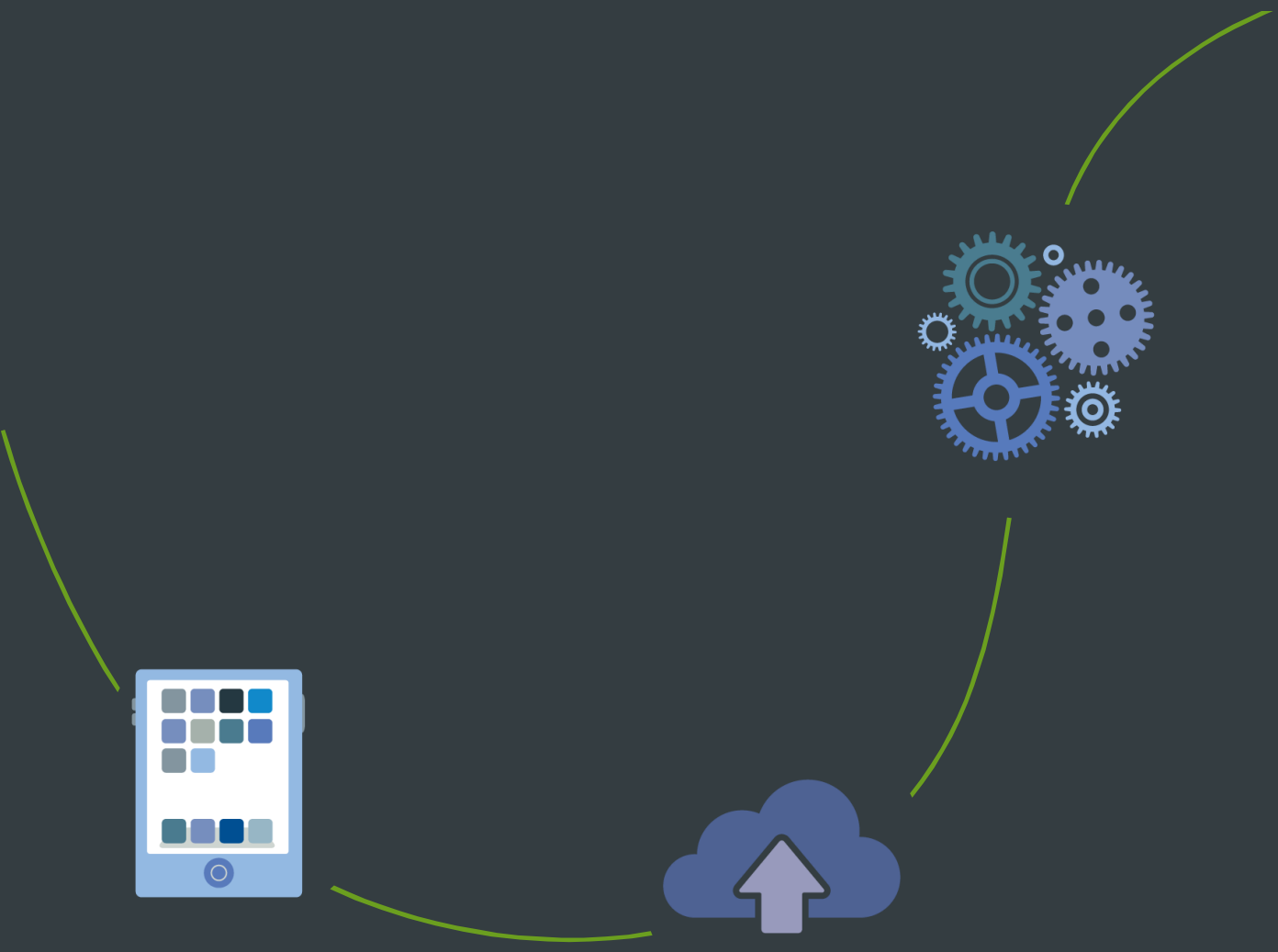
Bird & Bird

Cloud Computing and Privacy Series



January 2015

Contents

A multi-jurisdictional study

This series has been made possible thanks to the CoCo Cloud project (www.coco-cloud.eu) funded under the European Union's Seventh Framework Programme, and of which Bird & Bird LLP is a partner. Said project aims to establish a platform allowing cloud users to securely and privately share their data in the cloud.

This document collates six articles that were first published on the Bird & Bird website between 17 November and 22 December 2014. Active links to documents cited in the articles are made available in the versions published on our website.

Benoit Van Asbroeck
Partner
Brussels

Tel: +32 (0)2 282 6067

benoit.van.asbroeck@twobirds.com

Julien Debussche
Associate
Brussels

Tel: +32 (0)2 282 6044

julien.debussche@twobirds.com

Glossary

CJEU	Court of Justice of the European Union
CSP	Cloud (computing) service providers
Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
DPA	Data protection authority
EEA	European Economic Area
EHR	Electronic Health Records
ENISA	European Network and Information Security Agency
ePrivacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC
EU	European Union
GIODO	Inspector General for the Protection of Personal Data (Poland)
HSCIC	Health and Social Care Information Centre (United Kingdom)
HSP	Hosting service provider
ICO	Information Commissioner's Office (United Kingdom)
IEC	International Electrotechnical Commission
IG SIRI	Information Governance related Serious Incident Requiring Investigation (United Kingdom)
ISO	International Organisation for Standardisation
Key Member States	The ten selected EU Member States examined in the Multi-Jurisdictional Study carried out in the framework of the CoCo Cloud project, *i.e.* Belgium, Czech Republic, Denmark, Finland, France, Germany, Italy, Poland, Spain and the United Kingdom
PECS provider	Provider of an electronic communications service
US	United States

The general legal framework

Although cloud computing services constitute advancement in information and communication technologies, this phenomenon of remote services is far from novel. Nevertheless, cloud computing has undoubtedly attracted particular attention in recent years due to the development of new and innovative large-scale business models, but also due to technological evolution such as high-speed communications.

Consequently, interest in cloud computing has significantly increased in the past few years and led to numerous scientific studies regarding various aspects, including technical, commercial and legal ones. Public authorities in the EU have therefore been prompted to position themselves on the adoption of this new technological evolution. As a result, we observe that cloud computing is acknowledged by authorities at EU level and in all Key Member States.

Cloud computing at EU level

The EU has shown particular interest in cloud computing in the framework of its digital agenda. In September 2012, the European Commission adopted a strategy for "*Unleashing the Potential of Cloud Computing in Europe*".[1]

The strategy - which is the result of an analysis of the overall policy, regulatory and technology landscapes - encourages the use of cloud computing across all economic sectors. It sets out the most important and urgent additional actions, and identifies three key actions:

- safe and fair contract terms and conditions;
- cutting through the jungle of standards; and
- establishing a European cloud partnership.

Following the 2012 Strategy of the EU Commission, the Parliament adopted a Resolution on 10 December 2013.[2] The Resolution is based on the digital agenda and the various existing EU instruments in the field of information technology. More importantly, it puts forth the main challenges and examines various issues such as:

- the cloud as an instrument for growth and employment;
- the EU market and the cloud;
- public procurement, and procurement of innovative solutions;
- standards;
- consumers and the cloud;
- intellectual property, civil laws etc.; and
- data protection, fundamental rights and law enforcement.

Finally, the EU Commission has more recently published other documents relating to cloud computing, including, in July 2014, the Staff Working Document Report on the Implementation of the Communication "*Unleashing the Potential of Cloud Computing in Europe*", accompanying the Communication entitled "*Towards a thriving data-driven economy*".

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Unleashing the Potential of Cloud Computing in Europe' COM (2012) 529 final (Commission Communication (2012) 529).

[2] European Parliament resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe (2013/2063(INI)).

Cloud computing at national level

All Key Member States acknowledge cloud computing one way or another through various publications, and in particular guidance.

However, it shall be noted that, putting aside any specific publication in the field of privacy and data protection – which is undoubtedly the topic of greatest concern and thus most discussed (dealt with in the next chapter) – few countries have published general guidance on the subject of cloud computing. In addition, we note that for those countries that have published such type of guidance, the issues examined relate to specific aspects and in many instances to the use of cloud computing by public administrations.

More specifically, the publication of general guidance by public authorities regarding cloud computing varies between Member States (excluding any privacy and data protection guidance). Our analysis has enabled to identify the following four different situations:

Member State(s) providing no or very little guidance on cloud computing in general.

Among such countries we find the **Czech Republic**, where public authorities have not published any actual guidance but have nevertheless shown interest in cloud computing such as in the strategic document issued by the Czech Government entitled "*Digital Czech Republic v2.0: Road to the Digital Economy*". The situation in **Finland** is similar, where there is not much guidance concerning cloud computing specifically. The only guidance published by Finnish authorities concerns mainly questions closely related to cloud services such as outsourcing of the processing of personal data. Also, in the **United Kingdom**, it is interesting to note that even though there is no specific guidance on cloud computing, public authorities have nevertheless been active in this context, publishing in particular the so-called ICO Guidance, which is however limited to data protection (addressed in the next chapter).

Member State(s) providing guidance on specific issues only (excluding data protection).

Some Key Member States have not published general guidance applicable to cloud computing but rather guidance on particular subjects. Firstly, in **Poland**, the Financial Supervision Commission (the "KNF") has adopted in January 2013 "*Recommendation D*" on management of information technology and ICT environment security in banks and credit institutions operating on the Polish market. In **Germany**, The German Federal Agency for Security in Information Technology[3] published in February 2012 a guidance document entitled "*Security Recommendations for Cloud Computing Providers*". In addition, there are non-binding guidelines on cloud computing by German industry associations, namely the German internet association eco of December 2010 and the German IT association BITKOM of October 2009.

Member State(s) providing guidance on or acknowledgment of public-related cloud computing.

