card numbers, bank account statements, details of electronic payment methods and medical related information. The legislation also criminalises a wide range of online activity (see Q6 in section on Intellectual Property and Q7 in section on Public Sector & the Cloud below for examples of crimes under this new legislation)

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?

We are not aware of any current or planned legislation specific to cloud computing and data protection. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   The Emirates Authority for Standardisation and Metrology (ESMA) is responsible for creating new standards and identifying international standards that may be of use in the UAE. Although ESMA has approved a number of general IT related voluntary standards that may be relevant to cloud computing depending on the details of each case, we are not aware of any mandatory cloud related standards. Also see Q3 and Q4 in this section regarding Emirates eGovernment and public sector standards.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   Not for the private sector. We expect that the private sector adoption of standards with respect to cloud computing will be in line with international best practice. Standards and reference architecture have already been developed for the public sector as part of the Emirates eGovernment initiative.

4. Are there applicable international standards relevant for cloud computing that are commonly used?
   ESMA has approved a number of general IT related voluntary standards that may be relevant to cloud computing depending on the details of each case, but we are not aware of any mandatory cloud related standards. We expect that private sector adoption of standards will be in line with international best practice. Standards and reference architecture have already been developed for the public sector as part of the Emirates eGovernment initiative.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   No. Cloud service providers tend to develop their own SLA and EULA.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   No. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?
   Yes. All outsourcing of services and systems to third parties must be approved by the UAE Central Bank.

   The UAE Central Bank also regularly issues circulars and notices regarding operational matters that may be relevant depending on the specific details of any matter. ■

Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, provided that the original licensee has the right to sub-license the software under its licence. There may be licence registration requirements depending on the nature and purpose of the licence.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   No. Each cloud service provider tends to develop its own terms and conditions.

3. Is it possible to use Open Source Software for cloud computing?
   We are not aware of any specific legal restrictions on the use of Open Source Software (OSS). The use of OSS will be subject to the terms of the relevant licence.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   There are no specific legislative provisions dealing with the position in respect of the cloud and therefore the normal civil sanctions for breach of relevant intellectual property law and the Civil Transactions Law are likely to apply. For example, should there be an infringement of a copyright holder's rights, the rights holder may apply to court for precautionary measures to be taken against the infringing party (including seizure and prohibition orders). Damages for breach of rights would be assessed under the Civil Transactions Law.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   There are no specific legislative provisions dealing with the position in respect of the cloud and therefore the normal criminal sanctions for offences under intellectual property law are likely to apply. As well as fines and imprisonment for crimes committed under this legislation, the court may order confiscation and destruction of seized copies and equipment and the publication of the judgment in the newspapers. In relation to copyright crimes, the court may order the closure of the infringing business. ►

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?

There is no legislation in the UAE that deals specifically with cloud service provider liability in such situations. The Internet Access Management policy of the Telecommunications Regulatory Authority (TRA) imposes obligations on ISPs to deal with complaints and filter and block banned material (including materials that offend public morality or permit breaches of intellectual property rights). Violation may result in criminal and/or civil liability for the ISP. The two ISPs in the UAE, Etisalat and Du, have both established a process for users to notify them of abuses (as part of their Complaints Handling Process) and have implemented content filtering and blocking technology to support this.

Aside from intellectual property infringement, cloud service providers should be mindful of the provisions of the updated Cyber Crime Law, which criminalises a wide range of online activity including creating or running an electronic site or any information technology means to damage the reputation of the state, jeopardise state security, prejudice public morals, display contempt for holy symbols of Islam or promote narcotics and psychotropic drugs among other things. Any party that facilitates or co-operates in the commission of another cyber crime will potentially be liable for its commission and the possible sanctions include imprisonment, a fine and confiscation of all devices, programs or means used to commit the crimes. The Penal Code contains a number of provisions relating to enabling or encouraging others to commit a sin, which has in the past been construed broadly by the courts when they are unable to qualify specific types of crime and could extend to intellectual property infringement. If a cloud service provider is informed of such material on its servers and it fails to take any action to remove it, the chances of prosecution under these laws are increased. In mid January 2012, draft new federal Laws on commercial fraud are being considered which discuss the prohibition of misleading commercial advertisements, but it is yet to be seen if ISPs could be held liable in such a situation. ►

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?

To the best of our knowledge, there is no legislation that specifically deals with enforcing a takedown procedure in the UAE. Pursuant to the Internet Access Management policy, the TRA requires ISPs to respond to complaints (including complaints in respect of content) quickly and block prohibited content. If the ISP fails to respond to the complaint, an individual may contact the TRA for further assistance and resolution and the TRA may take action against the ISP. In our experience, the two ISPs in the UAE often quickly block access to sites which may hold infringing material.

As a result, ISPs often retain broad ranging rights in their standard customer terms and conditions in respect of the taking down/ deletion of material infringing third party rights or that offends public morality.

Also see point above regarding potential liability of the ISP under the updated Cyber Crime Law.

8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?

