fieldfisher

Fieldfisher Report:

Managing Global Data Residency Risk

MARCH 2015

Introduction

We live in an "always on", interconnected, data-hungry world. Our personal data is collected by our computers, our phones, and our wearables (and goodness knows what else) and transferred, in the blink of an eye, over Internet pipes to third party servers in countries all around the world. Once there it is stored, analysed, shared, monetised and subjected to a thousand other processing operations that most of us have little knowledge about nor the time to investigate and understand.

There are positives and negatives to the Information Age in which we live. We receive wonderful, informative online services for "free", but our personal data is profiled for the advertising that funds the majority of websites we visit. Cloud services enable access to our files in any place, at any time and from any device, yet concerns persist about the security of data hosted and which third parties may be accessing it. Law enforcement can better identify and prevent would-be perpetrators of terrorist activities, but reportedly do so using communications surveillance techniques that risk having a "chilling effect" on free speech and individual liberties.

Are these the unavoidable consequences of being connected citizens in Internet world? Or, through careful legislation and regulation, can societies promote the positives and discourage the negatives of the data economy? This is the ethical, political and legislative debate that has taken place for many years now, and will continue for many years to come, with vocal proponents and advocates representing the full spectrum of views across government, industry and civil society.

In its early years, the Internet was heralded for breaking down borders between countries, encouraging the spread of information, new business models and even democracies. But, in the wake of the revelations by NSA whistleblower Edward Snowden, combined with growing mistrust between certain countries on a wider geopolitical level, new borders have begun to be erected.

European Union countries have become increasingly concerned about the need to protect European citizens' data when ingested by digital giants in large offshore data centres, with some calling for an abandonment of the US-EU Safe Harbor framework; others going even further and calling (without, it must be said, much consideration as to the practical consequences) for a "European-only" Internet.

Similarly, many other countries have begun to introduce "EU-style" data residency rules (sometimes called data sovereignty rules), prohibiting businesses from moving the personal data they collect out-of-territory unless certain legal standards are fulfilled. It is an interesting statistic to note that, in 2011, 76 countries had data protection laws; by September 2013, that number had risen to 101 countries, with at least 20 more countries with data protection bills on the books.[1] **The trend is clear – the adoption of data privacy laws is accelerating worldwide; and, with that, so too will the adoption of data residency rules**.

About this report

This report compiles our research across 47 key territories worldwide to explore which of those territories have data residency rules (if you're wondering, 94% do!), and the potential for penalties where companies do not comply with these rules (in 89% of cases, local regulators can impose sanctions).

Specifically, it also explores whether the adoption of a binding business-wide data governance framework known as "Binding Corporate Rules" (explained later in this report) enables businesses to overcome these data export restrictions. Originally an EU-invented solution to the issue of managing global exports of data, this report demonstrates that the vast majority of worldwide countries surveyed (including non-EU countries) now recognize BCRs as a valid way to fulfil their local data residency requirements.

We intend this report to be a living and breathing document that we will expand and refresh in future years, so that it will serve as a valuable resource to global businesses looking to make strategic decisions about how to manage their international data exports.

We hope you find it useful, and welcome any and all feedback.

Phil Lee
Head of US Office and Partner, Privacy and Information Law
Fieldfisher

m +1 (650) 842 0821
e Phil.Lee@fieldfisher.com

> The trend is clear – the adoption of data privacy laws is accelerating worldwide; and, with that, so too will the adoption of data residency rules.

1. See research by Graham Greenleaf, University of New South Wales, Faculty of Law: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877

What You Need To Know About Global Data Residency Rules

- "Data Residency" refers to national laws that prohibit organisations from transferring personal data outside of their country or region unless certain legal standards are met.
- With the assistance of local privacy experts, Fieldfisher has analysed Data Residency rules in 47 countries across 6 geographical regions.
- In 94% of the countries analysed, organisations must satisfy Data Residency rules to transfer personal data abroad.
- In the overwhelming majority of countries analysed, the golden rule is that personal data can only be exported where the importing country or region ensures a level of data protection that is equivalent to local standards.
- Regulators and lawmakers increasingly view Binding Corporate Rules ("BCRs") as an effective mechanism for satisfying this equivalency requirement for international transfers of personal data within global organisations.
- 89% of the countries analysed recognise BCRs as a valid solution to local Data Residency requirements.
- In 89% of the countries analysed, the data protection regulators have the power to impose sanctions for failure to have in place appropriate Data Residency solutions.

The Report

Introduction

The revelations made by former US National Security Agency ("NSA") contractor and whistle-blower Edward Snowden in the summer of 2013 further fuelled existing legal, political, ethical and commercial debates regarding the cross-border access and transfer of classified data.