In **Italy**, the Agency Digital Italy ("AgID"), which is the Italian public authority competent for digitalization of Italian administration, issued documents relating to the adoption of cloud computing by public authorities, and in particular the document entitled "*Features of electronic systems for cloud in public administration*". It covers (i) possible cloud services to be adopted by public administration; (ii) a framework of architectures to be adopted for eGovernment services; (iii) the role of public administration in cloud computing; (iv) a description of the "OpenStack" project as acceptable standard for public administration; (v) IaaS, PaaS and SaaS in relation to some types of public tenders; (vi) data centre for public administration cloud services; (vii) conformity, interoperability, operating and security, management, resilience requirements of cloud in public administration; and (viii) classes of services.

Member State(s) providing general guidance applicable to the public and/or private sectors.

Finally, few Key Member States provide for general guidance that is not only destined to the public sector but also to private entities. These include for instance **Belgium**, where the Belgian Federal Public Service Economy published a study on cloud computing entitled "*An economic opportunity for Belgium*" (the "Unisys report") and which (i) offers a substantive definition of cloud computing; (ii) covers the opportunities and risks of cloud computing; and (iii) discusses the legal framework applicable to cloud computing. Similarly, in **France**, The Network and Information Security Agency ("ANSSI") published in December 2010

[3] Bundesamt für Sicherheit in der Informationstechnik – "BSI".

guidance on the outsourcing of information systems, and subsequently, on cloud computing.

In **Denmark**, the Agency for Digitisation has issued several guides and papers on cloud computing, such as in particular "*Cloud computing and the legal framework - guidance on legislative requirement and the contractual environment related to cloud computing*", "*Cloud audit and assurance initiatives*", "*New digital security models – discussion paper*" or "*Memorandum on legislation and rules that complicates the use of cloud computing in the public sector*".

Finally, public authorities in **Spain**, published two main guides relating to cloud computing. In the first place, they issued the Spanish National Interoperability Framework, setting out the principles and guidelines for interoperability in the exchange and preservation of electronic information by the Public Administration. In addition, they circulated the "*Guide for companies: security and privacy of cloud computing*" of 2011 ("INTECO Guide"). The latter guide shows the different levels of clouds, the way in which the services are deployed, as well as the legal framework of reference, looking closely at the main implications regarding security and privacy, and the keys to ensuring success in the use of cloud computing services.

The data protection legal framework

It clearly results from our cross-jurisdictional analysis of Key Member States that the issues of privacy and data protection are of paramount importance when considering cloud computing. This is logical as the provision of IT services over the Internet leads in many instances to the processing of personal data. This poses recurrent issues relating to the applicable law, the determination of the controller and the processor and their corresponding roles, cloud services contracts put in place, and the international transfer of data.

Without aiming to reiterate the legal analysis provided in many academic and learned studies and articles, the following sections examine whether EU and national authorities provide specific guidance or decisions on the subject of cloud computing and privacy.

Guidance on cloud computing and data protection provided by public authorities

EU guidance

The Working Party has issued numerous opinions on different aspects, many of which are relevant to cloud computing.

Among such opinions issued by the Working Party, the following are particularly relevant:

- Opinion 05/2014 on anonymisation techniques onto the web[4] (discussed in the fourth chapter);
- Opinion 03/2014 on personal data breach notification[5] (discussed in the fifth chapter);
- Opinion 03/2013 on purpose limitation[6];
- Opinion 15/2011 on consent[7];
- Opinion 8/2010 on applicable law[8]; and
- Opinion 4/2007 on the concept of personal data.[9]

More importantly, the Working Party published an opinion dedicated to cloud computing.[10] Opinion 05/2012 on Cloud Computing, adopted on 1 July 2012, analyses all relevant issues for CSPs operating in the EEA, and their clients, specifying all applicable principles from the Data Protection Directive and the ePrivacy Directive where relevant.[11]

National guidance

In addition to the EU general and specific guidance applicable to cloud computing, the question arises as to whether national DPAs have adopted specific guidance on the applicability of their local data protection legislation to cloud computing.

Most local DPAs have issued data protection guidance dedicated to cloud computing. Only very few DPAs have not issued cloud-specific data protection guidance, including **Belgium**, **Denmark** (there are however cloud–specific decisions of the Danish DPA, see below), **Finland** and **Poland**.

Also, those countries that have issued general guidance on cloud computing (see our first chapter) all cover data protection aspects (e.g., **Belgium** and **Denmark**). Moreover, the absence of

4 Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques onto the web' adopted on 10 April 2014 (WP216).
5 Article 29 Working Party, 'Opinion 03/2014 on Personal Data Breach Notification' adopted on 25 March 2014 (WP213).
6 Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation', adopted on 2 April 2013 (WP203).
7 Article 29 Working Party, 'Opinion 15/2011 on Consent' adopted on 13 July 2011 (WP187).
8 Article 29 Working Party, 'Opinion 08/2010 on Applicable Law' adopted on 16 December 2010 (WP179).
9 Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' adopted on 20 June 2007 (WP136).
10 In addition, it shall be mentioned that the Berlin International Working Group on Data Protection in Telecommunications published on 24 April 2014 a Working Paper on Cloud Computing - Privacy and data protection issues – "Sopot Memorandum".
11 See Article 29 Data Protection Working Party, 'Opinion 05/2012 on Cloud Computing' adopted on 1 July 2012 (WP 196), 1.

dedicated guidance on data protection in a cloud environment does not mean that other guidance published by local DPAs in such countries on more general topics does not apply to cloud computing, in just the same way that the data protection guidance at EU level is also relevant to cloud computing. Several other countries provide tailored guidance by local authorities on privacy and data protection in a cloud environment.

In general, this national guidance does not provide divergent views from the ones set out in the aforementioned Working Party Opinion 05/2012 on cloud computing.

For instance, in the **Czech Republic** the Czech Data Protection Office issued on 7 August 2013 its official position on the Protection of Personal Data within Cloud Computing Services. Such document, which almost entirely corresponds to the Working Party Opinion 05/2012, includes (i) definitions of the terms "Cloud Computing", "IaaS", "SaaS", "PaaS", "Public cloud", "Private cloud" and "Hybrid cloud", (ii) definitions of the data controller and the data processor, (iii) explanation on how the adequacy of the level of protection is assessed, (iv) rules regarding the transfer of personal data outside Czech Republic, and (v) explanation of Standard Contractual Clauses and Binding Corporate rules.

In **Spain**, the Spanish DPA has also provided guidance in 2013 on privacy and cloud computing with two specific guides: the "*Guide for clients using Cloud computer services*" and the "*Guide for Cloud service providers*".

The major findings of the Spanish Guidelines are summarised as follows:

- CSPs shall be considered as data processors;
- The customer shall be informed of the identification of services and the outsourcing company (including the country in which it develops its services if international data transfers are to take place);
- The customer can make decisions as a result of the intervention of subcontractors, *i.e.* it may terminate the agreement or refuse that the sub-contractors are appointed; and
- The CSP and subcontractors shall enter into a contract that includes guarantees equivalent to those included in the contract with the customer.

In the **United Kingdom**, the ICO published on 27 September 2012 a set of guidelines for businesses in relation to cloud computing. In addition to addressing the application of the rules contained in the Data Protection Act 1998 to the processing of information in the cloud, the ICO guidance runs through the three main types of cloud deployment models (private, community and public) and considers which role will be filled by the customer and provider. As the cloud customer will be making the decisions on the purposes and manner in which the data are processed, it will generally be the data controller and therefore it will be ultimately liable for compliance with the Data Protection Act. However, the precise role of the CSP should be reviewed on a case-by-case basis to determine whether it is processing personal data to such an extent that it could be operating as a data controller in its own right. The ICO guidance then highlights the key areas, which should be considered by organisations looking to move to the cloud, such as (i) the formalisation of the relationship, (ii) the auditing/monitoring of the CSP, (iii) the protection of data (with for instance an encryption algorithm), (iv) data retention and deletion, (v) the further processing, and (vi) the use of cloud services from outside the UK.[12]

National case-law relating to cloud computing and data protection

In addition to the guidance of the Working Party and several national DPAs across the EU, any judicial and administrative decisions on the matter are also of importance.

Where a particular decision does not specifically concern cloud computing it may still apply to such situation. It is therefore necessary to take into consideration the entire body of case-law available. This is for instance the case at EU level with the CJEU. The CJEU has currently not issued any decision on data protection and cloud computing. It remains that several decisions are worth being taken into account. This is the case for instance for the *Lindqvist* (C-101/01), *Google Spain* (C-131/12) and *Heinz Huber* (C-524/06) judgments. In this

[12] See our more detailed article on the ICO guidance at http://www.twobirds.com/en/news/articles/2012/ico-publishes-guidance-on-cloud-computing-1012.

context, it should be reminded that judgments of the CJEU apply throughout the EU.

The same logic applies in each Member State, where local decisions of the DPAs or the administrative and judicial courts may be relevant.

Our in-depth analysis of the current legal situation in Key Member States shows that two countries have cloud-specific decisions: Denmark and Spain.

Case-law in Denmark

Since 2011, the DPA in **Denmark** (*Datatilsynet*) has in a few cases dealt with cloud computing from a data protection perspective. In particular, topics relating to the obligations as data controller and data processor, security issues and transfer of personal data to third countries outside the EEA are covered in several decisions related notably to Dropbox, a driver's license system, Google Apps and Microsoft's Office 365.