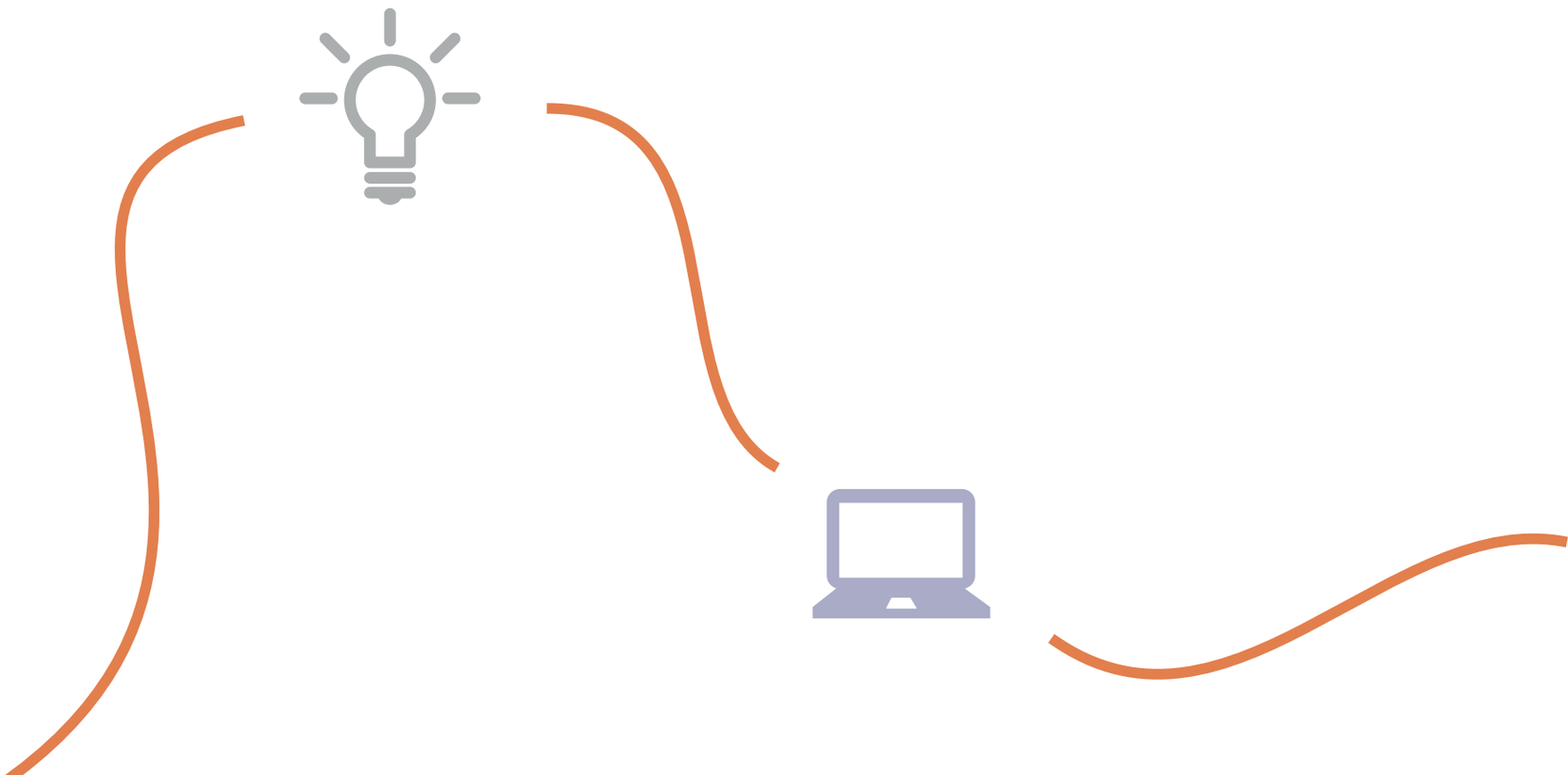
Customers and cloud service providers should consider the following:

Licensing: Although cloud computing contracts relate to the provision of services rather than to the supply of software to customers, appropriate software licences need to be granted to the customer to enable them to legally and correctly use the necessary software without the risk of copyright infringement.

Content: The customer will be required to grant to the cloud service provider a licence in respect of their content allowing the service provider to use any content stored on its servers. These licences are often expressed as being perpetual and irrevocable.

Intellectual property indemnities: The inclusion of intellectual property rights indemnities in cloud computing contracts remains important because customers have to rely on the service provider to ensure that software licensing issues have been resolved so as to entitle the customer to use the software as part of the service. ►

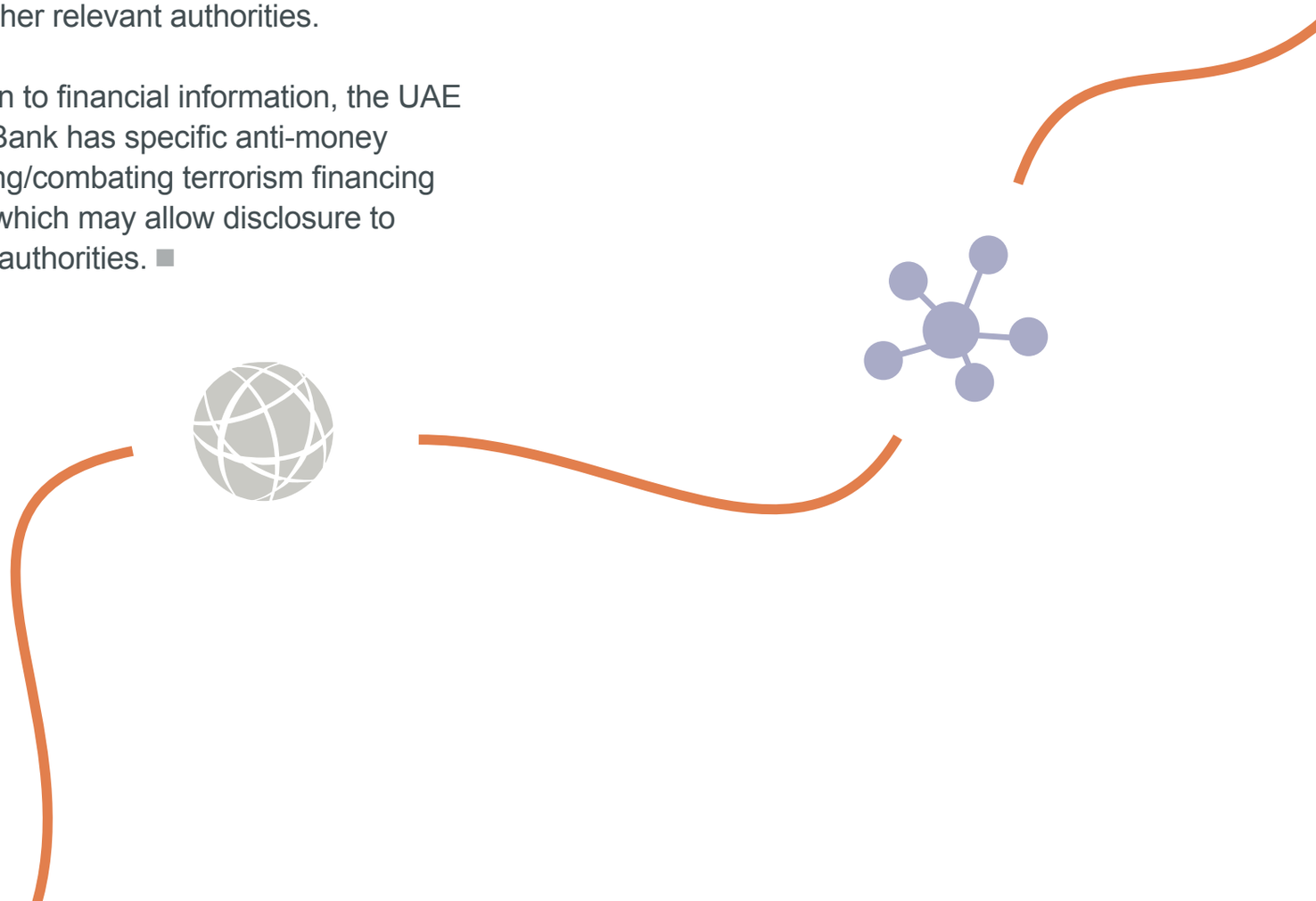
Cloud Service Provider Intellectual Property Protection: cloud service providers should attempt to deal with the protection of their own software and the extent to which customers may take advantage of know-how gained in a short-term contractual relationship, which may be terminated on short notice by a customer. ■



International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   We are not aware of any specific provisions relating to cloud services. Many providers retain broad ranging rights in their contracts to disclose information as required by law and to other relevant authorities.

