CharlesRussell Speechlys

Top tips for managing global data privacy compliance

Robert Bond, CCEP, Head of Data Protection & Cyber Security Law Group

charlesrussellspeechlys.com

Who we are

- Headquartered in London with offices in the UK, Europe and the Middle East, with an international network of data protection experts
- Our Data Protection & Cyber Security team has vast experience advising on, and managing, data privacy compliance programmes for multi-nationals
- The team, recognised in legal directories as one of the leading data privacy practices in the UK, is headed by Robert Bond who is listed in band one in this area in Chambers 2015
- We have a number of dual-qualified and multilingual lawyers with significant experience advising on global data privacy compliance projects

"What stands out is their commercial legal help and an immense can-do attitude... They're great problem solvers."
Chambers UK, 2016

"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."
Client

Robert Bond, CCEP
Partner

Tel: +44 (0)20 7427 6660
robert.bond@crsblaw.com

Robert Bond has over 37 years' experience in advising national and international clients on all of their technology, data protection and cyber law requirements. He is a legal expert and author in the fields of e-commerce, computer games, media and publishing, data protection, information security and cyber risks.

He is named in the National Law Journal's list of 50 Governance Risk & Compliance Trailblazers, listed in the top 10 in “the Who’s Who of Information Technology Lawyers 2015” and also in "Best Lawyers in UK 2016“.

"astounding" **Legal 500, 201**5

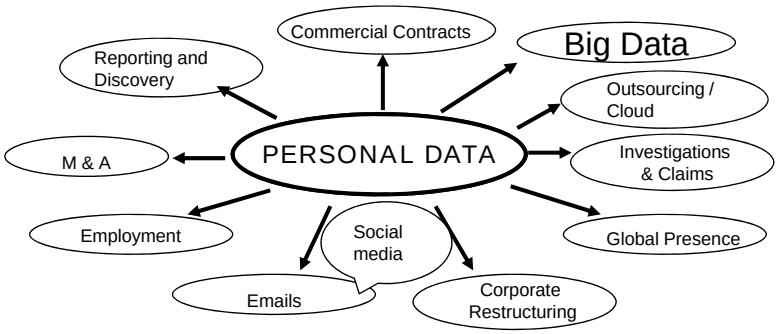
"absolutely exemplary" and the fact that his knowledge of data protection law is "astounding, and his application equally impressive."

Chambers UK, 2016

Topics

- Current hot topics in data privacy and cyber security
- Making data privacy compliance a core ethical and compliance issue for the Board
- What the future holds for data protection and how to prepare for it

Data protection is at the heart of any business



CRS | CharlesRussell Speechlys

HOT TOPICS OF THE MOMENT

CRS | CharlesRussell Speechlys

Often the biggest threat is ourselves

PROTECTION OF PERSONAL INFORMATION…

•… is nothing new

- Right to privacy according to Samuel Warren and Walter Brandeis
  - 1890
  - Right to be let alone
- European continental countries – right to privacy embedded in early constitutions
  - "Private life" referred in the French Constitution of 1791
  - Portuguese Constitution of 1822 set up the secrecy of letters
- Greatest recent examples of misuse of personal information
  - WW2 German occupied countries
  - 20th century European dictatorships
- **Privacy of personal information is not exclusive of the internet connected era!**

AND THEN IT GOT COMPLICATED!

- Advent of computerised world: storage / exchange of large quantities of information
  - Facilitated
  - Lost the strong connection with tangible world
- Data protection legislation developed from the early ’70s onwards
  - Land of Hesse Act (1970)
  - Swedish Data Act (1973)
  - Portuguese Constitution (1976)
- UK – Data Protection Act 1984

CRS | CharlesRussell Speechlys

And now it is more complicated….but don’t panic!