More specifically, the Google Apps case with Odense Municipality is probably the most well-known case brought before the Danish DPA. The Danish DPA rejected Odense Municipality's application to use the cloud service "Google Apps" to store data in relation to its public schools. Odense Municipality stated that data would be transferred initially to Google Ireland Limited. Google subsequently informed the DPA that it holds all data in numerous data centres worldwide, including in the US and Europe. Accordingly, data would initially be shared between Denmark and Ireland and then between Ireland and potentially every other country in which Google operates data centres (be it the US, within the EEA or others). The Danish DPA's view was that any Google data centres in the US would be covered by the EU-US Safe Harbour Framework; thus Odense Municipality was permitted to store data there as well as in Ireland. However, the Danish DPA decided it must assume that data would be transferred not only to Ireland and the US, but also to all the other countries in which Google maintains data centres, including those neither in the EEA nor the US (and thus not covered by Safe Harbour). It therefore deemed that Odense Municipality would not comply with current legislation because it was not proposing to enter into a contract based on the European Commission's standard contractual clauses with Google's individual data centres. Further the Danish DPA found that Odense Municipality had not conducted a sufficient risk evaluation, and that the data processor agreement which was to be entered with Google, did not comply with the legal requirements, most notably because it could be changed unilaterally by Google.

The other very relevant case from the Danish DPA, the Office 365 case, relates to the IT University of Copenhagen's request for use of Office 365 as e-mail solution for the University's students and employees. The Danish DPA restated the same arguments as in the Odense Municipality case but since Microsoft was more open to enter into a contract based on the European Commission's standard contractual clauses, the outcome was different. Even though the Danish DPA's decision in the Office 365 case is not a seal of approval for cloud computing in the public sector, it shows a path to follow when using cloud computing in the public sector.

Case-law in Spain

In **Spain**, the Supreme Court was compelled to examine several issues relating to claims against the Spanish Data Protection Regulation (the "Royal Decree 1720/2007" of 21 December 2007).

In its ruling of 15 July 2010, the Spanish Supreme Court dismissed the claimant's challenge as it considered that the data processor's duty to inform the data controller of its identifying data before proceeding with the subcontracting is applicable. Furthermore, it considered that the subcontractor must not only be identified, but that said identity of the subcontractor must also be notified to the client. The reason for this need to notify is that CSPs are considered to be data processors and the client is considered the data controller.

Moreover, the Spanish Supreme Court established that if third party processors are involved in the provision of cloud services, additional aspects must be guaranteed:

- The customer shall be informed of the identification of the outsourcing company (including the country where it develops its services if international data transfers are to take place);
- The customer can make decisions as a result of the intervention of subcontractors, *i.e.* it may terminate the agreement or refuse that sub-contractors are appointed;

- The CSP and subcontractors shall enter into a contract that includes guarantees equivalent to those included in the contract with the customer (back-to-back agreements).

The Spanish DPA has also applied the above criteria in other resolutions such as that regarding a Microsoft Office 365 cloud solution data transfer (9 May 2014), where it considered that the company fulfils the aforementioned requirements.

Case-law in the US

One of the areas of key concern for cloud vendors and customers currently is the interplay between EU data protection rules and laws in other countries which seemingly conflict, particularly in respect of government or court ordered access to information about individuals held on servers in the EU. Given the US origin of many of the largest cloud vendors, the size of the US market and revelations about NSA surveillance and information gathering, the position in the US continues to be watched closely.

The highest profile case is the Microsoft Warrants case, where on 31 July 2014, Chief US District Judge Loretta Preska ruled against Microsoft's appeal against a warrant to disclose emails and other records in a particular MSN email account.[13] Judge Preska ruled that the location of the data (in Dublin) was not relevant because Microsoft still "*controlled it*" and was therefore liable to provide it under warrant pursuant to the US Stored Communications Act. Microsoft decided not to comply with the order, voluntarily putting itself in contempt, and is continuing to seek ways to appeal the decision.

Apple, Cisco, Verizon and AT&T all filed Amicus briefs in support of Microsoft's appeal on the basis that finding in favour of the US Government would conflict directly with EU data protection laws. Viviane Reding, former EU Justice Commissioner, has said that "*the extraterritorial application of foreign laws (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the [European] Union*".

The case will continue but what is certain for now is that the lack of clarity and the potential conflicts of laws present real challenges for US cloud vendors and their customers or potential customers.

[13] For the magistrate's decision, see In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., __ F. Supp. 2d. __, 2014 WL 1661004 (SDNY 25 April 2014)

Security requirements and guidance

The issues related to confidentiality and security play an important role in data protection. This is even more so when considering an information technology environment, and thus when considering cloud computing. Security is therefore at the forefront of current issues that private but also public stakeholders must face today.

Legal security requirements

It results from our study that security is currently one of the most regulated topics in the field of data protection, as well as in the field of telecommunications.

The importance given to security is constantly increasing and is expected to keep playing a central role in the future. In this respect, we note in particular the upcoming data protection Regulation, which focuses notably on security aspects. We also note other EU initiatives such as in the field of cybersecurity, where the adoption of a Cybersecurity Directive is on the horizon.[14]

EU requirements

It shall be reminded that at **EU level**, the main requirements related to security are regulated by Article 17 of the Data Protection Directive. In a nutshell, it requires that the controller guarantees the security of the personal data and protects their integrity. In order to do so, the controller (or its processor where appropriate) must implement the 'appropriate' technical and organizational measures that are necessary to protect the personal data from accidental or unlawful destruction, accidental loss, as well as from alteration, access and any other unauthorized processing of the personal data "*in particular where the processing involves the transmission of data over a network*".[15]

More specifically, the controller shall adopt an internal security policy and implement technical and organizational measures to physically protect the premises where the information is stored, as well as the technical protection against hackers and unauthorized use of the system. The EU data protection legislation does not provide more details regarding the security obligation, but specifies nonetheless that the measures shall take into consideration the state of the art and the cost of their implementation, and that such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Other EU instruments provide for similar obligations. Article 4(1) of the ePrivacy Directive imposes a security duty on PECS providers.[16]

It derives from the foregoing that a risk-based approach is imposed on controllers (and processors) or PECS providers, requiring a continuous risk assessment. Such assessment shall reflect the nature of the data (for instance whether it is 'sensitive data'), the possible threats (technical and others) and the prejudice that could result from a security breach.

National requirements

The various legal provisions at EU level are formulated in general terms. Member States therefore have a relatively high level of discretion when implementing such instruments into their legal system.

[14] See in particular the European Parliament legislative resolution of 13 March 2014 on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)) (Ordinary legislative procedure: first reading); See our latest article on this topic at http://www.twobirds.com/en/news/articles/2014/global/european-cybersecurity-directive-moves-closer-to-becoming-a-reality.

[15] Data Protection Directive 95/46/EC, Article 17(1). [Emphasis added].

[16] Article 7 of the Data retention Directive 2006/24/EC also required providers of publicly available electronic communications services or of a public communications network to respect certain security principles with respect to data retained in accordance with the Directive. Directive 2006/24/EC has however been deemed to be invalid by the CJEU (8 April 2014, joined cases C-293/12 and C-594/12).

Our examination of the Key Member States has shown that legislators have taken different approaches. Whereas some of them have transposed the EU provisions rather faithfully (e.g., **the United Kingdom**), some others are more prescriptive.

We note nonetheless that several Member States provide for interesting details as to the measures that shall be put in place by the data controller (or its processor where appropriate) or the PECS provider.

For instance, although there is no specific law in **Poland** relating to cloud computing services, CSPs must comply with the regulations related to personal data protection and sector specific regulations or soft law, if applicable (e.g., financial services or in the health sector).

With respect to personal data protection, both the controller and the processor need to comply with very detailed regulations regarding technical and organisational measures set forth in the Polish Data Protection Act (Articles 36-39a) and in the Regulation by the Polish Minister of Internal Affairs and Administration as Regards Personal Data Processing Documentation and Technical and Organisational Conditions Which Should be Fulfilled by Devices and Computer Systems Used for Personal Data Processing ("Security Regulation").

In **Germany**, there is also no specific law aimed at cloud computing services. CSPs must nevertheless comply with Section 9 of the German Data Protection Act, which provides obligations to implement certain security measures listed in an annex to the law. Said list is quite comprehensive and all elements must be fulfilled.[17]

The situation in **Spain** is similar to that observed in Germany. In the absence of any specific law aimed at cloud computing services, the general security measures must be implemented depending on the level of sensitivity of the personal data processed. The Spanish Data Protection Regulation establishes a catalogue of security measures to be complied with by data controllers and data processors, depending on the "basic", "medium" or "high" level.

[17] For more practical details on the situation in Germany, read "Praxishandbuch Rechtsfragen des Cloud Computing" by Fabian Niemann and Jörg-Alexander Paul (more information at http://www.twobirds.com/de/news/books/p/praxishandbuch-rechtsfragen-des-cloud-computing).

General security guidance

In view of the importance attributed to security at EU and national levels, several authorities have published guidance in order to provide more general and practical guidelines on how to implement the, often vague, legal provisions. In this section, we provide an overview of some of the most interesting initiatives in this respect, excluding however particularities regarding the health sector (addressed in the sixth chapter).

EU guidance

ENISA[18] published numerous reports, some of which are specifically dedicated to cloud computing.

Furthermore, on 5 November 2001, the Working Party published an Opinion on the Commission Communication on *"Creating a safer information society by improving the security of information infrastructures and combating computer-related crime"*. This outdated opinion constitutes at present the Working Party's sole attempt to address security issues.

National guidance

In **Belgium**, the DPA has published a document entitled "*reference measures on the security of data*", which details ten areas of action regarding data security. In June 2012, the DPA also published guidelines for information security based on the ISO/IEC 27002 structure.

In **Germany**, the annex to Section 9 of the German Data Protection Act provides obligations to implement certain security measures.[17] In addition, some German DPAs and industry associations provide guidance on how to include these technical measures in data processing agreements. Furthermore, Section 11 of the German Data Protection Act enumerates the items that must be specified in a data processing agreement, such as *inter alia* the subject and the duration of the agreement; the type of data and group of persons

[18] ENISA is not specifically set up to implement security measures in the field of data protection and telecommunications but has a broader mission in order to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union.

affected; and the technical and organizational measures to be taken.