   In relation to financial information, the UAE Central Bank has specific anti-money laundering/combating terrorism financing policies which may allow disclosure to relevant authorities. ■



Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   There are no specific legislative provisions relating to loss of data in the cloud and therefore liability would be determined on the usual basis under contract and civil code obligations similar to western concepts of tort. Provisions dealing with liability for data loss will normally be included in the contract between the parties.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   It is widely accepted that in most B2B arrangements, it is possible for parties to limit their liability in a commercial arrangement (except for wilful misconduct, gross negligence and fraud). Courts have the discretion to disregard the contractual allocation of liability where they see fit.
   The same discretion applies to liquidated damages, where the court may disregard an agreement on liquidated damages where the loss suffered is at variance with the actual damages incurred. Under UAE contract law, a party may only recover its direct losses and is not able to recover indirect and consequential losses. Certain direct economic losses (e.g. profit, opportunity) may be recoverable in some circumstances. Under the federal Consumer Protection Law, the consumer in a B2C relationship shall have the right to recover for personal injuries and damages in accordance with normal principles. Any agreement to the contrary shall be void.

3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   No, except for legislative requirements for services in general.

4. What will happen in the case of insolvency/ bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   Whilst UAE law provides a fairly detailed insolvency and restructuring framework, the law in this area is largely untested and so most businesses look to put in place and enforce their own commercial risk management strategies. It is difficult to assess with any degree of certainty the legal consequences of a cloud service provider's insolvency. ►

Hopefully the position will become clearer in the near future as a new federal Financial Restructuring and Bankruptcy Law is expected to be enacted soon.

For the time being, customers are advised to make a risk assessment on the benefits of putting their data and processes into the cloud weighed against the risk, likelihood and consequences of the cloud service provider becoming insolvent and ceasing to provide the service. The customer may want to consider its exit arrangements in this context as well as the business continuity services offered by the cloud services provider. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   The ownership of intellectual property rights should be clearly addressed in the contract. In the absence of any agreement to the contrary, the intellectual property rights in the data should remain with the original rights holder, and will not transfer to the cloud service provider automatically through placement in the cloud.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud)? Who is also the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   The ownership of intellectual property rights in derivative and new data should be clearly addressed in the contract. In the absence of any agreement to the contrary, the usual rules of authorship are likely to apply. ■

Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes. The Emirates eGovernment initiative, under the direction of the Telecommunications Regulatory Authority (TRA), is charged with formulating and overseeing the implementation of a robust shared infrastructure for federal government entities, which supports, among other things, the federal e-Government plan 2012–2014 to transform government e-services. Recognising the potential for cost savings and improving stability and security, Emirates eGovernment has already taken some preliminary steps to roll out its own shared cloud services in the UAE to other government entities. Government entities can now take advantage of a number of private/community cloud services including, hosting, storage, backup and software applications (e.g. e-mail and other web-based tools) via the Emirates eGovernment portal.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
   Yes. Emirates eGovernment, under the direction of the Telecommunications Regulatory Authority (TRA), is charged with formulating and overseeing the implementation of a robust shared infrastructure for federal government entities. Emirates eGovernment has already taken some preliminary steps to roll out cloud services in the UAE to other government entities. Government entities can already take advantage of a number of private/community cloud services including, hosting, storage, backup and software applications (e.g. e-mail and other web-based tools) and further cloud based services are planned for the future.

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   The Emirates eGovernment initiative has developed its own private/community cloud offering with its own standards and reference architecture. We are not aware of anything similar for the private sector.

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   The Emirates eGovernment initiative is actively promoting the use of its private/community cloud services within government. IT representatives from government ►

agencies regularly attend and contribute to seminars, discussions and other cloud computing events relating to both the private and public sector.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
Through the Emirates eGovernment initiative, public bodies are encouraged to procure cloud services from the Emirates eGovernment portal. There are initiatives being undertaken at the emirate level. For example, the Abu Dhabi Systems and Information Centre (ADSIC) is building strategic alliances with certain key partners to enable local government entities to take advantage of preferential terms offered by such suppliers (including MSAs with Microsoft and Cisco).

6. Who is or would be the responsible regulator for cloud services?
This has not yet been determined in the UAE, although it is likely that the Telecommunications Regulatory Authority (TRA) will play some role. The TRA is charged with the management of every aspect of the telecommunications and information technology industries in the UAE.

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
The UAE has introduced stringent export control laws and regularly supports UN backed sanctions regarding the transfer of sensitive materials and equipment to sanctioned countries. Added to this, cloud service providers should be aware of the provisions of the updated Cyber Crime Law, under which it is a crime for anyone to run or create an electronic site or any information technology means to damage the reputation of the state or any of its institutions.

Other examples of criminal offences under this new legislation are running an electronic site or any information technology means to promote protests without a licence, to promote or trade weapons, to publish information online for a terrorist group or any illegal group, association, organisation or body, or which could promote disorder, hate, racism or sectarianism and damage national unity and public order. The 2013 proposed federal commercial fraud laws may also introduce further obligations on cloud service providers. ■

Security issues

1. Are cloud services providers free from content filtration or censorship obligations?
   We are not aware of any content filtration or censorship obligations specifically related to cloud computing. Under the Internet Access Management policy of the TRA, ISPs are required to filter and block access to prohibited online content. The two ISPs in the UAE, Etisalat and Du, have set up filtering regimes as per the regulations of the TRA and block access to such materials. Banned categories tend to relate to content which offends the public morality of the UAE, breaches intellectual property rights (e.g. free music sharing sites) or which otherwise poses a threat to the safety and wellbeing of UAE inhabitants.