CRS | CharlesRussell Speechlys

LEGAL FRAMEWORK

UNITED STATES	EUROPE	ASIA
About 20 sector-specific laws and hundreds of state laws	EU Data Protection Directive transposed into national law in 28 different member states	Varying national laws loosely based on the European Directive
e.g. HIPAA (The Health Insurance Portability and Accountability Act) and COPPA (Children's Online Privacy Protection Act)	e.g. The UK Data Protection Act 1998, Germany's Federal Data Protection Act 2001 and Italy's Privacy Code 2003	e.g. Malaysian Personal Data Protection Act 2010 and South Korea's Personal Information Protection Act (PIPA) 2011

REGISTRATION/NOTIFICATION REQUIREMENTS

UNITED STATES	EUROPE	ASIA
No requirement for companies to register	Requirements vary but most countries require registration before the processing of personal data	Varies according to country, and in countries such as Malaysia it is dependant on sector
No national Data Protection Authority (DPA)	Each member state has a DPA, but those DPAs have varying levels of expertise, funding and resources	DPAs are generally in their very early stages or operate at a regional level (if they exist at all)

COLLECTION AND PROCESSING

UNITED STATES	EUROPE	ASIA
Vary widely but generally require pre-collection notice and opt-out for use and disclosure of regulated personal information	Data controllers need to meet one of several conditions to collect and process personal data such as: - Consent - Legitimate reason - Performance of a contract - Protecting the data controller's vital interests	Requirements vary across the Asia-Pacific region but the fundamental principles of the European Data Protection Directive can usually be found in the various national laws e.g. purpose definition and use limitation
Opt in rules usually apply where information is considered 'sensitive' e.g. health information, children's information	There are stricter rules for processing sensitive personal data (e.g. gaining a data subject's explicit consent)	Countries such as South Korea, Singapore and Malaysia may take a strict view on how personal data is processed

TRANSFER

UNITED STATES	EUROPE	ASIA
No geographic transfer restrictions apply out of the US	Within the EEA is permitted. There are conditions to be met to transfer data out of the EEA such as: - Consent - Legitimate reason - Performance of a contract - Protecting the data controller's vital interests	Different restrictions apply but many reflect the conditions listed in the European Directive
	'Adequate protection' is required for transfers outside of the EEA e.g. "approved countries", Model Clauses, BCRs and Privacy Shield	APEC Cross Border Privacy Rules

SECURITY AND BREACH NOTIFICATIONS

UNITED STATES	EUROPE	ASIA
Most businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information	Data controllers must take appropriate technical and organisational measures	Varying standards expected – from detailed provisions in South Korea to more general expectations in Malaysia and Singapore
HIPAA regulated entities are subject to much more extensive data security requirements	These measures are aimed to prevent unauthorised processing, accidental loss or damage to personal data	Range from mandatory notifications in South Korea to no notifications in Singapore and Malaysia
Breach notifications are commonplace across the States	No mandatory breach notifications under the Directive but different obligations across Europe are in force	

ENFORCEMENT

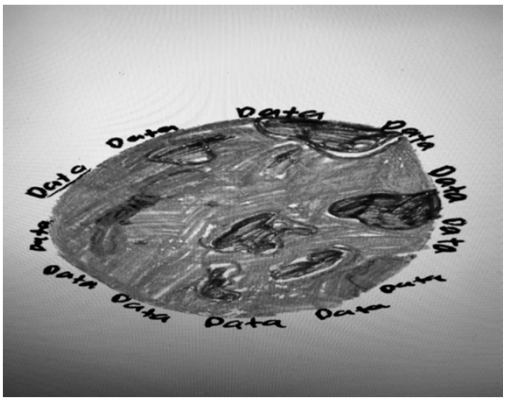
UNITED STATES	EUROPE	ASIA
Violations generally enforced by the FTC, State Attorney General, or the regulator for the industry sector in question	Violations enforced by each country's respective DPA. Generally range from $'000s to $'000,000s	Violations enforced by each country's respective DPA. May be up to $800,000 in Singapore
Highest penalty - $100m against LifeLock (Dec 2015)	Highest penalty - $4.5m by Portuguese DPA	DPAs in relatively early stages so not much fining history
Possibility of class action lawsuits	Google fined $1.2m by Spain	But some DPAs even provide for imprisonment for relatively minor offences!