In **Poland**, in 2007, GIODO published "*The ABC of rules on personal data security processed by means of IT systems*". It includes a brief description of the detailed Polish requirements as to the security and organizational measures set forth in the Security Regulation, including some guidelines related to hosting. It comprises a detailed description of what the Security Policy and the Instruction of the Security Management System should look like, basic requirements regarding functionality of the security systems and explanations as to the levels of security (basic, medium, high).

In **Spain**, in addition to the general security measures that must be implemented depending on the level of sensitivity of the personal data processed, the Spanish DPA published a guide for the drafting of the security document. More particularly, the guide covers security measures (including concept and use) and the security document (including concept and template). The guide lists the security measures required by Spanish data protection law, along with implementation strategies, including, (i) an explanation of the different security levels and their corresponding security measures; (ii) a template for the drafting of the compulsory internal security document; and (iii) a questionnaire to automatically evaluate applicable security levels and their level of compliance.

Specific security guidance and standards related to cloud computing

In addition to the aforementioned general guidance on security, some authorities at international or EU level and in the Key Member States provide for specific guidelines on security in a cloud environment. This is in many instances provided in the framework of general guidance related to cloud computing.

International ISO standards

Standards serve as an increasingly important tool for cloud customers to determine whether a cloud computing solution is secure and reliable. Up until recently, CSPs could only rely on existing general certification schemes to assure compliance with legal requirements.

However, a cloud-specific voluntary certification scheme saw the light of day in July 2014, when the ISO and the IEC teamed up for the publication of ISO/IEC 27018. This code of practice for data security directed at public CSPs is based on the 2012 European Cloud Computing Strategy as well as on the Working Party's Opinion 05/2012 on Cloud Computing. It further elaborates the general IT-related standards addressing data security, such as ISO/IEC 27001[19] and ISO/IEC 27002.[20]

ISO/IEC 27018's objectives are fourfold: (i) to function as a tool for CSPs in their compliance with the applicable data protection obligations; (ii) to allow CSPs to be more transparent vis-à-vis cloud service customers; (iii) to assist both CSPs and customers in the negotiation of cloud service contracts; and (iv) to provide cloud service customers with audit mechanisms.

It aims to achieve said objectives by *inter alia* requiring the CSPs certified under ISO/IEC 27018 to:

- Process personal information in accordance with the customer's instructions;
- Process personal information for marketing purposes only with the customer's express consent;
- Disclose personal information to law enforcement authorities only when legally obliged to do so;
- Disclose to the customer the identity of any subcontractors as well as the locations where personal information may be processed, prior to entering into a cloud services contract;
- Implement a policy for the return, transfer or erasure of personal information.

More recently, ISO/IEC 17788 and ISO/IEC 17789 were adopted, respectively providing for a common basic terminology and an architectural framework related to cloud computing.

EU guidance

[19] ISO/IEC 27001:2013, Information Technology – Security techniques – Information security management systems – Requirements.
[20] ISO/IEC 27002:2013, Information technology – Security techniques - Code of practice for information security controls.

ENISA published reports on security in a cloud computing environment. We highlight in particular the following, along with a brief description provided by ENISA:

- "*Cloud Computing: Benefits, risks and recommendations for information security*" (20 November 2009): outlines some of the information security benefits and key security risks of cloud computing. The report also provides a set of practical recommendations.
- "*Cloud Computing Information Assurance Framework*"(20 November 2009): provides a set of assurance criteria designed to assess the risk of adopting cloud services, to compare different CSP offers, to obtain assurance from the selected CSPs, and to reduce the assurance burden on CSPs.
- "*Security & Resilience in Governmental Clouds: Making an Informed Decision*": identifies a decision-making model that can be used by senior management to determine how operational, legal and information security requirements, as well as budget and time constraints, can drive the identification of the architectural solution that best suits the needs of their organisation.
- "*Procure Secure: a guide to monitoring of security service levels in cloud contracts*" (2 April 2012): a practical guide aimed at the procurement and governance of cloud services. This guide provides advice on questions to ask about the monitoring of security. The goal is to improve public sector customer understanding of the security of cloud services and the potential indicators and methods which can be used to provide appropriate transparency during service delivery.
- "*Good Practice Guide for securely deploying Governmental Clouds*" (13 November 2013): identifies the Member States with operational government Cloud infrastructures and underlines the diversity of Cloud adoption in the public sector in Europe. Moreover, through this document, ENISA aims to assist Member States in elaborating a national Cloud strategy implementation, to understand current barriers and suggest solutions to overcome those barriers, and to share the best practices paving the way for a common set of requirements for all Member States.
- "*Incident Reporting for Cloud Computing*" (9 December 2013): analyses how CSPs, customers in critical sectors, and government authorities can set up cloud security incident reporting schemes.
- "*Critical Cloud Computing-A CIIP perspective on cloud computing services*" (14 February 2013): looks at cloud computing from a Critical Information Infrastructure Protection ("CIIP") perspective and looks at a number of relevant scenarios and threats, based on a survey of public sources on uptake of cloud computing and large cyber-attacks and disruptions of cloud computing services.

The Working Party Opinion 05/2012 on Cloud Computing (see also our second chapter) comprises a section entitled "*Technical and organisational measures of data protection and data security*", which applies in addition to the ENISA "*Cloud Computing Risk Assessment*" report. The Working Party highlights the fact that "*in addition to the core security objectives of availability, confidentiality and integrity, attention must also be drawn to the complementary data protection goals of transparency, isolation, intervenability, accountability and portability*". The document analyses such questions more in depth.

National guidance

In **Germany**, the guidance paper "*Orientierungshilfe Cloud Computing*" of 26 September 2011 (updated version 2.0 of 9 October 2014) of the working groups "technology" and "media" of the German DPAs contains comprehensive recommendations on cloud computing, including rules on security which are similar to those in the Working Party Opinion 05/2012.

Furthermore, the guidance of the German Federal Agency for Security in Information Technology entitled "*Security Recommendations for Cloud Computing Providers*" of February 2012 mainly deals with IT security related topics, such as security management; security architecture (data centre, server, network, application, platform, data, encryption); rights management; control options for users; monitoring and security incident management; business continuity management; portability and interoperability; security testing and audit; requirements of personnel of providers; drawing up agreements, incl. transparency and SLAs; data protection; and compliance.

The paper includes check-boxes and different levels of (security) requirements depending on the sensitivity of data stored in the cloud. It includes three different levels, which are however only described in general:

- Category B (basic requirement) includes those requirements which are basic for all CSPs;
- Category C+ (high confidentiality) includes additional requirements where data with a high protection requirement in terms of confidentiality is to be processed;
- Category A+ (high availability) includes additional requirements where services with a high protection requirement in terms of availability are to be considered.

In **Spain**, while there is no explicit guidance on security in the cloud, such topic is covered in the following documents:

- The 2013 cloud-related guides of the Spanish DPA, one for users and one for providers;
- The "*Guide for companies: security and privacy of Cloud computing*" of 2011 ("INTECO Guide"), published by the Ministry of Industry, which examines closely the main implications as regards security and privacy, and in particular covering security in the cloud, including security on the part of the CSP and on the part of the client.

A legal perspective on data anonymisation

The issue related to rendering data anonymous or pseudonymous has been a hot topic in the past few years and in particular with the emergence of new phenomena such as big data, the Internet of things (IoT) or cloud computing. Indeed, they all require at some point taking into account issues relating to privacy and the processing of personal data. It is therefore only natural that there has been a growing interest in techniques that would allow eliminating or at least mitigating the risks related to the processing of such data.

In this chapter we examine to what extent anonymisation, and in some cases even pseudonymisation, could play a role in a cloud computing environment. Thereto, in the following sections we examine how anonymisation and pseudonymisation techniques are acknowledged in the EU and in certain Key Member States.

Anonymisation: a new concept in the EU?

In spite of the relatively recent interest in the issues related to anonymisation, the Data Protection Directive already addressed the question in 1995, putting forth the following logic under Recital 26:

- The principles of data protection must apply to any information concerning an identified or identifiable person;
- To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person;
- The principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

Although the above provides an interesting basis, it is not sufficient to understand precisely what encompasses the notion of 'anonymisation' and the related concept of 'pseudonymisation'.

Anonymisation and pseudonymisation: blurred concepts?

Anonymisation is a process by which information is manipulated (concealed or hidden) to make it difficult to identify data subjects.[21] This can be done either by deleting or omitting "identifying details" or by aggregating information.[22] Pseudonymisation, on the other hand, involves replacing names or other direct identifiers with codes or numbers.[23]

One possible technique of pseudonymisation is encryption. Encryption is the process of changing a plain text into unintelligible code.[24] The use of encryption has been tipped as essential for the wider adoption of cloud computing services.[25] In that respect, it has been argued that as far as the encryption is effective, which requires a strong encryption algorithm and a strong encryption key that is kept secure, the data may not be considered personal in the hands of the CSP. Indeed, the CSP may not know that encrypted data is stored on its (or its sub-provider's) infrastructure, considering it is uploaded by the customer in self-service fashion.[26] Nevertheless, in its 'Opinion 05/2014 on anonymisation techniques onto the web', the Working Party takes a stricter approach (see below).

---

[21] Paul Ohm, 'Broken Promises of Privacy: responding to the surprising failure of anonymisation', UCLA Review 57, 2009, 1707.

[22] Hon W Kuan, Christopher Millard and Ian Walden, 'The Problem of Personal Data' in *Cloud Computing – What Information is Regulated? The Cloud of Unknowing*, International Data Privacy Law (2011) 1(4), 211-214.

[23] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', adopted on 20 June 2007 (WP136), 18.

[24] Aaron Perkins, 'Encryption Use: Law and Anarchy on the Digital Frontier [comments]' Houston Law Review. Vol.41.No.5. (2005) 1628.