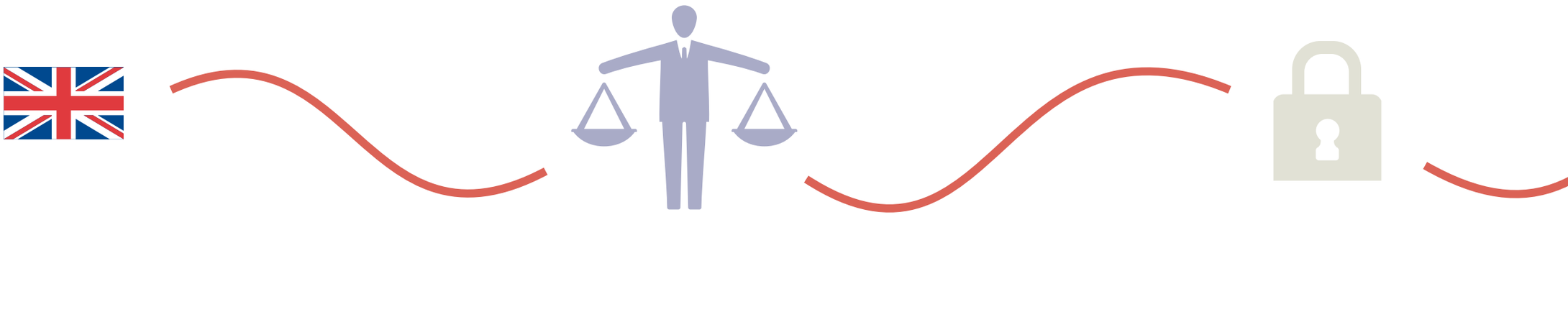
   Cloud service providers should be mindful of provisions in the updated Cyber Crimes Law (and of similar provisions in the Telecommunications Act) which make it an offence to eavesdrop, receive or intercept communications travelling across the Internet or information technology devices, record or disclose conversations, take photographs of others, create electronic photographs of others or disclose, copy or save photographs of others. Cloud service providers should bear this in mind when deploying content monitoring applications used to provide the services.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   There are no specific laws relating to cloud computing. Cloud service providers do however have obligations under the various privacy/cyber crime laws discussed in other questions. ■

UK

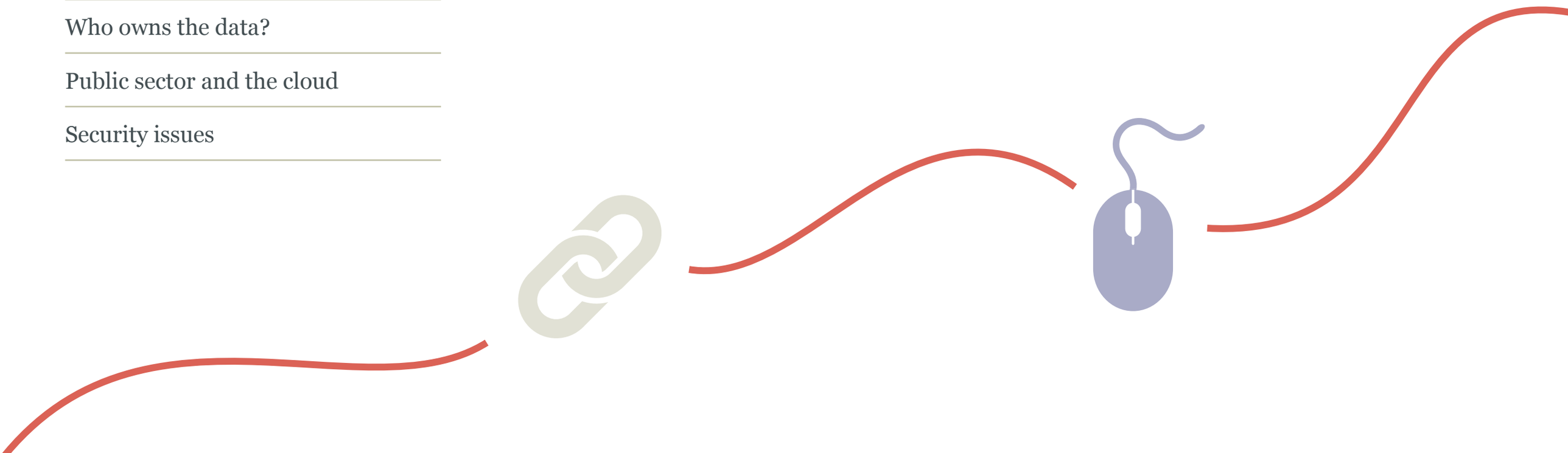
In the UK, we have seen very rapid adoption of cloud computing in the business environment – driven principally by a need by organisations to cut costs. IT budgets have been a principal target for these cost savings. SaaS is now routinely the preferred deployment model for new applications but organisations have also built their future ICT strategies around building cloud into their existing outsourced ICT. Organisations are keen on the flexibility and scalability this will provide and happy to trade-off some of the control that exists in having traditional bespoke services. This includes the public sector where, for example, the procurement process for the third iteration of the pan-government G-Cloud Framework will soon be underway.

Due to the widespread positive interest in these technologies, regulators and security accreditors in the UK are trying, as far as possible, to adopt a supportive approach and accept risk-based approaches to cloud adoption. However, this does not mean that cloud is viewed as appropriate for all applications and datasets so it cannot be viewed as a one size fits all solution. An additional challenge in the UK is how suppliers collaborate in multi-vendor environments built upon different services. Risk allocation and revenue recognition issues are key concerns when building multi-tenancy cloud services into traditional outsourcing arrangements. ■



General

1. Are click-wrap agreements (where a user has to click to agree to terms and conditions before using a product – usually software) lawful?
   The 2010 Foxtons case questioned the enforceability of click-wrap agreements that are overly lengthy and/or introduced too late in the process (so unlikely to be read by the customer). However, they remain the main approach to online contracting. ■



Applicable law

1. Is it possible to freely choose law/ jurisdiction in the contract?
   Yes, but there may be rules on applicable law and jurisdiction which apply irrespective of contractual provisions (e.g. in relation to consumer and data protection).

2. In B2B litigation, which law is applicable if there are no contract provisions regarding governing law/jurisdiction?
   For contractual obligations, the Rome Convention applies. This stipulates that, where no law has been expressly chosen in the contract, the law of the country in which the party who will perform obligations characteristic of the contract has its central administration or habitual residence will apply – this will typically be the country where the servers of the cloud service provider are located. For non-contractual obligations and where there is no express law chosen by the contract, subject to certain exceptions, the applicable law will be that of the country where the damage occurs or is likely to occur.

