W Kuan Hon

EE
Elgar

DATA LOCALIZATION LAWS AND POLICY

The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens

Forewords by Rosemary Jay and Christopher Kuner

Data Localization Laws and Policy

The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens

W Kuan Hon

Solicitor; Editor, Encyclopedia of Data Protection and Privacy*; Fellow, Open Data Institute*

Edward Elgar PUBLISHING

Cheltenham, UK • Northampton, MA, USA

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2017931739

This book is available electronically in the **Elgar**online
Law subject collection
DOI 10.4337/9781786431974

ISBN 978 1 78643 196 7 (cased)
ISBN 978 1 78643 197 4 (eBook)

Typeset by Columns Design XML Ltd, Reading
Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY

Foreword

This new text marks a significant step in the analysis and understanding of the challenges of cloud computing and the protection of personal data. Kuan Hon is particularly well qualified to provide this guide to the issues, having a background in law, technology and the commercial world.

Importantly any work by Kuan is always readable, accessible and lively. These are important features in helping to bridge the gap which can sometimes exist between the academic and the practical work. The range of her experience helps Kuan to bring a broad perspective to the topic.

At the same time of course it examines in real depth the technology and the real, as opposed to the presumed, risks cloud computing can bring and how these can be addressed. Those of us who are weathered practitioners in this area have watched the doctrine that personal data is at risk once it has left the European Union and must be tightly constrained to prevent this risk assume increased importance over the years. There was no such presumption under the Council of Europe Convention (Treaty 108) which led to the UK's first data protection law in 1984. On the contrary, transfers of personal data were permitted but could be stopped if the regulator considered that the data would be at risk in the receiving jurisdiction.

The impulse and justification for Directive 95/46/EC was the need to establish a single market in the Union; the erection of a corresponding barrier to the free interchange of personal data with the rest of the world was something of a sideways consequence. Yet over the years it has become an aim in its own right; the barriers to free interchange have become more and more like an article of faith. Kuan shows how inappropriate those barriers are in today's environment and how little they are associated with real risk.

This text addresses what may seem to be academic issues, but in reality they are far from academic in nature. They impact on every facet of our commercial and social environment. It is a text which skilfully examines the issues and should make us focus on the real issues. It

should be read by every data protection supervisory authority and lawmaker in Europe. Let us hope that it will.

Rosemary Jay
October 2016

Foreword

Kuan Hon's new book deals with a crucial question, namely how to protect personal data that are processed and transferred on the global Internet. Her dual background as a computer scientist and a lawyer allows her to analyse the relevant issues from both the technical and legal perspectives.

There is currently a debate in academia, business and politics about how data protection law should be applied to protect personal data that are processed and transferred across national borders. One set of views has been variously called data localization, data nationalism or informational sovereignty, and refers to the creation of incentives or requirements to localize data processing and storage. The other side rejects such initiatives as incompatible with a free and borderless Internet.

Discussions about data localization have become highly politicized in recent years. Data processing has attained great importance in economic, social and technological terms, and it is not surprising that this is reflected in the political debate. But the politics of the discussion often obscure the important questions that this phenomenon raises. It is the accomplishment of this book to illuminate the substantive legal and technical issues that are at stake in the debate about data localization.

Applicable law and jurisdiction have often been viewed as narrow technical areas of the law of interest only to specialists. As this book demonstrates, they are actually key topics of the information society, since they determine what rights individuals will have in the processing of their personal data, and how these rights can be enforced.

Data localization is not just a short-term phenomenon, but reflects a profound unease with increasing globalization, and a lack of certainty as to whether we want national borders carried over onto the online space. This book helps illuminate the choices that we face as a society in deciding where we want those boundaries to be set.

Christopher Kuner
Brussels, October 2016

About the author

Dr W Kuan Hon MA (Cantab), LLM (UPenn), MSc (Imperial), LLM (QMUL), PhD (QMUL) is an Editor of the *Encyclopedia of Data Protection and Privacy*, a Fellow of the Open Data Institute, a solicitor specializing in data protection law and cloud computing in the City of London and Adjunct Research Director at International Data Corporation (IDC). Formerly a Senior Researcher investigating cloud legal issues at Queen Mary University of London, she devised and taught its first cloud computing law LLM module.