[25] However, the fuller exhaustion of the technology is hindered by the legal restrictions on the import, export and use of encryption in different jurisdictions. See Christopher Kuner, 'Legal Aspects of Encryption on the Internet' (1996) International Business Lawyer 24, 186.

[26] W Kuan Hon, Eleni Kosta, Christopher Millard and Dimitra Stefanatou, 'Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation', Tilburg Law School Legal Studies Research Paper Series No. 07/2014, 10.

The Working Party considers that equating pseudonymisation to anonymisation is one of the misconceptions among many data controllers. This is because pseudonymised data still allows an individual data subject to be singled out and linkable across different data sets. Therefore, in most instances it can be concluded that pseudonymised data remains subject to the data protection rules.[27] Accordingly, all privacy and data protection principles fully apply.

Anonymisation and pseudonymisation: guidance and recognition

Recital 26 of the Data Protection Directive specifies that codes of conduct may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible. Our study shows that almost two decades were necessary to see the emergence of comprehensive opinions and/or decisions at EU and national levels on the topic of anonymisation.

EU guidance

At **EU level**, the Working Party adopted on 10 April 2014 'Opinion 05/2014 on anonymisation techniques onto the web' already mentioned above , which analyses in depth the effectiveness but also the limits of anonymisation techniques.

After underlining the legal background[28], the Working Party concludes that the "*underlying rationale is that the outcome of anonymisation as a technique applied to personal data should be, in the current state of technology, as permanent as erasure, i.e. making it impossible to process personal data*".

Moreover, Opinion 05/2014 highlights four key features:

- Anonymisation can be a result of processing personal data with the aim of irreversibly preventing identification of the data subject;
- Several anonymisation techniques may be envisaged, there is no prescriptive standard in EU legislation;
- Importance should be attached to contextual elements; and
- A risk factor is inherent to anonymisation.

Since Opinion 05/2014 underlines that "*anonymisation constitutes a further processing of personal data"*, the process of anonymisation must comply with the test of compatibility with the original purpose. According to the Working Party, for the anonymisation to be considered as compatible with the original purpose of the processing, the anonymisation process should produce reliably anonymised information.

However, addressing the anonymisation process as compatible or incompatible with the original purpose might not represent a sound approach. This is because, for example, anonymisation could be used to comply with Article 6(1)(e) of the Data Protection Directive, which requires that information should be kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed in a form that permits identification. In this sense, anonymisation might constitute a compulsory processing activity that enables one to comply with its data protection duties.[29]

According to the Working Party, once data is truly anonymised and individuals are no longer identifiable, EU data protection rules no longer apply. However, some commentators have been critical of such proposition on the basis that the Working Party applies an absolute definition of acceptable risk in the form of zero risk.[30] First, the Data Protection Directive itself does not require a zero risk approach. Second, if the acceptable risk

[27] See Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques onto the web', adopted on 10 April 2014 (WP216), 10. See also at 29 noting that pseudonymisation reduces the linkability of a dataset with the original identity of a data subject; as such, it is considered a useful security measure but not a method of anonymisation.

[28] Directive 95/46/EC but also the ePrivacy Directive 2002/58/EC.

[29] Khaled El Emam and Cecilia Alvarez, 'A Critical Appraisal of the Article 29 Working Party Opinion 05/2014 on Data Anonymisation Techniques', Draft paper for a web conference, 3-9.

[30] Draft Regulation, Recital 23 states that "to ascertain whether means are likely reasonably to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development".

threshold is zero for any potential recipient of the data, there is no existing technique that can achieve the required degree of anonymisation. This would imply that anonymisation, or for that matter, the sharing of data would only be possible on the basis of the legitimate grounds (including consent) listed in Article 7 of the Data Protection Directive.[29] This might encourage the processing of data in identifiable form, which in fact presents higher risks.

Therefore, the notion of identifiability should be approached in light of the *"all means likely reasonably"* test provided in recital 26 of the Data Protection Directive. In other words, the question rests on whether identification has become *"reasonably"* impossible. This would be measured mainly in terms of both time and resources required to identify the individual.[30] Accordingly, if it is not reasonably possible, given the time; expense; technology; and labour required, to associate the data to a particular individual, then the data would remain non-personal. Another factor that needs to be considered is whether there is any kind of data in the hands of the controller or any other person that could be used to identify the individual. For example, if a data controller keeps the original (identifiable) data, and hands over part of this dataset by removing or masking the identifiable data to another party; the resulting dataset will still constitute personal data.[31]

In the third and substantial section of Opinion 05/2014, the Working Party examines the various anonymisation practices and techniques, elaborating on the robustness of each technique based on three cumulative questions:

- Is it still possible to single out an individual?
- Is it still possible to link records relating to an individual?
- Can information be inferred concerning an individual?

According to the Working Party, "*knowing the main strengths and weaknesses of each technique helps to choose how to design an adequate anonymisation process in a given context*".

Opinion 05/2014 provides some conclusions and recommendations. In a nutshell it indicates that "*anonymisation techniques can provide privacy guarantees, but only if their application is engineered appropriately*". Indeed, according to the Working Party, some techniques show inherent limitations and each technique examined fails to meet with certainty the criteria of effective anonymisation in light of the three questions above. Consequently, a case-by-case approach should be favoured in order to determine the optimal solution, always in combination with a risk analysis. Overall, the Working Party seems to imply that a true anonymisation might not be achievable in a world of "open" datasets; indicating that given the current state of technology and the increase in computational power and tools available, identification is easily attainable.[32] **Such an approach will significantly affect the widespread use of cloud services.**

In conclusion, Opinion 05/2014 provides an important clarification of the status of anonymisation techniques. However, it does not seem to encourage businesses to use anonymisation and pseudonymisation when processing personal data. Furthermore, the Opinion does not provide any guidance to be followed by data controllers or data processors in the anonymisation of their data.[29] As the Working Party has indicated, combinations of different anonymisation techniques could be used to reach the required level of anonymisation, in which case the Data Protection Directive does not apply. A further consideration could be to mitigate some obligations with respect to the use of a specific anonymisation technique if certain risks no longer exist.[33] This kind of approach moves away from the "all or nothing approach" regarding personal data, making room for "more or less personal" data and accordingly "more or less protection".[34] This would not only encourage the wider use of such techniques but could also lead to the wider adoption of cloud computing services.

---

31 See Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques onto the web', adopted on 10 April 2014 (WP216).

32 It is clear from case studies and research publications that the creation of a truly anonymous dataset from a rich set of personal data, whilst retaining as much of the underlying information as required for the task, is not a simple proposition. For example, a dataset considered to be anonymous may be combined with another dataset in such a way that one or more individuals can be identified.

33 For example, the European Commission has held, in its Frequently Asked Questions (FAQs), that the transfer of key-coded data outside the EU without transferring or revealing the key does not involve transfer of personal data to a third country; W Hon Kuan, Christopher Millard and Ian Walden, 'The Problem of 'Personal Data' in *Cloud Computing – What Information is Regulated? The Cloud of Unknowing,* International Data Privacy Law (2011) 1(4), 216.

34 Neil Robinson, Hans Graux, Maarten Botterman, and Lorenzo Valeri, 'Review of the European Data Protection Directive' (2009) RAND Europe technical report, 26-27.

National recognition of anonymisation and pseudonymisation techniques

Our study shows that half of the Key Member States have not issued any guidance or do not provide any case-law covering the issues of anonymisation. The situation is however different for the other half. While three of them only have administrative decisions, our study demonstrates that the authorities in **France**[35] and the **United Kingdom** provide specific guidance, the "*ICO Code of Practice on Anonymisation*" in the United Kingdom being the most substantial instrument (examined below).

In **Italy**, there is no specific guidance or similar document focused on data anonymisation or pseudonymisation techniques. Nevertheless, some references to such kind of measure can be picked up in some resolutions or decisions of the Italian DPA on specific matters, including:

- Code of conduct and professional practice applying to processing of personal data for statistical and scientific purposes dated 16 June 2004 (Annex A.4 to the Italian Data Protection Code[36]) specifying the criteria that render information capable of identifying an individual.
- Decision of 16 January 2014 related to the "*Processing of personal data contained in the Italian Registry of Dialysis and Transplantation*" and the decision of 10 April 2014 related to the "*Processing of health data collected by diagnostic equipment*" in which the Italian DPA suggested examples of solutions that make data "anonymous".[37]

More generic decisions on this matter are:

- Decision of 4 April 2013 related to the "*Implementing Measures with Regard to the Notification of Personal Data Breaches*", describing the criteria according to which data could be considered unintelligible from the Italian DPA's point of view.
- Decision of 10 July 2014 relating to Google, holding that information stored in so-called back-up systems "*must be protected against unauthorised access by means of suitable encryption techniques or, where necessary, by anonymising the data in question*", specifying that such provision is in line with the principles set forth by the Working Party Opinion 05/2014.

Also in **Spain**, there are no practice guides on the subject of anonymisation. However, the Spanish DPA has established its criteria through resolutions.

Article 5 of the Spanish Data Protection Regulation defines the dissociation procedure as "*any data processing allowing dissociated data to be obtained*". Data can either be anonymous from the outset or may be associated with personal data and then be anonymised through the use of a dissociation process which, reversibly or irreversibly, destroys the link with personal data.

In this sense and following the criteria that the Spanish DPA is currently following in its resolutions, the following elements must be taken into account on a case-by-case basis in order to determine if the process would be reversible, hence, if the data is effectively anonymised data or not: (i) reasonable means to identify a person; (ii) time; (iii) costs; and (iv) disproportionate endeavour.

Moreover, as per the Spanish DPA report n° 119/2006, anonymisation may be achieved by using an identifiable characteristic that would allow the processor to classify the data but not to link it to a data subject. However, it shall be noted that the Spanish DPA has determined that when a company is named after a physical person, said name shall not be considered as personal data. Hence, it will not fall within the scope of anonymisation.

