Multi-Jurisdictional Study: Cloud Computing Legal Requirements

Bird & Bird

Julien Debussche
Associate
January 2015

Content

1. General Legal Framework
2. Data Protection Legal Framework
3. Security Requirements
4. Data Anonymisation
5. Security & Data Breach
6. Sensitive (health) Data

coco CLOUD

Bird & Bird

Context of this Multi-Jurisdictional Study

Objective: highlight some of the particularities of national laws on key specific issues in ten selected EU Member States


Belgium


Czech Republic (and Slovakia)


Denmark


Italy


Poland


Finland


France


Germany


Spain


United Kingdom

1. General Legal Framework

1. General Legal Framework
EU Level

- EU Commission: Strategy for "Unleashing the Potential of Cloud Computing in Europe" (Sept. 2012)
  - Three Key Actions
    - Safe and fair contract terms and conditions
    - Cutting through the jungle of standards
    - Establishing a European cloud partnership
- EU Parliament: Resolution on unleashing the potential of cloud computing in Europe (Dec. 2013)
  - Main challenges and issues
- EU Commission Staff Working Document Report on the Implementation of the Communication 'Unleashing the Potential of Cloud Computing in Europe' (July 2014)

© Bird & Bird LLP 2015

1. General Legal Framework
National Level

- Czech Republic
- Finland
- United Kingdom

No or very little guidance on cloud computing in general

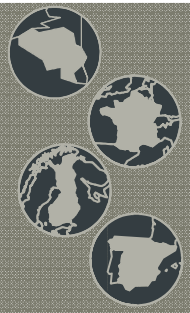
- Poland
- Germany

Guidance on specific issues only (excluding data protection)

- Italy

Guidance on or acknowledgment of public-related cloud computing

- Belgium
- France
- Denmark
- Spain



General guidance applicable to the public and/or private sectors

© Bird & Bird LLP 2015

Bird & Bird

COCO CLOUD

2. Data Protection Legal Framework

2. Data Protection Legal Framework
EU Level

- Article 29 Working Party opinions
  - Opinion 4/2007 on the concept of personal data
  - Opinion 8/2010 on applicable law
  - Opinion 15/2011 on consent
  - Opinion 03/2013 on purpose limitation
  - Opinion 05/2014 on anonymisation techniques onto the web
  - Opinion 03/2014 on personal data breach notification
  - Opinion 05/2012 on **Cloud Computing** (1 July 2012)
    - analyses relevant issues for cloud computing service providers ("CSP") operating in the European Economic Area (EEA), and their clients
    - specifies all applicable principles from the EU Data Protection Directive (95/46/EC) and the ePrivacy Directive 2002/58/EC (as revised) where relevant

© Bird & Bird LLP 2015

2. Data Protection Legal Framework
National Level - Guidance

- Most DPA's issued guidance dedicated to cloud computing
- Few DPA's have not issued cloud-specific data protection guidance
  - E.g.: Belgium, Denmark, Finland and Poland
  - However countries that have issued general guidance on cloud computing all cover data protection aspects (e.g.: Belgium and Denmark)
- In any case, guidance on more general topics may apply to cloud computing
- Tailored guidance by DPA's on privacy and data protection in a cloud environment – e.g.:

Czech Data Protection Office issued on 7 August 2013 its official position on the Protection of Personal Data within Cloud Computing Services

Spanish DPA provided guidance in 2013 on privacy and cloud computing with two specific guides: the "guide for clients using Cloud computer services"(link) and the "guide for Cloud service providers"

UK ICO published on 27 September 2012 a set of guidelines for businesses in relation to cloud computing

© Bird & Bird LLP 2015

Bird & Bird

COCO CLOUD

2. Data Protection Legal Framework
Case-law

- No specific cloud computing decisions at EU level
  - But other more general decisions worth taking into account
  - E.g.: Lindqvist (case C-101/01), Google Spain (case C-131/12) and Heinz Huber (C-524/06)

- National level – out of 10 countries only 2 have cloud-specific decisions

Danemark: the DPA has in a few cases dealt with cloud computing from a data protection perspective. Several decisions related notably to **Dropbox**, a driver's license system, **Google** Apps and **Microsoft's** Office 365

Spain: the Supreme Court was compelled to examine several issues relating to claims against the Spanish Data Protection Regulation.
The Spanish DPA has also applied the criteria of the Supreme Court in other resolutions such as regarding **Microsoft's** Office 365

© Bird & Bird LLP 2015

3. Security Requirements & Guidance

3. Security Requirements & Guidance
Legal requirements - EU Level

- Article 17 of Directive 95/46
  - Controller to guarantee the security of the personal data and protects their integrity
  - Controller (or its processor) must implement '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*"

- Article 4(1) of the ePrivacy Directive 2002/58/EC (as revised)
  - Security duty on providers of publicly available electronic communications services

- **Risk-based approach** is imposed
  - Requires a continuous risk assessment, which 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

© Bird & Bird LLP 2015

3. Security Requirements & Guidance
Legal requirements - National Level

- Member States have relatively high level of discretion when implementing EU provisions formulated in general terms

- Some countries provides for details as to the measures to implement

Detailed regulations regarding technical and organisational measures set forth in
- the Polish Data Protection
- the Security Regulation by the Polish Minister of Internal Affairs and Administration

Section 9 of the German Data Protection Act
- Obligations to implement certain security measures listed in an annex to the law (comprehensive list where all elements must be fulfilled)

- 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.