An English solicitor and a (non-practising) New York attorney, Kuan has degrees in law and computing science and a joint law/computer science doctorate. Lead author of eight chapters in *Cloud Computing Law* (OUP 2013, Millard ed.) including four on data protection, she has also published numerous articles.

Formerly a member of the British Computer Society's Information Privacy Expert Panel, Kuan participates in the EU PRISMACLOUD project's user advisory board, and she is an invited observer of the Code of Conduct Task Force of CISPE (Cloud Infrastructure Services Providers in Europe). A UK Cloud Awards judge (2016–17), she was awarded a lifetime professional membership of the Cloud Industry Forum in 2017.

Kuan is a regular presenter at events, including for CERN, the Cloud Security Alliance and ENISA, and has been quoted and interviewed in the media.

Preface

Across the world, countries are introducing more – and more stringent – data localization laws, requiring certain digital data to be kept within equipment physically located on national soil, with limited exceptions. This increasing trend threatens digital globalization. Data localization laws are major barriers holding organizations back from using cloud computing, despite cloud's acknowledged benefits. Data localization is touted in the name of preserving individuals' privacy, which is of course an important goal. However, better ways exist to safeguard privacy and protect individuals' personal data from both corporations and governments, whether of individuals' own countries or other countries. These better ways should be developed further, instead of always focusing on data localization, which I argue is the wrong solution for privacy.

Calls for further and tighter data localization laws were spurred particularly by contractor Edward Snowden's revelations in 2013 ('Snowden's revelations') of mass collection and interception, by the US National Security Agency (NSA), the UK intelligence agency (GCHQ) and other authorities, of the digital data of many countries' citizens. Underlying these calls is the understandable aim of protecting a country's residents from excessive surveillance by other countries' authorities. However, far from data localization laws achieving their purported aim of preserving privacy and preventing bulk surveillance, the constant emphasis on data localization as the 'one true way' in fact primarily serves to cause other, better ways to be overlooked and, the cynical might suggest, diverts attention away from countries' mass surveillance of their *own* citizens (Ferracane 2015), enabling them to maintain and enhance their ability to surveil (Sargsyan 2016) – and control (Chander and Lê 2015) – their citizens by keeping citizens' data within easier reach (Kuner 2013a).

Taking a multidisciplinary approach, this book demonstrates data localization's dangers by using, as a case study, the EU restriction on international transfers of personal data in the context of cloud computing, as the most pertinent exemplar. However, most of its arguments apply equally to other countries' data localization laws, i.e. cross-border transfers from *non*-EU countries, partly because many non-EU countries have adopted very similar data protection laws. While I analyse the

impact on cloud computing of the international transfers restriction under the Data Protection Directive and General Data Protection Regulation, many of my arguments also apply to cross-border transfers of *non*-personal digital data, and to cross-border transfers in technology sourcing, outsourcing or other transactions *not* involving cloud computing.

This book outlines cloud computing; explains the reasons for its scope, delineating it more precisely; and provides an overview of the DPD and the Restriction. Then, it discusses the Restriction's historical background and objective; analyses the meaning of 'transfer' 'to' third countries; unpicks assumptions underlying the Restriction, showing their inapplicability today; discusses uncertainties and practical problems with the Restriction's 'adequate protection' and 'adequate safeguards' concepts; and highlights compliance and enforcement problems. It then suggests how, given such issues, a different approach would better achieve the Restriction's avowed legislative objective, while being more technology-neutral: notably, focusing on control of access to personal data, particularly intelligible personal data, through emphasizing security and accountability regardless of data location. Where relevant, I also discuss other privacy-related policy objectives that may now underlie the Restriction's invocation, showing how they, too, are not necessarily advanced by restricting data location.

This book reflects the position as at October 2016. Developments thereafter are not covered unless stated, but updates (and links to many references cited here) are available from www.e-elgar.com/data-localization-laws-and-policy-companion-site.

W Kuan Hon, http://www.kuan0.com
London, October 2016

Acknowledgements

I dedicate this book to Erica Wells and Siobhan Ward, who have enriched my life immeasurably. I wouldn't be anywhere without you. Thank you so much for your unstinting love, friendship and support throughout the years. I thank Grace Yeoh, too, for her constant friendship since our schooldays.