In the **United Kingdom**, the ICO published in November 2012 a Code of Practice on managing the risks related to anonymisation. The Code explains how to balance

35 In France, the issues relating to the anonymisation and pseudonymisation of data are only referred to within the guides already mentioned in this Study, and in a more general perspective, within the Guide on the Security of Personal Data which comprises a dedicated factsheet (Factsheet n°16) on anonymisation.

36 Similar provisions were already contained in a former version of the Code (*Code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the national statistical system*) dated 2002.

37 E.g., the prediction of discrete values of the attributes in place of continuous values, as ranges instead of point values, i.e., the introduction where possible of binary values, such as true / false, instead of multi-valued attributes, etc., that ensure the extrapolation of only records whose combinations of attribute values are reported to a number of data subjects greater than or equal to three units).

the privacy rights of individuals while providing rich sources of data.

The Code contains a framework enabling practitioners to assess the risks of anonymisation related to data protection and identification of individuals. It also includes examples of how successful anonymisation can be achieved, such as how personal data can be anonymised for medical research when responding to Freedom of Information requests, and how customer data can be anonymised to help market researchers analyse purchasing habits. It contains less technical detail than the Working Party Opinion and also takes a different view on when data will constitute personal data. The view in the UK is that where information is anonymous in the hands of the recipients, it will not be considered to be personal data in the hands of those recipients, even if the original controller retains the ability to re-identity that data.

The ICO also announced that a consortium led by the University of Manchester, along with the University of Southampton, the Office for National Statistics and the government's new Open Data Institute, will run a new UK Anonymisation Network ("UKAN"). The UKAN will enable the sharing of good practice related to anonymisation, across the public and private sector.

We would like to thank the Norwegian Research Centre for Computers and Law of the University of Oslo for their valuable input.

Security and data breach legal requirements

This fifth chapter in our cloud computing and privacy series addresses the topic of data breach notification requirements. Although these requirements may not necessarily apply directly to CSPs, they ought to be taken into account and assessed by all actors involved in the provision or the use of cloud services in light of existing (but also upcoming) EU and national obligations.

Considering that serious breaches of confidentiality and security often constitute the quickest route through which a company can damage its image and reputation due to adverse press and media publicity, the question of data breach handling is of utmost importance.

More specifically, the notification of breaches follows various purposes, such as:

- Increasing transparency over operational failures;
- Allowing to mitigate damages and further risks;
- Helping stakeholders (including authorities and other companies) to identify the risks and the causes of failure;
- Developing adequate and appropriate responses to minimise future risks.

The present chapter therefore examines the legal requirements or guidance related to the notification of competent authorities and individuals impacted by serious incidents affecting the confidentiality and security of personal data at EU level and in certain Key Member States. This chapter does however not examine in depth any sector-specific requirements, such as may exist in the financial sector or the Payment Card Industry (PCI).

Current strict EU rules applicable to PECS providers

In spite of the importance of breach notification, the Data Protection Directive does not provide for an explicit obligation in this respect.

The "ePrivacy Directive does however currently provide breach notification obligations for the so-called PECS providers, e.g. telecommunications companies, internet service providers and email providers. Article 4 provides a defined protocol for the electronic communications sector, as completed by Commission Regulation (EC) 611/2013 of 24 June 2013[38] Since the publication of the Commission Regulation, a common regime applies to PECS providers within the 28 Member States.

More specifically, the ePrivacy Directive defines 'personal data breach' as being *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community*" (Article 2(i)).

Such incidents can trigger the following implications:

- In case of a particular risk of a breach of the security of the network, the PECS provider must inform the subscribers concerning such risk, and in certain cases of the possible remedies.
- In the case of a personal data breach, the PECS provider shall notify the personal data breach:

[38] Commission Regulation (EC) 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications [2013] OJ L173/2 (entered into force in all Member States on 25 August 2013); read our latest report on this Regulation at http://www.twobirds.com/en/news/articles/2013/global/new-data-breach-rules-for-telcos-and-isps.

- within 24 hours after detection (where feasible) to the competent national authority; and possibly

- without undue delay to the subscriber or individual, when the personal data breach is likely to adversely affect the privacy of such person. This is not required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures to render the data unintelligible to any person who is not authorised to access it (see also the previous chapter on data anonymisation).

Such requirements would only apply in limited circumstances when considering a cloud environment, notably when the CSPs or the client qualify as PECS providers pursuant to the applicable Member State legislation transposing the EU PECS provider definition.

It should be noted that ENISA has provided (i) guidelines to National Regulatory Authorities in the framework of Article 13a of Directive 2009/140/EC of 25 November 2009[39]; (ii) a general report entitled "*Data Breach Notification in the EU*"[40] of 13 January 2011; and (iii) a specific report entitled "*Cloud Security Incident Reporting - Framework for reporting about major cloud security incidents*".[41]

Current and future EU requirements and guidance

In spite of the absence of a general EU rule applicable to all organisations, breach notification is gradually becoming the norm in the EU. Indeed, all kinds of operators are increasingly urged to disclose breaches to the competent authority. The Draft General Data Protection Regulation will in all likelihood introduce a general data breach notification obligation. Furthermore, the draft Cybersecurity Directive also provides for breach notification in the framework of network and information security (NIS) applicable to certain 'market operators' who remain to be defined (see more details in the third chapter on security requirements and guidance).

EU guidance by the Working Party

It should also be noted that the Working Party has adopted on 25 March 2014 Opinion 03/2014 on Personal Data Breach Notification. Said Opinion provides guidance to organisations acting as data controllers in order for them to determine, on a case-by-case basis, whether they should notify affected individuals in case of a personal data breach.

In the introductory chapter of the Opinion, the Working Party highlights on the basis of the ePrivacy Directive the notification requirement to (i) the competent national authority, and (ii) the data subject in case the breach is likely to adversely affect his privacy or personal data. The Working Party further recommends controllers to take appropriate technological and organisational measures and to proceed with notification in case they have doubts about the likelihood of the adverse effects on the privacy or personal data of the data subject.

In the second and substantial chapter, the Working Party proposes a list of scenarios where data subjects should be notified. Each scenario is assessed on the basis of the following "classical security criteria":

- Availability breach – accidental or unlawful destruction of data;
- Integrity breach – alteration of personal data;
- Confidentiality breach – unauthorized access to or disclosure of personal data.

In the contemplated practical examples, the Working Party provides the appropriate safeguards that might have been able to reduce the risks and thus to avoid the need to notify the data subject if they had been implemented.

39 See in particular the Marnix Dekker and Christoffer Karsberg 'Technical guidance on the incident reporting in Article 13a' (ENISA, November 2013); and Marnix Dekker, Christoffer Karsberg 'Technical guidance on the security measures in Article 13a' (ENISA, November 2013).

40 Andreas Rockelmann, Joshua Budd, Michael Vorisek, 'Data Breach Notification in the EU' (ENISA, 13 January 2011).

41 Marnix Dekker, Dimitra Liveri, Matina Lakka, 'Cloud Security Incident Reporting - Framework for reporting about major cloud security incidents' (ENISA, 9 December 2013).

Current national breach notification regimes

In addition to the Working Party's Opinion 03/2014, which anticipates the adoption of a broader obligation of breach notification at EU level, several Member States have adopted measures in order to expand the notification requirement to actors other than PECS providers.

One of the most topical illustrations of the advancement of some Member States over others is the case of **Germany**, which has introduced since 2009 amendments to the German Federal Data Protection Act, including on data breach notification. Some countries, such as **Belgium** or the **United Kingdom**, have adopted non-mandatory general guidance. Others have adopted some limited opinions or requirements applicable to specific sectors.

In **Germany**, under Section 42a of the German Data Protection Act, the data controller is obliged to notify the DPAs and the individuals affected (alternatively if individual information is not reasonably possible, through a press release/ad in mass media) in specific cases of data breach where the following two cumulative conditions are met:

- Particular data are concerned: either (i) sensitive data, or (ii) data effected by professional secrecy, such as health data controlled by doctors, or (iii) data concerning criminal or administrative offenses, or (iv) bank and credit card related data; and
- Material negative consequences for the individual are possible due to the breach.

Data processors are not directly addressed by Section 42a, but are obliged to notify breaches to the controller under the data processing agreements.

In **Belgium**, the local DPA has published on 21 January 2013 a recommendation addressed to any controller processing personal data, requiring that public incidents (*i.e.* where a personal data breach results in a public leakage of private data) are notified to the DPA within 48 hours. In addition, a public information campaign should be rolled out within 24-48 hours after notifying the DPA.

In the **United Kingdom**, the ICO published in 2012 guidance on the "Notification of data security breaches to the ICO" and on "Data Security Breach Management".

The ICO acknowledges that there is no legal obligation for data controllers to report breaches of security which result in loss, release or corruption of personal data. The ICO however believes serious breaches should be brought to the attention of the ICO. The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under data protection law. Although "serious breaches" are not defined, the guidance identifies three areas to be considered by data controllers when determining whether a breach should be reported:

- The potential detriment to data subjects;
- The volume of personal data lost/released/corrupted; and
- The sensitivity of the data lost/released/corrupted.

The guidance states that all serious breaches should be notified to the ICO using the DPA security breach notification form.

In addition to the foregoing, breach notification in the healthcare sector is also addressed in the United Kingdom. The process for reporting IG SIRIs which occur in health, public health and adult social care services has recently changed. All health service organisations must now use the IG Toolkit Incident Reporting Tool.[42] This will report IG SIRIs to HSCIC, the Department of Health, the ICO and other regulators.

HSCIC published a checklist dated 1 June 2013 for reporting, managing and investigating IG SIRIs. This guidance is supported by the ICO.