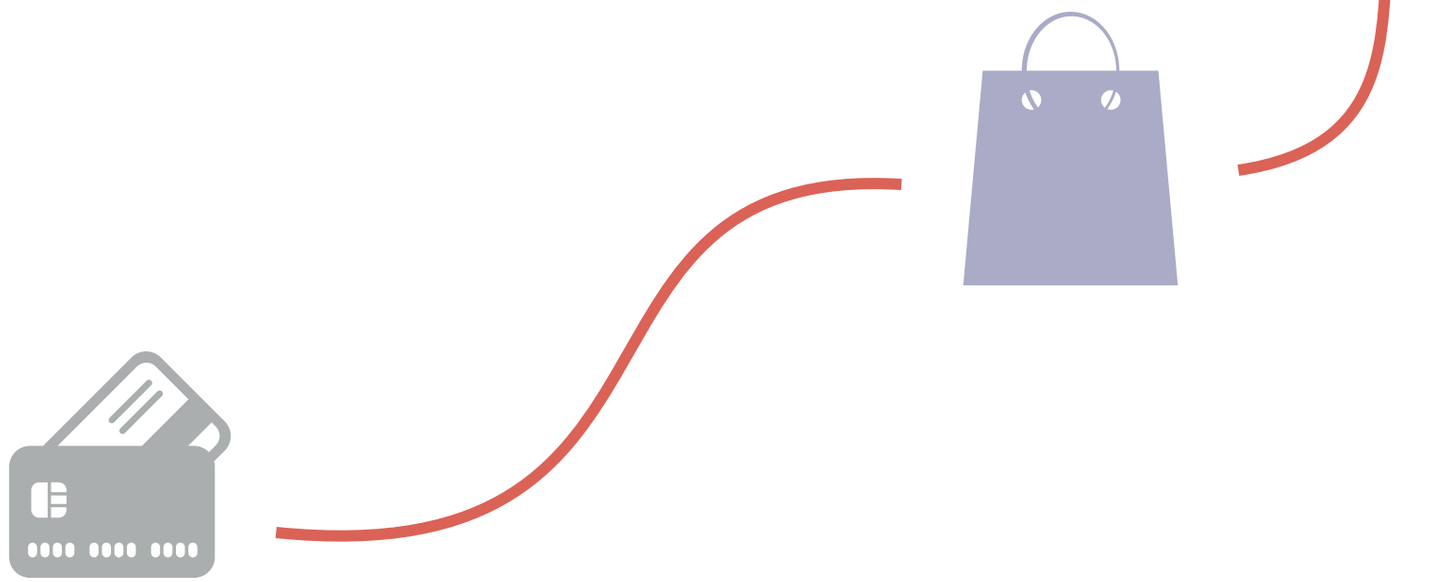
3. In B2C litigation, which law is applicable if there are no contract provisions regarding governing law and jurisdiction?
   Depending on the circumstances, it may be as in relation to B2B cloud services (see Q2 of this section) or it may be that the applicable law is the law of the country in which the consumer has its habitual residence. The Rome Convention provides that it is not possible to contract out of certain protection provisions of the law of the country in which the consumer has its habitual residence.

4. Are there any other relevant issues related to applicable law and cloud computing?
   Not specifically addressing cloud services, but depending on the type of service (e.g. communications) or data processed, other legislation could apply, whether from the UK or other jurisdictions (e.g. US PATRIOT Act). ■

Consumer protection

1. Are there any consumer protection issues that may be relevant for cloud computing services?

   The general view in the UK is that consumer protection legislation applies to cloud services arrangements. For example, the reasonableness of contract terms may be challengeable by consumers under the Unfair Terms in Consumer Contracts Regulations. ■



Data protection

1. **Is the data protection law compatible with the EU Data Protection Directive considering cloud computing issues?**
   UK data protection rules implement the EU data protection directive, and as such are not tailored to cloud scenarios.

2. **Which law is applicable in the case of a dispute concerning data protection and cloud computing?**
   The UK DPA applies to:
   - UK registered companies;
   - companies with an office, branch or agency in the UK;
   - companies with a regular practice in the UK;
   - individuals who are ordinarily resident in the UK;
   - data controllers established outside the EEA but who use equipment in the UK for the processing of data (otherwise than only for transit through the UK).

3. **Who is the data controller in a cloud computing service?**
   The data controller is the entity that determines the purposes and means of the processing of personal data and is responsible for compliance with data protection law. For B2B cloud services, the ICO usually views the customer as the data controller, although when the supplier has a large amount of control over the processing of personal data they may be considered a joint data controller. For B2C cloud services, the supplier is likely to be considered a data controller.

4. **Who is the data processor in a cloud computing service?**
   The data processor is a person/entity who processes data on behalf of a data controller. The ICO will regard the cloud service provider as a data processor in most B2B arrangements; unless they are a joint data controller (see Q3 of this section).

5. **If the cloud provider is a data processor, what are its obligations under data protection law?**
   The obligations under the Data Protection Act are on the data controller. A data controller should only allow a third party to process data on its behalf if it has appropriate organisational and technical measures in place to protect the data. This needs to be set out in the contract. ►

6. Is there a requirement to notify end users about the use of cloud services?
Data controllers can only process personal data for the purposes originally consented to. If the processing of that data within a cloud service goes beyond the original consent, the end customers may need to provide further consent.

7. Is there a requirement to notify local data protection authorities about the use of cloud services?
Not specifically, but general data protection registration rules apply.

8. Is it possible to send data outside the EU/EEA and if so what are the requirements?
The Data Protection Act implements EU data protection laws which prevent companies sending personal data outside the EEA except in circumstances where the destination country has been pre-approved as having adequate data protection. Only a handful of countries, including Argentina, Canada and Switzerland, have qualified as having adequate protection. In the event that adequate protection is not deemed to be in place, data may be transferred out to the US if the receiving entity is a member of the Safe Harbour scheme, or failing this, an organisation may transfer internally under binding corporate rules (BCRs), or externally under the Model Contract Clauses.

9. Are cloud providers permitted to use sub-processors?
Yes, if provided for under the contractual arrangements in place and only with the consent of the data controller. The data controller would usually place obligations on the data processor to pass on key data protection obligations, to ensure that any liability is covered off – ultimately the data controller is liable for any failure to abide by the Data Protection Regulations.

10. What are the security requirements connected with processing data?
No specific data security requirements are prescribed in the Data Protection Act and what is appropriate in each case will differ. The Data Protection Act requires data controllers to ensure appropriate technical and organisational measures are in place. The Information Commissioners Office has given the following guidance:

- security within the data controller's organisation is designed and organised to fit the nature of the personal data that the data controller holds and the harm that may result from a security breach; ►

- there is a clear understanding as to who within the data controller's organisation is responsible for ensuring information security;
- the right physical and technical security is put in place, and is backed by robust policies and procedures and reliable, well-trained staff;
- the data controller is prepared to respond to any breach of security swiftly and effectively.

11. Are there any special regulations concerning sensitive or/and financial information relevant to cloud computing providers?
Yes, the Data Protection Act has additional requirements for sensitive personal data (e.g. health, political and religious affiliations). The Financial Services Authority regulations apply to cloud service arrangements used by financial institutions.

12. Is there existing or planned legislation related to data protection and cloud computing that may be relevant?
No. ■

Data portability/standardisation

1. Are there any official public institutions responsible for standardisation?
   The Cabinet Office is looking to standardise use of IT within the public sector but there is no official body with a broader standardisation remit.