© Bird & Bird LLP 2015

3. Security Requirements & Guidance
Guidance - EU Level

Article 29 Working Party

- Opinion on the Commission Communication on "*Creating a safer information society by improving the security of information infrastructures and combating computer-related crime*" (5 Nov. 2001)
- Opinion 05/2012 on Cloud Computing

*ENISA**

- Published numerous reports (some specifically dedicated to cloud computing)
- Examples:
  - "Cloud Computing Risk Assessment"
  - "Cloud Computing Information Assurance Framework"
  - "Security & Resilience in Governmental Clouds"

**European Network and Information Security Agency*

© Bird & Bird LLP 2015

3. Security Requirements & Guidance
Guidance - National Level (1)

- DPA published "reference measures on the security of data" detailing ten areas of action regarding data security
- DPA published guidelines in 2012 for information security based on the ISO/IEC 27002 structure

- Inspector General for the Protection of Personal Data published "The ABC of rules on personal data security processed by means of IT systems"

© Bird & Bird LLP 2015

Bird & Bird

coco cloud

3. Security Requirements & Guidance
Guidance - National Level (2)

- Some DPAs and industry associations provide guidance on how to include technical measures in data processing agreements
- Section 11 of the German Data Protection Act enumerates the items that must be specified in a data processing agreement
- Guidance paper "Orientierungshilfe Cloud Computing" of 26 September 2011 (updated Oct. 2014) of the German data protection authorities
- guidance of the German Federal Agency for Security in Information Technology entitled "Security Recommendations for Cloud Computing Providers" of February 2012

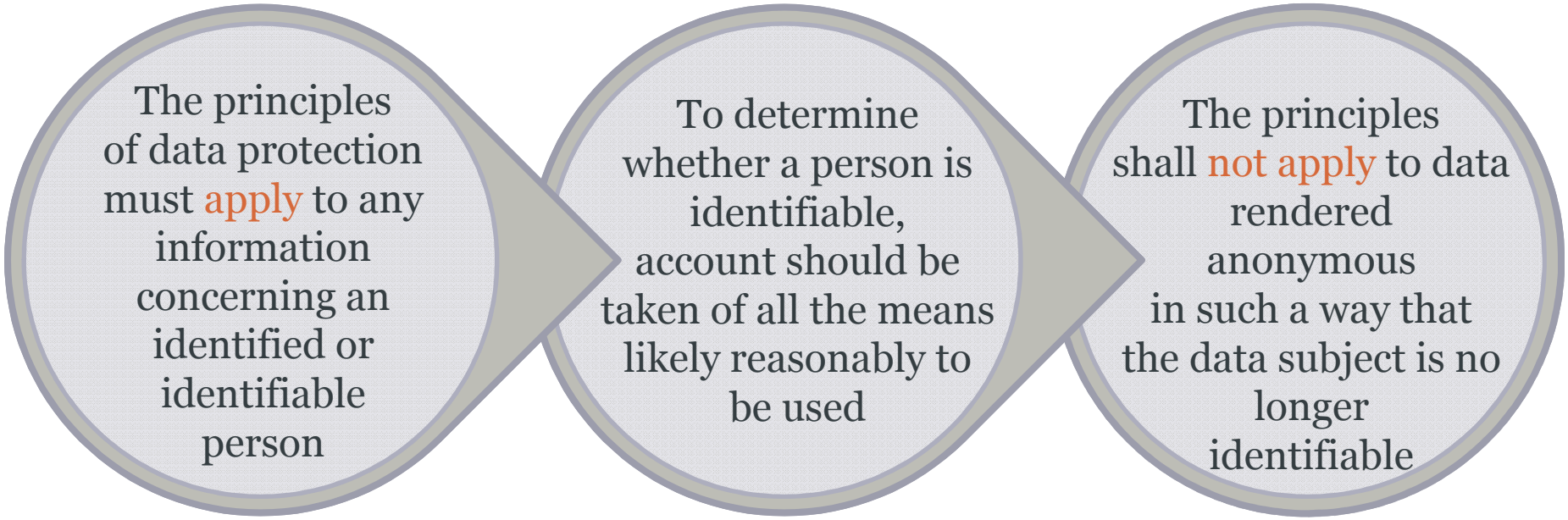
- Spanish DPA published a guide for the drafting of the Security document
  - Covers security measures (including concept and use) and the security document (including concept and template)
  - Lists the security measures required by Spanish law and implementation strategies
- The 2013 cloud-related guides of the Spanish DPA, one for users (link) and one for providers
- The "Guide for companies: security and privacy of Cloud computing" of 2011 ("INTECO Guide")

© Bird & Bird LLP 2015

4. Data Anonymisation

4. Data Anonymisation
Introduction

- Concept enshrined in Directive 95/46 (Recital 26):



- Not sufficient to understand precisely what encompasses the notion of 'anonymisation' and the related concept of 'pseudonymisation'.