This book is also dedicated to my inspirational early career mentors, Richard Bethell-Jones and Richard Newton-Price. To me, they set the standard in legal expertise and professionalism, in focus and clarity of thought. In particular, I have always sought to emulate Richard Bethell-Jones's uniquely transparent and accessible writing style. I am also very fortunate to have had the privilege of working with Robin Parsons, Jonathan Rushworth and Jenifer Williams in my past finance/insolvency life, whose leadership and support I very much appreciated.

In writing this book I stand on the shoulders of giants, and I must mention Christopher Kuner's seminal writings on international data transfers. I also learned much about practical data protection from the works of Rosemary Jay. I am honoured that they are contributing Forewords.

I am also grateful to Chris Reed, Hamed Haddadi, Chris Marsden and Toktam Mahmoodi for their invaluable guidance and insight, Christopher Millard and Ian Walden for the opportunity to participate in Queen Mary University of London cloud projects, Robin Callendar-Smith, Marc Dautlich and Sarah Cameron for their continuing encouragement, and Louise Townsend for her thoughts regarding security measures in adequacy criteria.

Finally, I thank the European Commission, Council and Parliament, EU Fundamental Rights Agency, Datainspektionen (Sweden), Datatilsynet (Denmark), the Information Commissioner's Office (UK) and Gartner for their helpful responses to my queries.

Abbreviations/glossary

1990-Proposal	1990 DPD draft, COM(90)314 final – SYN 287
1992-Proposal	1992 DPD draft, COM(92)422 final – SYN 287
2010 Decision	Commission Decision 2010/87/EU
2010 SCCs	SCCs under 2010 Decision
AEPD	Agencia Española de Protección de Datos, Spain's DPA
APEC	Asia-Pacific Economic Cooperation, comprising 21 countries
Authority, authorities	governmental authority(ies), whether law enforcement or intelligence/security
AWS	Amazon Web Services, Amazon's cloud services arm
BayLDA	Bayerisches Landesamt für Datenschutzaufsich, Bavaria's DPA
BCRs	binding corporate rules
CAHDATA	the Ad hoc Committee on data protection, established by the CoE's Committee of Ministers
CBP	College bescherming persoonsgegevens, Netherlands' DPA (former name)
CDN	content delivery or distribution network – p. 105
Ch.	chapter of this book
chap.	chapter of a cited reference
Charter	the EU Charter of Fundamental Rights
CIA	confidentiality, integrity and availability – 7.1.2
CIDPR	Community institutions' data protection regulation, Regulation (EC) 45/2001
CJEU	the Court of Justice of the European Union, formerly the ECJ

CNIL	Commission nationale de l'informatique et des libertés, France's DPA
CoE	Council of Europe
Commission	European Commission
Community	European Communities, the EU's predecessor
Controller	data controller within the DPD's Art.2(d)
Convention108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108)
Convention108-AP	Additional Protocol to Convention108
Convention108-APER	Convention108-AP's Explanatory Report
Convention108-ER	Convention108's Explanatory Report
Council	EU Council of Ministers
Council [number/year]	Pre-legislative Council document, under the heading Official documents – EU, sub-heading Council, in the Table of Legislation
CP	the Council's common position on the draft DPD, 1995/1/EC
CP-SR	the CP's statement of reasons
CPVP	Commission for the Protection of Privacy (Commission de la protection de la vie privée), Belgium's DPA
Data protection	data protection under the DPD/DPD Laws
Data subject(s)	individuals whose personal data are regulated under the DPD/DPD Laws
Datainspektionen	Sweden's DPA
Datatilsynet	Denmark's DPA
DoC	US Department of Commerce
DPA(s)	EEA data protection authority (national supervisory authority overseeing regulation of its DPD Laws). This may include, at EEA level, WP29
DPD	Data Protection Directive 95/46/EC
DPD Laws	national laws implementing the DPD, e.g. the UK Data Protection Act 1998

ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECJ	the European Court of Justice, now the CJEU
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EEA controller	controller incorporated in a Member State – p.9, n.20
Effective jurisdiction	a country's claimed jurisdiction to apply its laws to situations, which is enforceable in practice – p.7–8
ENISA	the EU's Agency for Network and Information Security
EU	European Union
Export	transmitting data to third country-located infrastructure
FISA	US Foreign Intelligence Surveillance Act
fn(n).	footnote(s) in cited reference
FRA	EU Fundamental Rights Agency
FTC	US Federal Trade Commission
Garante	Garante per la protezione dei dati personali, Italy's DPA
GATS	General Agreement on Trade in Services 1994
GCHQ	Government Communications Headquarters, the UK's security/intelligence agency
GDPR	General Data Protection Regulation (EU) 2016/679
GDPR's Restriction	GDPR provisions (primarily in its Chapter V) restricting international transfers (1.6.3), which will replace the Restriction
GPEN	Global Privacy Enforcement Network, whose members include many DPAs and other authorities internationally
Harborite	organization self-certified under Safe Harbour