Finally, in **Italy**, provisions have been adopted by the Italian DPA with reference to banks. In particular, at point 5 of resolution 192/2011, in force as from October 2014, the DPA strongly recommends that, without undue delay, banks inform:

- data subjects "*of any unlawful processing operations performed by persons in charge of*

[42] Excluding health service organisations in Scotland, Northern Ireland and Wales.

data processing on the personal data relating to them"; and

- the Italian DPA "*of appropriate details of any cases where accidental and/or breach of personal data protection have been established - providing such violations are material on account of either the type or amount of the data concerned and/or the number of customers affected – and such violations give rise to the destruction, loss, modification and/or unauthorized disclosure of customers' data*".

Moreover, the data controllers in Italy will need to seek compliance with mandatory data breach obligations in force, or coming into force, in other sectors. In particular, a general provision of the Italian DPA dated November 2014 imposed an obligation on the data controllers that process biometric data to notify to the DPA within 24 hours any breach related to the biometric data according to a specific procedure and based on a data breach form made available by the DPA.

A draft decree aimed to identify the technical rules for setting up national EHR (drafted based also on the opinions released by the Italian DPA) also contains an express provision about the obligation for the data controllers to promptly notify the Italian DPA in case of violations related to the data processed under the EHR.

Legal issues related to sensitive (health) data

This final chapter of our cloud computing and privacy series discusses the legal issues related to the processing of sensitive data and the hosting of health data in a cloud environment.

The Data Protection Directive provides for a special regime applicable to so-called 'sensitive data'. The rationale behind a reinforced legal regime is based on the presumption that the misuse of such category of data "*could have more severe consequences on the individual's fundamental rights*". For instance, the misuse of health data "*may be irreversible and have long-term consequences for the individual as well as his social environment*".[43]

Considering that cloud computing services and infrastructures are increasingly being used to store and process personal data of such a sensitive nature, the present chapter examines how the processing of sensitive data, and in particular health data, is regulated in the EU as well as in certain Key Member States. Although this chapter addresses the issues of EHR, it does not examine the specific issues relating to non-privacy requirements such as those linked to criminal law, medical ethics, health legislations or patients' rights.

The concept of sensitive (health) data in the EU

Pursuant to Article 8 of the Data Protection Directive, sensitive data concerns "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and (...) data concerning health or sex life*".

As highlighted by the Working Party in its Advice Paper on special categories of data ("sensitive data") of 4 April 2011, Article 8 of the Data Protection Directive has been implemented in similar ways across the EU. However, there are some differences, notably with respect to the categories of sensitive data.

All national data protection legislations in the Key Member States include the data listed under Article 8 of the Data Protection Directive. Some Member States have, however, included additional types of data. For instance, when focusing on health data, we note that the **Czech** Data Protection Act explicitly includes in the legal definition of sensitive data genetic and biometric data. Similarly, the **Polish** Data Protection Act includes genetic code, as well as addictions. Also, a few countries explicitly provide for a more detailed list, such as the **United Kingdom** which refers for instance to "physical and mental health".

The Working Party admits that health data represents the most complex area of sensitive data and that it displays a great deal of legal uncertainty. Consequently, the proposition to create new categories of sensitive data has emerged. This notably includes the idea of adding genetic and biometric data, but also data of minors or on individuals' geo-location. As a result of the problems relating to certain categories of sensitive data, and in particular health data, in the national implementation of the Data Protection Directive, the Working Party has encouraged a revision of the current system.

The processing of sensitive data in the EU

As a matter of rule, the processing of sensitive data is prohibited. However, the Data Protection Directive provides for several strict exceptions allowing for the processing of sensitive data:

- The data subject has given his explicit consent to the processing of those data; or
- The processing is necessary for the purposes of carrying out the obligations of the controller in the field of employment law; or

[43] Article 29 Working Party Advice Paper on special categories of data ("sensitive data") of 4 April 2011.

- The processing is necessary to protect the vital interests of the data subject or of another person; or
- The processing is carried out in the course of legitimate activities by a non-profit-seeking body with a political, philosophical, religious or trade-union aim; or
- The processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

The prohibition also does not apply where processing is required for specific purposes of the health sector.[44] Moreover, Article 8(4) of the Data Protection Directive provides for a residual exception for "*reasons of substantial public interest (…) either by national law or by decision of the supervisory authority*".

The Working Party published a Working Document on 15 February 2007 on the processing of personal data relating to health in EHR.[45] It highlights the potential privacy and data protection issues relating to the constitution of so-called EHR and notably examines several exceptions allowing for the processing of sensitive data. Since the publication of the Working Document, the EU has adopted the European eHealth Action Plan 2012-2020 on Innovative healthcare for the 21st century. In this context the EU Commission insisted on the fact that "*Data protection issues also need to be addressed in respect to the use of cloud computing infrastructures and services for health and wellbeing data processing*".[46]

In the paragraphs below, we examine in more detail some of the grounds allowing for the processing of sensitive (health) data and the implementation of EHR.

First, on the justification of the processing on the basis of the vital interests of the data subject, the Working Party notes the strict conditions: "*the processing must relate to essential individual interests of the data subject or of another person and it must – in the medical context – be necessary for a life-saving treatment in a situation where the data subject is not able to express his intentions*". Such exception will therefore apply in very limited cases.

Second, with respect to the processing of medical data by health professionals, the Working Document puts forth the following three cumulative conditions:

- It only covers the processing for the specific purpose of providing health-related services of preventive, diagnostic, therapeutic or after-care nature and for the purpose of the management of these healthcare services; and
- The processing must be "required" for the specific purposes mentioned in the first condition; and
- The processing must be performed by medical or other staff subject to professional (medical) secrecy or an equivalent obligation to secrecy.[47]

Given the above strict conditions and their restrictive interpretation, the Working Party has cast doubts as to whether such legal ground is appropriate to legitimise EHR.

Also, in its general advice paper relating to sensitive data, the Working Party highlights that such exception may pose difficulties given that in practice (i) health data are processed for various purposes; (ii) it is often not clear who belongs to the category of "health professionals"; and (iii) there are currently no explicit grounds justifying the processing of sensitive personal data in case of injuries, when health data are transmitted by non-medical personnel.

Third, the Data Protection Directive provides a ground allowing for a high degree of Member States' discretion, *i.e.* the "substantial public interest", aiming at situations such as public health, social protection, scientific research and government statistics.[48] Relying on such exception requires striking a balance between the protection of the data subject's rights and the legitimate interests of data controllers, third parties and the public interest which may exist. Strict conditions

[44] Article 8(3) Data Protection Directive.

[45] Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records (EHR) of 15 February 2007.

[46] In a communication of 6 December 2012, the EU Commission outlines the action plan, highlighting some important privacy and data protection aspects. For instance, it recommends that "eHealth and wellbeing ICT initiatives should integrate the principle of privacy by design and by default as well as make use of Privacy Enhancing Technologies (PET's), as foreseen in the proposed Data Protection Regulation".

[47] It shall be noted that the terms "health professional" may be diverging across the EU.

[48] Recital 34 of the Preamble of the Data Protection Directive.

however apply, such as in particular: a special legal basis is required, it must be justified by a substantial public interest, and specific and suitable safeguards must be put in place.

Fourth, Article 8(2)(a) of the Data Protection Directive stipulates that the explicit consent may also serve as a basis permitting the processing of sensitive personal data. Such ground will in all likelihood be the most suitable one to legitimise EHR.

It is important to remember that in order for consent to be valid, it must be (i) unambiguous; (ii) freely given; (iii) specific; and (iv) informed.

With respect to the second condition, the Working Party has had the opportunity in its Opinion 15/2011 on the definition of consent to lay down several scenarios in the context of EHR:

- If the creation of the summary record is absolutely voluntary, and the patient will still receive treatment whether or not he or she has consented to the creation of a summary record: the consent is deemed to be freely given because the patient will suffer no disadvantage if consent is not given or is withheld;
- If there is a moderate financial incentive to choose the EHR: the consent is deemed to be freely given because the patient refusing the EHR does not suffer disadvantage (the costs do not change);
- If patients refusing the e-health system have to pay a substantial extra cost compared to the previous tariff system and the processing of their file is considerably delayed: the consent cannot be deemed to be freely given because it creates a clear disadvantage for those not consenting. Consequently, relying on other legitimate grounds to process sensitive data is necessary.

In addition, consent in the context of sensitive data must be explicit. This notably means, as expressed by the Working Party and some Member States (e.g., **Denmark**), that opt-out solutions will not be sufficient.[45]

The Working Party is of the opinion that such explicit consent does not have to be written and that it can therefore also be given orally. The results of our study however nuance such statement. While explicit consent is a requirement across the EU and while it is stricter than "ordinary" consent, we have noted some discrepancies between the Key Member States.

In addition to providing certain grounds where sensitive data may be processed under specific circumstances and for instance in the context of healthcare, data protection law in **Finland** regards express consent as one ground allowing processing of sensitive data. Although the law does not literally require written consent[49], its preparatory works mention that express consent should usually be given in writing. Further, more specific requirements for processing sensitive data, such as health data, are laid down by special legislation as also described in this chapter.

In **Poland**, the consent for sensitive data processing shall be explicit and in written (hard copy) form in order to be valid. Also, consent cannot be alleged or presumed on the basis of a declaration of will or other content, and it is not sufficient to have an e-signature or click-to-accept. Pursuant to a judgment of 4 April 2003 (unpublished), all aspects of the explicit consent should be clear at the moment when the consent is given.

Requirements are similar in **France**, where courts have considered that explicit consent is necessarily provided in writing in order to be valid. The French DPA had thus initially adopted a strict view of consent for sensitive data processing, specifying that consent should be obtained through a separate consent form. Nevertheless, the French DPA may adopt flexible positions; for instance, in the healthcare sector, the French DPA has deemed valid a consent provided through ticking a box at the bottom of a digital form.