© Bird & Bird LLP 2015

4. Data Anonymisation
EU Level

- Article 29 Working Party 'Opinion 05/2014 on anonymisation techniques onto the web'
  - Analyses in depth the effectiveness and the limits of anonymisation techniques
  - 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

© Bird & Bird LLP 2015

4. Data Anonymisation
National Level

- Few Member States provide guidance or case-law on anonymisation

- Anonymisation only referred in general guidance and within the Guide on the Security of Personal Data which comprises a dedicated factsheet on anonymisation

Reference to anonymisation in decisions/resolutions of DPA

- Code of conduct and professional practice applying to processing of personal data for statistical and scientific purposes (16 June 2004)
- Recent decisions related to the health sector, data breaches or Google

- Spanish DPA has set elements to take into account on a case-by-case basis in order to determine if the process would be reversible
- Report no. 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

- ICO Code of Practice on managing the risks related to anonymisation (2012)
- Upcoming UK Anonymisation Network to share good practice related to anonymisation across the public and private sector

© Bird & Bird LLP 2015

Bird & Bird

COCO CLOUD

5. Security and Data Breach

5. Security and Data Breach
Introduction

- Serious breaches of confidentiality and security can easily damage a company's image and reputation due to adverse press and media publicity

- Notification of breaches follows various purposes:
  - 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

© Bird & Bird LLP 2015

5. Security and Data Breach
EU Level (1)

- Data Protection Directive 95/46 does <u>not</u> provide for an explicit obligation related to breach notification
- ePrivacy Directive provides for a breach notification in the **telecommunications sector**
  - Article 4 includes a defined protocol (completed by Regulation 611/2013)
  - Includes a definition of personal data breach
    "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"
  - Strict requirements related to the notification of any breach
- ENISA Guidance:
  - Guidelines to National Regulatory Authorities in the framework of Article 13a of Directive 2009/140/EC
  - General report on "Data Breach Notification in the EU"
  - Specific report on "Cloud Security Incident Reporting - Framework for reporting about major cloud security incidents"

© Bird & Bird LLP 2015

5. Security and Data Breach
EU Level (2)

- Notification of breaches becomes the norm
  - Draft Data Protection Regulation
  - Draft Cybersecurity Directive

- Article 29 Working Party Opinion 03/2014 on Personal Data Breach Notification
  - Recommendations
  - Scenarios (practical examples)

© Bird & Bird LLP 2015

Bird & Bird

5. Security and Data Breach
National Level

- Section 42a of the German DP Act: the controller shall notify in specific cases of breach

- Belgian DPA recommendation of 2013 addressed to any controller
  - requiring breaches to be notified to the DPA within 48 hours
  - requiring the roll out of a public information campaign within 24-48 hours after notifying the DPA

- ICO guidance (2012) on:
  - "Notification of data security breaches to the ICO"
  - "Data Security Breach Management"

- Limited guidance to specific sectors
  - Resolution 192/2011 of the DPA applicable to the financial sector
  - Processing of biometric data [upcoming legislation]

© Bird & Bird LLP 2015

6. Sensitive (health) Data

6. Sensitive (health) Data
Concept of "sensitive data"

- Article 8 of Directive 95/46:

  "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and (…) data concerning health or sex life"

- Diverging concept throughout the EU?
  - All Member States include the data listed under Article 8
  - Some Member States have included additional types of data.
    - When focusing on health data, the **Czech** Data Protection Act explicitly includes genetic and biometric data
    - The **Polish** Data Protection Act includes genetic code, as well as addictions.
  - Some Member States explicitly provide for a more detailed list, such as the **United Kingdom** which refers for instance to "physical and mental health"

- Article 29 Working Party:
  - Health data represents the most complex area of sensitive data and that it displays a great deal of legal uncertainty

© Bird & Bird LLP 2015

6. Sensitive (health) Data

Processing of "sensitive data" in the EU

- General prohibition
- Several strict exceptions
  - 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
  - The processing is necessary to protect the **vital interests** of the data subject or of another person
  - 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
  - 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
- Prohibition also does not apply where processing is required for specific purposes of the health sector
- Residual exception for "*reasons of **substantial public interest** (…) either by national law or by decision of the supervisory authority*"
- Working Party published a Working Document (2007) on the processing of personal data relating to health in electronic health records ("EHR")

© Bird & Bird LLP 2015

6. Sensitive (health) Data

Hosting of Health Data

- Outsourcing of the hosting activity of health data is specifically regulated under the national laws of certain Member States

Specific laws relating to public health, rights of patients or medical data

© Bird & Bird LLP 2015

Conclusion

Bird & Bird

Thank you & Bird & Bird

Julien Debussche

Julien.Debussche@Twobirds.Com

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 15 Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.

twobirds.com