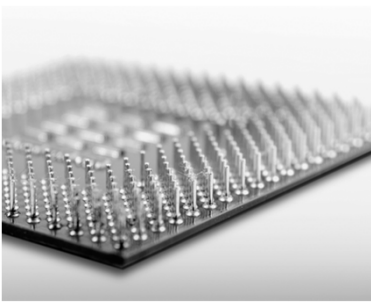


Speechly Bircham

EU DATA PRIVACY COMPLIANCE FOR US DRIVEN PROJECTS



18 May 2014

Monica Salgado
Portuguese Lawyer
(Advogado) / Registered
European Lawyer

Janine Regan
Solicitor

Monica Salgado



Monica is a Portuguese qualified Lawyer and a Registered European Lawyer with experience assisting clients with the most varied data protection issues, both in Portugal and the UK.

She has notably assisted clients preparing submitting registrations and requests for authorisation with relevant data protection authorities, analysing processor / controller agreements - including conducting previous due diligence procedures - and trans border flows of personal data.

Monica has also participated in preparing replies to subject access requests and other data protection related requests, implementing data protection compliance measures and tools, including drafting relevant data protection policies, performing data protection compliance assessments, providing data protection training and also assisting business to comply with E-Privacy rules, notably by conducting cookies audits, drafting cookies policies and implementing cookies consent tools.

Monica is a regular speaker on Speechly's webinars and external data protection events, such as the Privacy and Data Protection Conference, and also contributes regularly to internal and external publications, including the PDP journal.

"provides top-notch client service"
Legal 500, 2011



2 EU data privacy compliance for US driven projects | 18 May 2014 Speechly Bircham

JANINE REGAN- CIPP/E



Janine advises on global data protection compliance and outsourcing projects for multinationals in sectors such as financial services, pharmaceutical, construction and marketing and advertising.

She advises on filings with relevant data protection authorities, processor / controller agreements, trans-border flows of personal data, data breaches, data protection provisions in outsourcing contracts and has provided tailored training for clients and for PDP training.

Janine is a regular presenter on Speechly Bircham's data protection webinars and contributes regularly to internal and external publications such as Data IQ, the Society of Corporate Compliance and Ethics, the Society for Computers and Law and Bloomberg BNA.

She also possess the Certified Information Privacy Professional (Europe) (CIPP/E) qualification.



3 EU data privacy compliance for US driven projects | 18 May 2014 Speechly Bircham

OUR TEAM

- Speechly Bircham is an ambitious, full-service law firm with over 250 lawyers, headquartered in London. We work with business and private clients across the UK and internationally and focus on the financial services, private wealth, technology, real estate and construction sectors
- We have offices in Paris, Luxembourg, Zurich and Geneva
- Our Data Protection & Information Law team provide a range of expertise on data privacy audit, compliance, risk management, information security and data breaches
- We are listed in Chambers 2014 and Legal 500 as a leading law firm for Data Protection and have advised on this area of law since 1983
- *"What I liked was the fact that the team was very willing for us to see itself as an extension of our existing in-house team. I like the way it integrated – members sat alongside and guided us. That was what impressed."*
- *"Robert Bond and his team have always provided comprehensive, practical advice on a timely basis. Their knowledge of the EU regulatory scene, including experience with specific agencies, as well as privacy issues globally has been instrumental in establishing our privacy policies and procedures."*

4 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham


TOPICS

- **What are we going to do?**
 - Introduction to the privacy map
 - 10 steps to take when outsourcing the processing of personal data
 - Changing requirements and obligations under the proposed general data protection regulation
 - Scenario 1 – outsourced global human resources database
 - Scenario 2 – outsourced marketing database
- **What will we achieve?**
 - An understanding of the main data privacy concerns when outsourcing the processing of personal data
 - Sharing of experiences dealing with US driven international projects
 - Achieving a better understanding of local concerns and constraints
 - Ultimately (and ideally), improving procedures regarding international data privacy compliance and outsourcing projects

5 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham


PRIVACY MAP – COMPLEXITY OF LEGAL REQUIREMENTS – US VIEW:



6


SpeechlyBircham

PRIVACY MAP – COMPLEXITY OF LEGAL REQUIREMENTS – IN REALITY...LEAST STRICT COUNTRIES:




7 SpeechlyBircham

PRIVACY MAP – COMPLEXITY OF LEGAL REQUIREMENTS – IN REALITY...MODERATELY STRICT COUNTRIES:




8 SpeechlyBircham

PRIVACY MAP – COMPLEXITY OF LEGAL REQUIREMENTS – IN REALITY...VERY STRICT COUNTRIES:




9 SpeechlyBircham

BUT IT DOESN'T END WITH EUROPE...



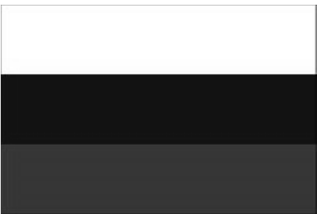
10 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

ARGENTINA



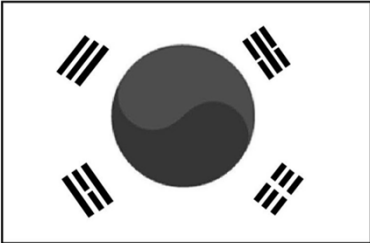
11 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

RUSSIA




12 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

SOUTH KOREA



13 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

...AND THAT'S JUST TO NAME A FEW!!