Hosting of health data

In addition to examining the particularities under data protection laws related to the processing of sensitive data, our study on cloud computing has also investigated the potential issues related to the hosting of health data. It revealed that the outsourcing of the hosting activity of such category of data is specifically regulated under the national laws of certain Member States, which ought to be

[49] The Finnish Data Protection Authority issued in July 2010 guidance on consent, available in Finnish and Swedish

taken into account when considering the adoption of cloud computing services.

More specifically, our study has revealed the particular situation in **France**. In addition to the French Code of Public Health, the hosting of personal health data is regulated under French law by Act n°2002-303 of 4 March 2002, which aims to protect the confidentiality, integrity and availability of patients' data. Pursuant to this Act, such hosting activity can only be implemented by a HSP previously approved by the Shared Healthcare Information Systems Agency ("ASIP"), a department within the Ministry of Health, following a strict accreditation procedure.[50]

Pursuant to the French Public Health Code, health professionals, healthcare establishments, and data subjects themselves are under the obligation to use the services of an accredited HSP if: (i) health data is not stored on the health professional's own information systems; and (ii) health data is collected or produced within the framework of prevention, diagnosis or care activities.[51] The Code further requires the conclusion of a contract between the HSP and the healthcare professional.[51] However, the law does not prescribe any particular contractual form but lists the mandatory provisions that must be included.

The use of the health professional card (i.e. "Carte de Professionnel de Santé") or an equivalent, is mandatory in case of access by healthcare professionals to personal health information stored on electronic supports.[52]

A high level of interconnection/exchanges security must be guaranteed given the risks involved in the transmission of degraded information or disclosure thereof to third parties. The National Commission on Informatics and Liberty ("CNIL") considers that the telemedicine devices must guarantee: health professionals' authentication; data confidentiality; encryption of transmitted data; logs traceability; data integrity; and a secured data archiving must be implemented. The technologies used in the context of telemedicine (e.g., software) must comply with interoperability and security frameworks developed by the ASIP. When the processing relies on an authorised HSP, the express consent of the patient to the hosting is required. This can be expressed electronically.

As for the situation in **Finland**, although there is no law governing the hosting of health data specifically, Finnish national law, such as recent regulation on electronic processing of customer data in healthcare, needs to be complied with by any service provider. Also, certain Finnish accreditation procedures must be considered, as well as the sensitivity of the data and secrecy obligations.

First, processing of personal health data by relevant (usually public) entities is subject to relatively strict regulation. For instance, the Act on the Status and Rights of Patients regulates the processing of patient documents and their confidentiality. In addition, public entities are subject to special regulation providing e.g. certain confidentiality and security obligations. As a rule, entities providing healthcare services are responsible for compliance with such regulation also when they decide to outsource the processing of personal health data. Therefore, obligations related to personal health data apply to processors indirectly as specified in the relevant contract. In practice, when outsourcing services, a healthcare unit such as a hospital or a health centre needs to sign a written agreement with the service provider and define the tasks and responsibilities related to data processing as well as confidentiality and secrecy obligations related to patient documents as further described by law.

Second, processors need to pay attention to the recent regulation on electronic processing of personal health data setting requirements for services (ICT systems) used in public and private healthcare. For example, the Act on the Electronic Processing of Customer Data in Social Care and Healthcare (159/2007) updated in 2014 provides, in brief, that the services used in processing the customer data of healthcare need to fulfil the essential requirements of interoperability, data security, data protection and functionality. Such requirements as further elaborated by law need to be taken into account in the design, production and functions of the service. The service needs to be suitable for its purpose and must fulfil the requirements of law. Its capacity needs to be the same as informed by its producer. The requirements need to be fulfilled both whenever using the service alone and in connection with other systems meant to be connected with it.

[50] To learn more about the accreditation procedure, read our brochure at http://www.twobirds.com/~/media/PDFs/Brochures/Privacy%20and%20Data%20Protection/Hosting%20Health%20Data%20-%20The%20French%20Requirements.pdf.

[51] Article L.1111-8 of the French Public Health Code.

[52] Article R.1110-3 of the French Public Health Code.

Finally, in **Poland**, there are also no specific regulations on cloud hosting in relation to health data.[53] However, the Regulation of the Minister of Health on Types and Scope of Medical Data and Means of its Processing of 21 December 2010, as well as other provisions, in particular regulations as to medical documentation, contain inter alia provisions on taking the medical documentation outside of health professional's premises (but note that they can be processed by different entities than health professionals). The above provisions are the basis for outsourcing medical data.

In addition to the above rules, general rules on professional secrecy apply. Health data protected by professional medical secrecy can be disclosed to a third party for IT purposes by entities which provide medical services in two situations only:

- the data subject has consented to the disclosure of its professional medical secrecy; or
- the statutory provision expressly allows for such disclosure.[54]

Currently there is no such statutory provision.

GIODO does not provide any particular official guidelines regarding outsourcing of personal health data. Generally, since 2011, GIODO has been underlining that IT outsourcing in the medical sector is not allowed due to lack of clear legal provisions with regard to disclosure of medical secrecy. According to GIODO, entities/persons that provide medical services can outsource services only in limited circumstances (not defined) and only as an exception.[55]

The draft "Guidelines on Electronic Medical Records" state that in case of outsourcing medical data it is not sufficient for the IT provider to fulfil the requirements set forth in different medical data security regulations. It is necessary to prevent the IT provider from having access to the data by using the Public Key Infrastructure, and the data should be encrypted by the use of Hardware Security Module.

The above uncertainty may change as the Ministry of Health is conducting a public consultation on proposed amendments to several acts, introducing specific exclusions from the professional secrecy.

[53] It shall be noted that the Minister of Health is working on a final version "Guidelines, rules and recommendations for service providers in the subject of construction and application of safe processing of electronic medical records" issued by the Minister of Health ("Guidelines on electronic medical records"). The Guidelines recognise three models (IaaS, SaaS and PaaS) with a very detailed description as to what the service provider and medical institution should implement, and how to implement those models in compliance with law.

[54] Act on Patients' Rights and the Commissioner for Patients' Rights of 6 November 2008, the Act on Doctor and Dentist Professions of 5 December 1996 and Act on of Nurse and Midwife Professions of 15 July 2011.

[55] Presented in one of the articles and not in the form of formal guidelines, and not supported with any legal provisions.

Further Info on Cloud

Looking for more information on Cloud? Download Our Cloud Services App.

Bird & Bird's cloud app provides responses to commonly asked legal questions relating to cloud computing services across 17 jurisdictions. Whether you are a supplier or a user of cloud services, this app covers the main issues you need to think about when setting up a cloud service and answers your questions on what you need to do to ensure you are compliant.

The app reviews issues of applicable law, consumer protection, data protection, data portability, intellectual property, liability, security and the use of the cloud by the public sector. The app also aims to give a comparative approach to commonly asked legal questions in these fields for the countries that we have covered: **Australia, • Belgium, Czech Republic, Denmark, Finland, France, Germany, Hungary, Italy, Netherlands, Poland, Singapore, Spain, Sweden, Switzerland, UK and UAE**

Requirements: Optimised for iPad; iOS6 and 7 and Android Tablets.

http://www.twobirds.com/en/sectors/information-technology/cloud-computing

Watch our latest Tech & Comms video: Moving to the Cloud.

In this video, partners Fabian **Niemann** and **Howard Rubin** explain how to maximise value when moving to the cloud and give some tips for businesses on avoiding the potential pitfalls. Other topics discussed include:

- Strategies for maximising value when moving to the cloud
- Why moving services to the cloud in stages is a key part of any cloud strategy
- How the NSA scandals have impacted the perception of cloud security
- How cloud services have changed the way that IT is supplied to companies

http://www.twobirds.com/en/news/videos/moving-to-the-cloud

Contacts

Belgium

Benoit Van Asbroeck Partner,

Tel: +32 (0)2 282 6067
benoit.van.asbroeck@twobirds.com

Jasmien Cesar Associate

Tel: +32 (0)2 282 6045
jasmien.cesar@twobirds.com

Julien Debussche Associate

Tel: +32 (0)2 282 6044
julien.debussche@twobirds.com

Czech Republic

Vojtech Chloupek Counsel

Tel: +420 226 03 0518
vojtech.chloupek@twobirds.com

Denmark

Nis Peter Dall Partner

Tel: +45 39 14 16 50
nis.dall@twobirds.com

Finland

Jesper Nevalainen Partner

Tel: +358 9 622 66789
jesper.nevalainen@twobirds.com

Iiro Loimaala Associate

Tel: +358 9 622 6670

iiro.loimaala@twobirds.com

France

Nathalie Metallinos Counsel

Tel: +33 (0) 1 42 68 60 21
nathalie.metallinos@twobirds.com

Lorraine Maisnier-Boché Associate

Tel: +33 (0) 142 68 63 33
lorraine.maisnier@twobirds.com

Germany

Fabian Niemann Partner

Tel: +49 171 5664080
fabian.niemann @twobirds.com

Italy

Debora Stella Senior Associate

Tel: +39 (0)2 30 35 6000
debora.stella@twobirds.com

Poland

Izabela Kowalczuk Associate

Tel: +48 22 583 79 00
izabela.kowalczuk@twobirds.com

Spain

Paula Fernandez-Longoria Senior Associate

Tel: +34 91 790 6037
paula.fernandez.longoria@twobirds.com

United Kingdom

Barry Jennings Senior Associate

Tel: +44 (0)20 7905 6382
barry.jennings@twobirds.com

Elizabeth Upton Associate

Tel: +44 (0)20 7905 6280
elizabeth.upton@twobirds.com

Gabriel Voisin Associate

Tel: +44 (0)20 7905 6236
gabriel.voisin@twobirds.com

twobirds.com

Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Skanderborg & Stockholm & Sydney & Warsaw