Understand jurisdictional privacy frameworks

- Historical influences and empires
- English common law influences
- European civil law influences
- OECD Guidelines
- Convention 108

Appreciate global privacy principles

- Sectoral approach
- Human rights/human dignity
- Protective nationalist approach
- Privacy by design
- Ethics and trust
- Independent regulators
- Government controlled privacy



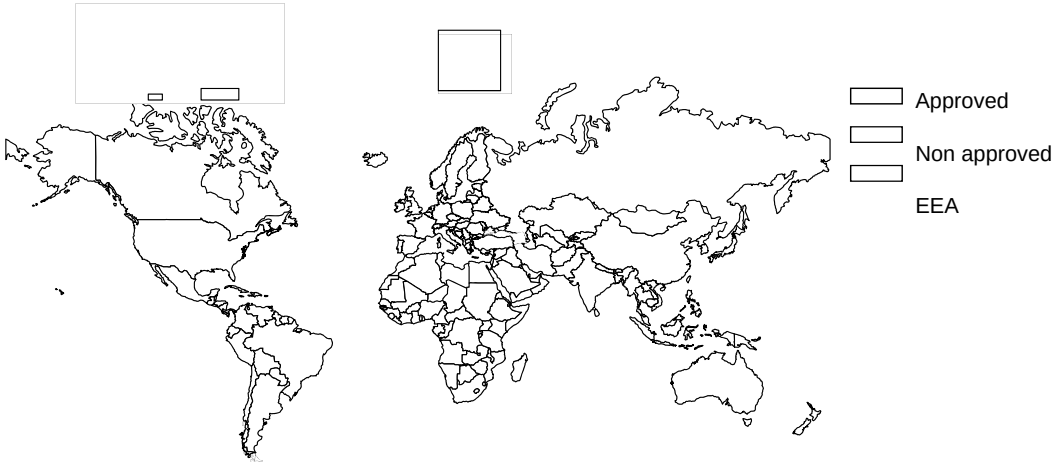
New EU General Data Protection Regulation

- Scope of regime:
  - Wider definition of Personal Data
  - All organisations
  - Pan-European (no local legislation)
  - Extra-territorial application??

New EU General Data Protection Regulation

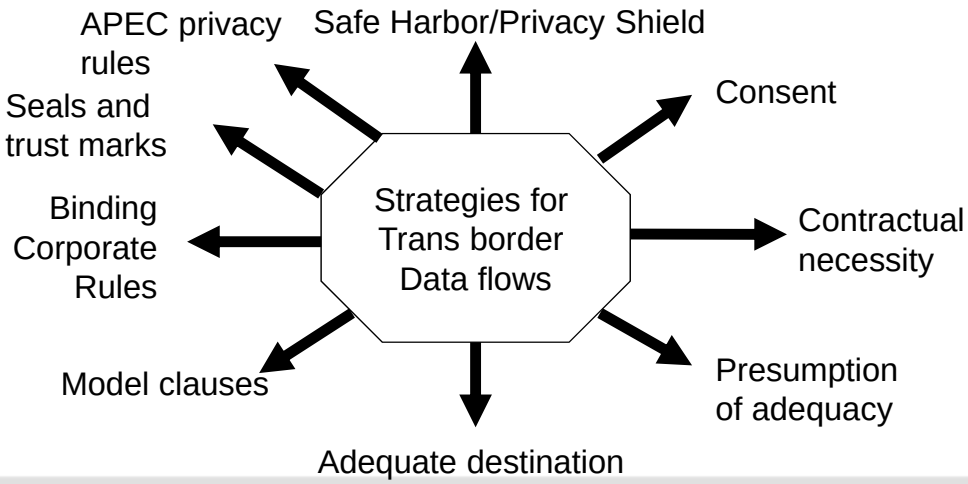
- Definitions of Personal data
- Consent
- Children's (Parental) consent
- Information
- Data Subject rights & access
- Right to be forgotten
- Data portability
- Controller and Processor responsibilities
- Data protection by design and default
- Designation for non-EU controllers
- Documentation
- Breach notification – Regulator & Data subject Privacy Impact Assessments
- Compulsory DPOs
- Certifications and seals
- International transfers
- One-stop shop regulation
- Cooperation and consistency
- EU Data Protection Board
- Fines
- Sector exemptions – e.g. Media & Health