Malaysia Singapore Taiwan


14 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

First, let's dispel a myth...

"The Outsourcer will comply with all of its obligations under applicable data protection law"

= MEANINGLESS!




15 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

1. Assess vendor's security measures before they are engaged

- Certifications?
- Incident management procedure?
- Information Security policies?
- Human resources?
- Data Security
- Authentication & Access Control
- Network Security
- Physical Security
- Vulnerability and Risk Management
- Backup and Disaster Recovery
- Sub-processing?




16 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

2. Ensure that the contract contains at least the mandatory provisions that are required under EU data protection law

- The processor acts in accordance with the instructions of the controller
- The processor shall implement the appropriate security measures to protect the personal data
- The processor shall ensure the reliability of its personnel handling the personal data

The contract must be in writing!




17 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

3. Assess whether any other appropriate data protection provisions ought to be inserted in the contract?

- Restrictions on data transfers
- Restrictions on sub-processing
- What if they have a data breach?
- Deleting and returning data at the end of the contract?
- Right to audit



18 EU data privacy compliance for US driven projects | 18 May 2014 SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

4. Check other clauses in the contract which may be impacted because of data privacy law requirements

- An obligation for the data processor to comply with all of its obligations under data protection laws with regards to the client's personal data
- Too broad force majeure clause
- "Data loss" liability excluded or highly restricted
- SLAs that do not allow to get your personal data on time



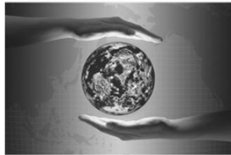
19 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

5. Check where in the world personal data will be processed

- Clarify all parties have the same understanding of the term 'processed'
- Safe Harbor certificate?
- Model contracts?



20 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

6. Ask the vendor whether any processing of personal data is sub-contracted

- Very complex in cloud provision contracts
- Less sophisticated vendors will not have this information on hand
- Reflect the authorised subcontracting chain in the agreement
- Build with your vendor a practical mechanism to subcontract which allows you to comply with your data protection obligations



21 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

7. If sub-processors are located outside of the EU, assess what data transfer mechanisms can be put in place to legitimise the transfer of personal data

- The reality of the data flows
- A matrix of data transfer agreements
- Back-back obligations



22 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

8. Assess whether you need to up-date any notifications/filings with the relevant data protection authorities or obtain approvals from the DPAs before the processing activities commence

- Some DPAs only require "worldwide transfers" to be mentioned
- Some DPAs require certain transfers to be specifically named by country and / or vendor and /or processor
- Some DPAs require all vendors to be fully identified
- Some DPAs require certain types of arrangements to be forwarded to them
- Some DPAs require certain types of arrangements to be approved by them



23 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

9. During the term of the contract, continue to assess the vendor's compliance with security measures

- How often may depend on the type of data processed
- Physical inspections / audits if possible and if the contract provides
- Data security questionnaire



24 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

TEN STEPS TO TAKE WHEN OUTSOURCING THE PROCESSING OF PERSONAL DATA

10. At the end of the contract, ensure that all personal data is returned to you and that all copies are securely and permanently destroyed/deleted
- Use the termination clause
 - Create an exit management plan
 - Consider business continuity and transferability of the personal data to new vendor
 - Create a template certificate of destruction and include as schedule



25 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

CHANGING REQUIREMENTS AND OBLIGATIONS UNDER THE PROPOSED GENERAL DATA PROTECTION REGULATION

- Why those 10 steps will become even *more* important under the proposed Regulation
- Data breach notification requirements
 - Public register of data breaches = increased negative publicity and drop in consumer confidence
 - Fines – 5% of annual worldwide turnover / EUR 1 million
 - Without notice investigations by data protection authorities



26 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

CHANGING REQUIREMENTS AND OBLIGATIONS UNDER THE PROPOSED GENERAL DATA PROTECTION REGULATION

What will change for data processors under the proposed Regulation?

- The Regulation not only applies to data processors located in the EU but it will also apply to data processors located outside of the EU if they process personal data of EU individuals
- All data processors will, for the first time, be required to implement data protection by design and by default when determining the means for processing personal data
- Data protection by design shall be a prerequisite for public procurement tenders



27 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

CHANGING REQUIREMENTS AND OBLIGATIONS UNDER THE PROPOSED GENERAL DATA PROTECTION REGULATION

What will change for data processors under the proposed Regulation?

- The obligations on data processors under data processing contracts will increase substantially, including the responsibility to delete copies of data at the end of the contract and to assist the data controller in the event of a personal data breach
- Data processors will be required to have a **detailed security policy** which, amongst other things, must include: (i) the ability to restore the availability and access to data in a timely manner in the event of an incident that impacts the availability of such data; (ii) the ability to take additional measure in relation to the protection of sensitive personal data; and (iii) a process for regularly testing the effectiveness of security measures and policies



28 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

SCENARIO 1 – OUTSOURCED GLOBAL HUMAN RESOURCES DATABASE



29 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

SCENARIO 2 – OUTSOURCED MARKETING DATABASE



30 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham

FURTHER INFORMATION

For more information on our services, please contact:

Monica Salgado
Monica.Salgado@speechlys.com
+44(0)20 7427 6554

Janine Regan
Janine.Regan@speechlys.com
+44 (0)20 7427 6798



31 EU data privacy compliance for US driven projects | 18 May 2014

SpeechlyBircham