Hardware	physical media and/or equipment housing/transmitting data: servers, storage appliances, portable drives, laptops, cables, etc.
IaaS	Infrastructure-as-a-Service
IAPP	International Association of Privacy Professionals
ICC	International Chamber of Commerce
ICO	Information Commissioner's Office, UK's DPA
Infrastructure	infrastructure for processing data, including datacentres and hardware
Intelligible access	access to personal data in intelligible form, i.e. to information contained in personal data – p.7
Mechanism	Mechanism for allowing transfers under adequate protection or adequate safeguards e.g. the Shield, SCCs (DPD), or adequate protection or appropriate safeguards (GDPR), as the context requires
Member State(s)	EEA Member State(s)
Microsoft warrant case	case against Microsoft in the US – p.93
n(n).	footnote(s) of this book
NIST	US National Institute of Standards and Technology
NSA	US National Security Agency
OECD-ExplanMem	Explanatory Memorandum to the OECD Guidelines
OECD Guidelines	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980
OECD Guidelines-2	OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013
Onward transfer(s)	transmission of transferred personal data from a third country 'to' another third country; sometimes, to others in the same third country
OPC	Office of the Privacy Commissioner of Canada, Canada's federal DPA
PaaS	Platform-as-a-Service
Parliament	European Parliament

Participant	Member State under DPD/CIDPR, party under Convention108/Convention108-AP, member country under the OECD Guidelines
PCPD	Office of the Privacy Commissioner for Personal Data, Hong Kong's DPA
PDPC	Personal Data Protection Commission, Singapore's DPA
PIPEDA	Canada's Personal Information Protection and Electronic Documents Act
Principles	substantive principles aimed at protecting personal data, stipulated under DPD and DPD Laws (excluding the Restriction and security requirements, not considered herein to be substantive principles)
Processing	processing of personal data within DPD Art.2(b); includes storage, transmission
Processor	processor within DPD Art.2(e)
Processor agreement	controller-processor agreement/contract under Art.17 DPD
Rec.	Recital
Restriction	the restriction on 'transfer' of personal data 'to' 'third countries', under Arts.25–6 DPD
SaaS	Software-as-a-Service
Safe Harbour	EU–US Safe Harbour scheme, under the Safe Harbour Decision
Safe Harbour Decision	Commission Decision 2000/520/EC
SCCs	standard contractual clauses (model clauses) in Commission Decisions promulgated under DPD Art.26(4)
Sensitive data	'special category' personal data under DPD Art.8, e.g. health data
Shield	EU–US Privacy Shield, under the Shield Decision
Shield Decision	Commission Decision (EU) 2016/1250, approving the Shield
Shield participant	organization self-certified under the Shield
SLAs	service level agreements (p.270, n.22)

SMEs	small/medium-sized enterprises
Snowden('s) (revelations)	former NSA contractor Edward Snowden's revelations in 2013 of mass acquisition, interception and surveillance of data by the NSA, GCHQ and other governmental intelligence/security authorities, widely reported since Greenwald and MacAskill (2013)
SSRN	Social Science Research Network
Strongly encrypted	secure against decryption for most practical purposes most of the time in the real world; in particular, encrypted, and keys secured, to recognized industry standards and best practices – 7.2.3.3.5, p.286
TBDF	transborder data flows
Third country	non-Member State country
TPB	The Pirate Bay file-sharing service (7.5.1.1)
Transfer	'transfer' of personal data within DPD Arts.25–6
Transmission	data conveyance, intra- *or* extra-EEA
VM	virtual machine (p.105 n.57)
Whitelisted country(ies)	country(ies) found 'adequate' under a DPD Art.25(4) Commission decision
WP29	Article 29 Data Protection Working Party, established under Art.29 DPD
WP[number]	WP29 working paper (opinion), see References – e.g. *WP196*

Table of cases

COURT OF JUSTICE FOR THE EUROPEAN UNION

NATIONAL COURT CASES

Ireland

United Kingdom