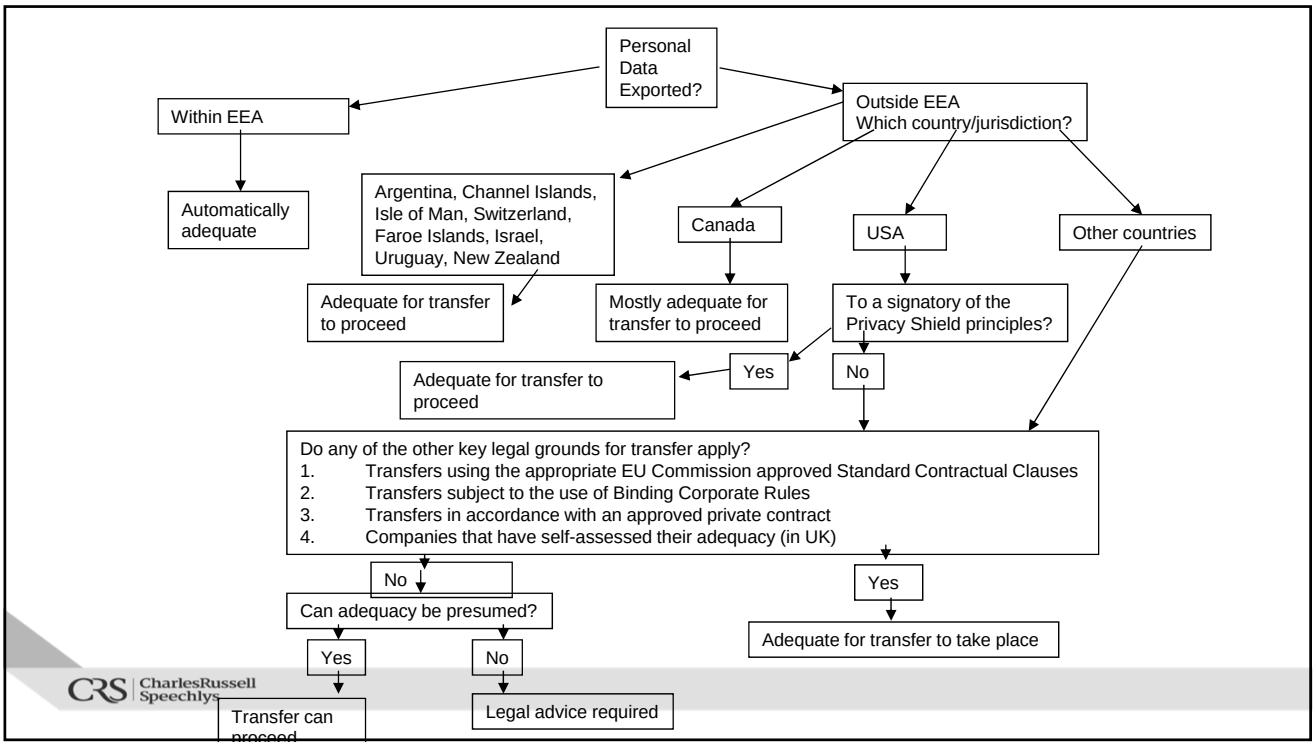
Data transfers – Countries approved by EU



Only countries in green have been approved as providing "adequate protection" for transfer of personal data: Andorra / Argentina / Canada / Faroe Islands / Guernsey / Isle of Man / Israel / Jersey/ Switzerland/ New Zealand/ Israel/ Uruguay