2. Is there any law establishing standards of portability and interportability of cloud computing platforms?
   No. We are not aware of any plans.

3. Is there a set of guidelines/standards commonly used in the context of interportability?
   We are not aware of any but there may be some that are seen as good practice among technical experts.

4. Are there applicable international standards relevant for cloud computing that are commonly used?
   We are not aware of any but there may be some that are seen as good practice among technical experts.

5. Are there any model Service Level Agreements or End User Agreements tailored to cloud computing that are commonly used?
   Each cloud service provider develops its own standard terms and service levels to match its service and attitude to risk.

6. Are there any other relevant issues concerning data portability/standardisation and cloud computing?
   Some customers are requiring tests of portability prior to accepting or adopting a service. ■

Financial sector and the cloud

1. Are there any special regulations connected with the financial sector applicable to adopting of cloud computing?
   Financial institutions have to comply with the FSA Handbook including security requirements where cloud services amount to a material outsourcing. In addition, MiFID (implemented in the UK by amending existing legislation) requires that:
   - proper due diligence on the CSP's finances and expertise is carried out;
   - the CSP supervises its performance, manages associated risks and discloses any developments which may compromise the service(s) provided;
   - all records for a period of 5 years are retained;
   - a right to access data related to the services and to the CSP's premises for itself and its auditors, the FSA and any other appropriate regulator. ■

Intellectual property

1. Can the software be sub-licensed for the customer by the cloud provider?
   Yes, it depends on the terms of the licence. Where third party software is used, the third party licensor needs to grant a specific sub-licence right to the cloud service provider.

2. Are there any standard terms and conditions connected with cloud computing that are commonly used?
   Each cloud service provider develops its own standard terms and service levels to match its service and attitude to risk.

3. Is it possible to use Open Source Software for cloud computing?
   Yes. Open source is commonly used in cloud service infrastructures.

4. Are there any civil sanctions for putting material protected by Intellectual Property Rights into the cloud?
   There is no separate body of intellectual property law that relates only to cloud computing; the general principles and civil sanctions of intellectual property law apply, including injunctions.

5. Are there any criminal sanctions for putting material protected by Intellectual Property Rights into the cloud?
   There is no separate body of intellectual property law that relates only to cloud computing; the general principles and criminal sanctions of intellectual property law apply.

6. Can Internet Service Providers be held liable for infringing material placed in the cloud by their users? If yes what are the possible sanctions for the ISP?
   It is possible that the cloud service provider could be liable for intellectual property right infringement. That includes assisting a third party in distributing infringing material, especially if the cloud service provider has knowledge or reason to believe that the material in question is infringing.

7. Is there any notice-and-takedown procedure that may oblige ISPs to remove infringing material from the cloud? If yes, is the ISP also obliged to inform any authorities about the infringing act of the end user?
   There is no legislation specifically enforcing a takedown procedure. It is considered best practice for cloud service providers to implement their own notice-and-takedown procedures to mitigate the liability risks (see Q6 of this section). ►

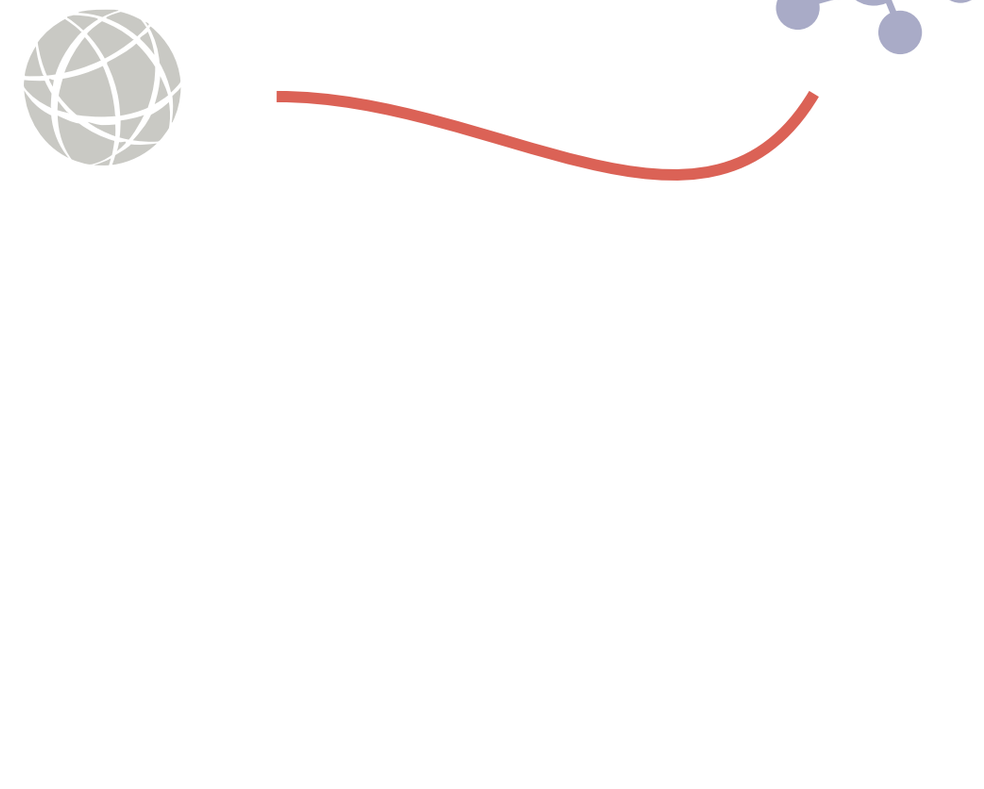
8. Are there any other special Intellectual Property law issues that can be relevant to cloud computing (e.g. unusual termination of the license provisions)?

Although cloud computing contracts relate to the provision of services rather than to the supply of software to customers, appropriate software licences may need to be granted to the customer to enable them to legally and correctly use the necessary software without the risk of copyright infringement.

Recent decisions at the European Court of Justice may impact the ability of cloud providers to restrict customers from developing functionally equivalent versions of the cloud service (provided the code itself is not copied). ■

International issues

1. Do you have specific provisions which would allow for disclosures of data from the cloud service to US (or other non-EU) law enforcement authorities in order to meet US/non-EU laws (e.g. the US Patriot Act)?
   No. The general provisions of law apply. ■



Liability issues

1. In the case of data loss in the cloud – who is responsible and what are the potential sanctions?
   Subject to mandatory consumer and data protection rules, which party is ultimately liable and what the sanctions are will be set out in the relevant contract between the parties. In addition to contractual liabilities, the ICO and the FSA have powers to fine bodies for data breaches/losses. The FSA has imposed heavy fines on financial institutions for data breaches/losses.

2. Are there any prohibitions on limitation of liability that can be relevant for cloud computing?
   Yes. The general rules on exclusions of liability apply (e.g. standard form and consumer contracts must be reasonable pursuant to the Unfair Contract Terms Act and the Unfair Terms in Consumer Contracts regulations).

3. Are there any kind of binding norms in context of warranties that may be relevant for cloud computing?
   Yes the general rules on statutory implied warranties will apply, together with the constraints on the exclusion of these warranties.

4. What will happen in the case of insolvency/bankruptcy of the cloud computing provider? What are the potential risks and who is liable?
   The cloud users will in general be unsecured creditors and have no special grounds to recover their data. This is no different to the insolvency/bankruptcy of any other entity under UK law. ■

Who owns the data?

1. Who is the owner of the data that is placed in the cloud?
   There is no ownership right in data under English law. Normal rules relating to the ownership of intellectual property rights and confidentiality of data will apply.

2. Who is the owner of the data placed in the cloud and then modified somehow by the tools available in the cloud (e.g. formatted by the open program in the cloud)? Who is also the owner of copies of documents placed in the cloud (e.g. copies of sent e-mails)?
   Normal rules relating to the ownership of intellectual property rights in data will apply. The person who makes the arrangements for the creation of the work will normally be the first owner of the rights. ■

Public sector and the cloud

1. Are public bodies looking at cloud computing for their own needs?
   Yes, central government actively promotes cloud adoption. The Cabinet Office has set up the G-Cloud framework for public bodies to buy cloud services without running full competitive procurements. Other Government departments are looking to introduce cloud services into their existing outsourcing arrangements.

2. Is there any kind of 'Government Cloud' operating? Do you know if any public institution is operating using cloud computing services?
   The Government has decided against building its own cloud but has established a G-Cloud framework through which suppliers can provide cloud services to the public sector. The public sector is already using a wide range of cloud services (particularly at Local Authority and schools level).

3. Are there any best practice guides or other instructions dedicated to cloud computing services and published by public institutions?
   There is a wide array of published guidance from public bodies (as part of G-Cloud).

4. Are there any public initiatives that are trying to explain the opportunities and risks connected with cloud computing?
   The Government ICT strategy includes cloud as a key component.

5. Are there any procurement models for sector specialised cloud computing services approved by the government?
   The Cabinet Office has set up the G-Cloud Framework agreement.

6. Who is or would be the responsible regulator for cloud services?
   There is no cloud regulator as such. The ICO has responsibility for data protection matters and the FSA for cloud services adopted by financial institutions. OFCOM is responsible for communication and broadcasting aspects.

7. Are there any special obligations connected with state security/safety that may be relevant for potential cloud services providers in this area?
   Regulation of Investigatory Powers Act (RIPA) establishes rules around data retention and provision of information to authorities. ■

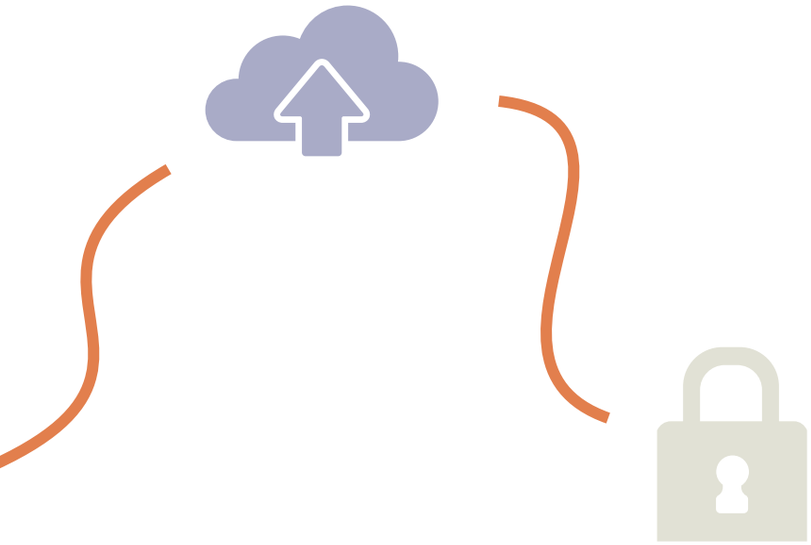
Security issues

1. Are cloud services providers free from content filtration or censorship obligations?
   There is no mandatory / general filtering or censorship of content in the UK. Where the services amount to broadcasting the general rules apply.

2. Is there any obligatory law for cloud services providers requiring them to ensure the security of data?
   See the Data Protection section for regulations relating to personal data. There are no generic regulations in relation to data security more generally. ■

Some of our experience in cloud computing

Bird & Bird has assisted many well-established and start-up clients and public sector organisations to move to the cloud both locally and internationally, across a range of jurisdictions. We will help you to overcome any legal issues you may face, such as data protection, compliance and regulation or procurement.



Helping a US based company move to the Cloud in 20 EMEA countries

Our client, a major US headquartered multinational company, decided to procure and implement a global cloud computing solution, including moving their email and HR systems to cloud based solutions. They sought a practical solution to the regulatory issues raised on both the telecommunications and sensitive data aspects of the offering.

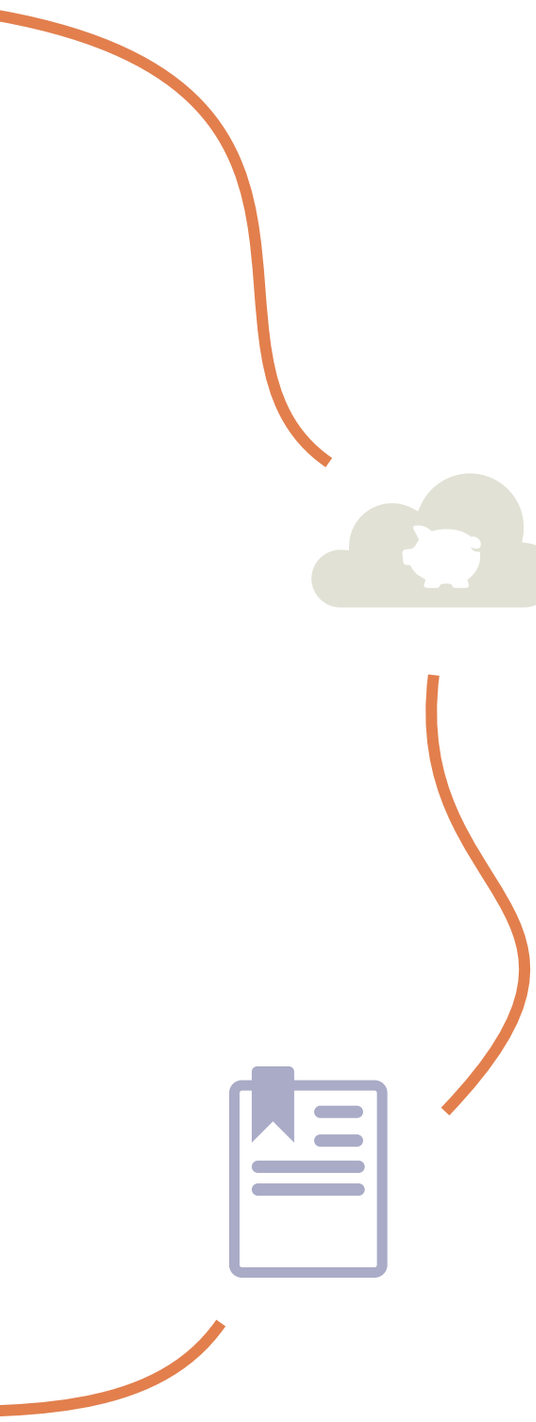
Working closely with our client, we helped them to evaluate their options and identify appropriate solutions across 20 EMEA jurisdictions. We initially focussed on:

- The general permissibility and local data protection requirements of cloud computing.
- The issues arising from providing telecommunication services outside of the EU within a cloud solution.
- The transfer of, and access to, health and other sensitive data to the US through the cloud and the additional security and other requirements that this entailed.

Having reviewed these findings with our client, we helped them to ensure that their solution would meet the compliance requirements by:

- Determining the most practical structure for the internal data processing agreements, based on EU standard contract clauses (SCC).
- Implementing an efficient, effective strategy to minimise the impact on BAU; ensure uniform employee notifications and timely filings to data protection authorities.
- Advising on their agreements with the third party cloud providers, including drafting practical language for the required amendments to the standard agreements.

Acting as a one-stop-shop, we provided a seamless service across Europe and beyond, providing practical, uniform solutions for complex scenarios. Drawing upon our extensive experience of advising cloud providers and customers, national governments and industry associations, we are able to work with our clients to deliver innovative, pragmatic solutions to achieve their business objectives. ►



Supporting the UK Government as they implement their G-Cloud Programme

The UK Cabinet Office and Government Procurement Service are putting into place the third iteration of the G-Cloud framework, with an online cloudstore offering services from over 300 companies. The G-Cloud Programme aims to improve public sector IT services whilst realising significant savings and efficiency benefits. The deployment of cloud services within a public sector context constrained by EU procurement laws and a reliance on large scale IT outsourcing arrangements is as complex as anything happening in the IT sector right now.

Bird & Bird advised on the programme between 2010 and 2012 during strategy and conception phases. This demonstrates our commitment to enabling and shaping the IT market place for the public sector and beyond, engaging meaningfully at the strategic and transaction level on extremely complex areas of IT and policy. This is an exciting programme at the forefront of innovation in the development of legal and commercial thinking within the IT sector, an area which plays to our history of acting at the leading edge of technology.

Highlights of the support we have provided to the G-Cloud programme include:

- Having a senior associate appointed to act as the industry co-lead for the commercial strategy workstream between May 2010 and January 2012.
- Drafting a detailed options paper with a risk benefit analysis of the different contractual, procurement and commercial delivery models for pan-governmental cloud services.
- Advising on legal issues impacting the programme and allocating the risks under ICT contracts.
- Supporting on the choices that exist in creating a new market place for cloud-based services in the public sector, including accrediting suppliers and services and monitoring performance.
- Undertaking peer review of the technical, security, service delivery and programme management work stream deliverables.

The Cabinet Office has recognised G-Cloud as the future model for ICT and framework procurement and delivery for the public sector and we continue to support both Government Departments and a variety of IT suppliers on the opportunities and challenges associated with these emerging procurement and delivery models. ■

Useful links

Guidance on cloud computing

ICO DP guidance on the use of cloud computing
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Cloud Standards Customer Counsel
http://www.cloudstandardscustomercouncil.org

IBM Thoughts on Cloud
http://thoughtsoncloud.com

Cloud computing authorities

CloudTweaks
http://www.cloudtweaks.com

IEEE Cloud Computing
http://cloudcomputing.ieee.org

Cloud news sites

Cloud Buzz
http://cloudbuzz.net

Cloud Pro (articles with advice for both business buyers and IT departments)
http://www.cloudpro.co.uk

Cloud Computing Intelligence
http://cloudcomputingintelligence.com

The Cloud Circle
http://www.thecloudcircle.com

Business Cloud News
http://www.businesscloudnews.com

Cloud Tech
http://www.cloudcomputing-news.net

Cloud Tweaks
http://www.cloudtweaks.com

Blogs

Real Time Cloud
http://real-timecloud.com

Big 4 accountancy firms coverage

PWC - Cloud computing
http://www.pwc.co.uk/technology/publications/cloud-computing.jhtml

Deloitte - Cloud computing
http://www.deloitte.com/view/en_US/us/Industries/technology/center-for-edge-tech/tech-cloud-computing/index.htm

KPMG - Tax in the cloud
http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Pages/tax-in-the-cloud.aspx

Ernst & Young - Cloud computing issues and impacts
http://www.ey.com/Publication/vwLUAssets/Cloud-computing_issues_and_impacts/$FILE/Cloud_computing_issues_and_impacts.pdf

Contact us

Want to know more about cloud in your country or moving to the cloud and need some advice? We can help you.

Roger Bickerstaff

Co-Head of International IT Group

Call me on: +44 (0)20 7905 6000

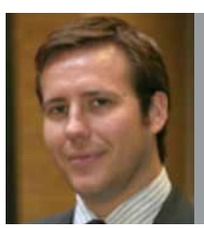
Email | Profile

Fabian Niemann

Partner

Call me on: +49 (0) 211 2005 6000

Email | Profile



Barry Jennings

Senior Associate

Call me on: +44 (0)20 7905 6000

Email | Profile

Contributors

We'd like to thank those who've contributed their legal expertise to this PDF/app.

- Czech Republic – Pavel Hejl
- Denmark – Jesper Langemark, Nis Peter Dall
- France – Stephane Leriche
- Germany – Fabian Niemann
- Hungary – Balint Halasz, Zoltan Tarjan
- Italy – Roberto Camilli, Gian Marco Rinaldi, Massimiliano Mostardini, Debora Stella
- Poland – Maciej Gawronski
- Spain – Alexander Benalal
- Sweden – Fredrik Ahlesten
- UK – Barry Jennings
- UAE – James Leeson, Nadia Barazi, Melissa Murray