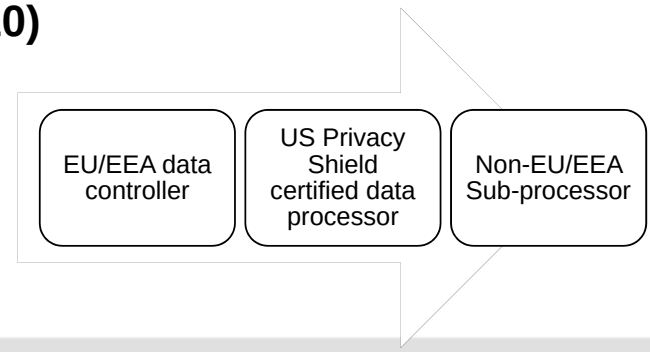
UNDERSTANDING DATA TRANSFER RULES





EU/US Privacy Shield

- Annexe II to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield – **Section II (3)** and **Section III (10)**



CharlesRussell Speechlys

24

EU/US Privacy Shield

- **<u>Section III (10) of Annex II</u>**
- Makes clear that "*data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in the Privacy Shield*" (**section III (10) Contracts for Onward Transfers**)
- Wave this section 10 at US vendors when they push back on your data protection clauses!!

EU/US Privacy Shield

The purpose of the contract (i.e. contract with EU/EEA data controller to non-EU/EEA data processor) is to require the processor to:

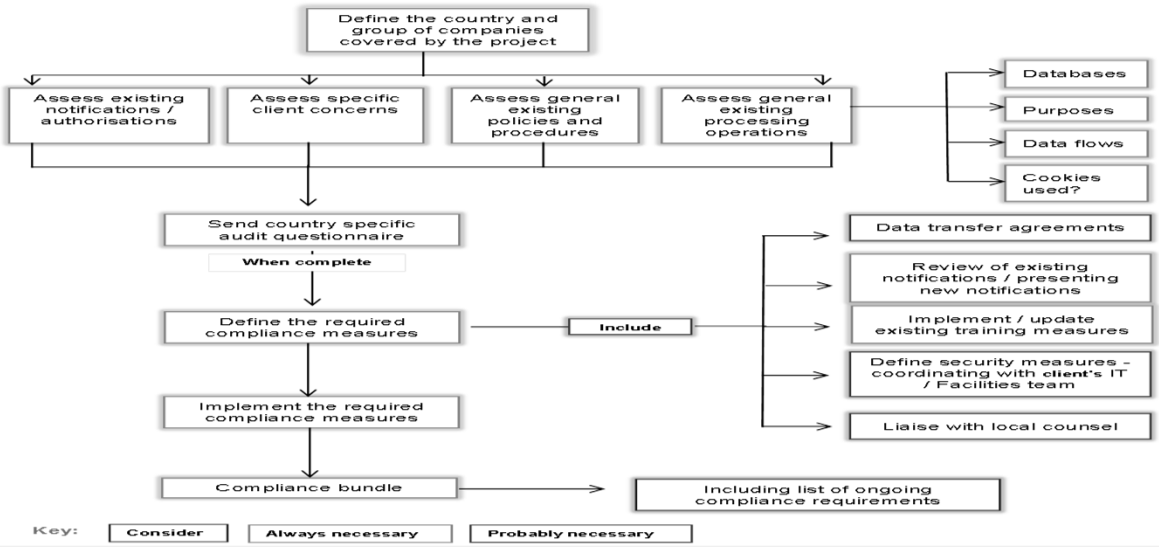
- Act only on instructions from the controller
- Provide appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access
- Taking into account the nature of the processing, assist the controller in responding to individuals exercising their rights under the Privacy Shield Principles

EU/US Privacy Shield

Section II (3) of Annex II - when a US Privacy Shield certified organisations ***sub-processes*** the processing to a third party, it must:

- transfer such data only for limited and specified purposes
- ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles – **must be provided for in contract**
- take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles – **must be provided for in contract**
- require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles – **must be provided for in contract**
- upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing – **must be provided for in contract**
- provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request – ***should*** **discuss this with sub-processor and provide for in contract**

APPROACH TO DATA PRIVACY COMPLIANCE



Questions?

CRS
CharlesRussell
Speechlys

charlesrussellspeechlys.com