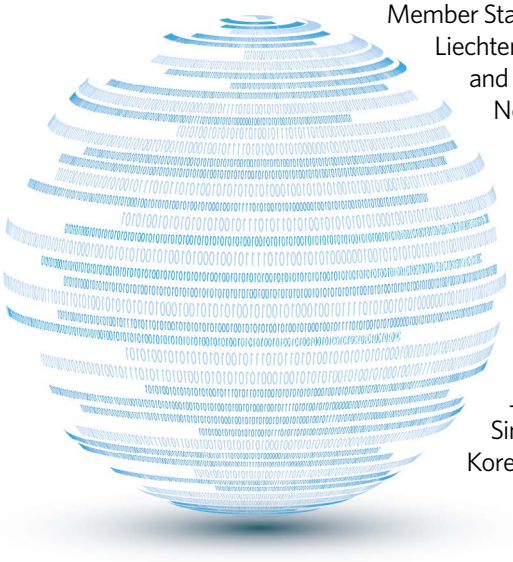
These debates have a significant impact upon national data privacy laws, as policy-makers continue to assess the sufficiency of existing legal protections for international data transfers. Indeed, two particularly notable results of this post-Snowden stock-taking have been the ongoing discussions around the future of the US-EU Safe Harbor framework and a growing trend towards stricter data residency requirements in the EU and beyond, with countries like Russia and Australia announcing new, high profile, data residency rules.

Quite simply, the cross-border transfer of personal data has rarely (if ever) been under such scrutiny from regulators, the press and individual citizens. Against this backdrop, the Fieldfisher Privacy and Information Law team (with assistance from our network of local privacy practitioners) has assessed and analysed the status of Data Residency rules in key jurisdictions across the globe.

In doing so, we hope to shed some light on a much-discussed but seldom analysed topic by setting out the report's methodology and responding to the following five key questions – (1) What are Data Residency rules? (2) How many countries have Data Residency rules in place? (3) What are the most common legal grounds to transfer personal data abroad? (4) Are Binding Corporate Rules ("BCRs") a recognised means of satisfying Data Residency rules and transferring personal data abroad? (5) What are the Data Residency enforcement risks?

Methodology of report

In late 2014, Fieldfisher analysed the national laws in relation to Data Residency and data transfers in 47 countries across 6 geographical regions – Europe (28 EU Member States plus Iceland, Liechtenstein, Norway and Switzerland); North America (United States and Canada); South America (Argentina, Brazil and Uruguary); Asia (China, India, Israel, Japan, Malaysia, Singapore and South Korea); Africa (South Africa); and Oceania (Australia and New Zealand).



In early 2015, we compiled, cross-referenced and cross-checked our analysis in an attempt to build up a truly global picture of Data Residency rules. This Report represents the culmination of our work. We plan to update this Report in future years to ensure its ongoing accuracy and expand the scope of its geographic coverage.

What are Data Residency rules?

The term Data Residency is undefined in most national laws. However, in broad terms, it refers to national data protection laws which prohibit organizations from transferring personal data outside of their country or region unless certain legal standards are met.[2]

The best known example of a Data Residency rule is the EU's Data Protection Directive which prohibits organizations from transferring personal data to recipients outside of the EU unless they ensure an "*adequate*" level of protection for the personal data e.g. by signing so-called "standard contractual clauses", self-certifying under the US-EU Safe Harbor framework or implementing Binding Corporate Rules for intra-group transfers of data. Other examples include countries like Canada, Australia, Israel, and South Korea, all of which have similar Data Residency Requirements.

How many countries have Data Residency rules in place?

44 out of the 47 countries analysed have Data Residency rules in place, demonstrating that compliance with these requirements is a global issue and one that presents a significant challenge for business. This is particularly the case for data-intensive businesses, such as enterprise and consumer cloud service providers, online social media companies, and large life sciences and healthcare conglomerates.

The United States, South Africa and New Zealand were the only countries analysed which do not currently have Data Residency rules in force. The United States has sectoral restrictions but no cross-cutting transfer restrictions. With regard to South Africa, although there is some constitutional and sectoral legislation which covers privacy rights, there is no specific data privacy legislation in force as of yet. The Protection of Personal Information Act 4 of 2013 ("POPIA") was adopted by the South African government on 26 November 2013 as the national data privacy law. However, the South African government has yet to confirm the date for the POPIA's entry into force.

With regard to New Zealand, the Privacy Act 1993 does not contain a prohibition on the international transfer of personal data. However, the New Zealand Law Commission has recommended the introduction of formal accountability rules relating to international disclosure and outsourcing of personal

information. Developments in South Africa and New Zealand would seem to herald the introduction of Data Residency rules in the coming years and thus bring the nations into line with the other analysed countries.

In other words, we can expect these countries – and more – to implement Data Residency rules within the foreseeable future.

What are the most common legal grounds to transfer personal data abroad?

Across the 47 countries analysed there is a very broad range of legal grounds on which personal data can be transferred. The principal common legal grounds are as follows:

- If the consent of the data subject to the transfer has been obtained;
- If the transfer is necessary for the performance of a contract between a data controller and a data subject; and
- If the transfer is necessary for law enforcement purposes (though there is significant ongoing debate as to whether foreign law enforcement requests should permit global data transfers).

It is worth noting that many grounds vary according to the type of personal data being transferred and its intended use/purpose. For instance, in Russia, the cross-border transfer of personal data typically requires the written consent of the data subject. Therefore, consideration should always be given to precise local legal requirements whenever transferring personal data abroad.

Are BCRs a recognised means of transferring personal data abroad?

Binding Corporate Rules, or BCRs, can be thought of as an internal data governance policy framework adopted by the business, under which it commits to protect the data it collects and processes to certain required data privacy standards.

BCRs are both internally binding on staff through contractual, policy and disciplinary measures, and externally binding on and between group companies through the use of an intra-group agreement or similar legal mechanism. The policy commitments made by participating group companies must be implemented in practice through appropriate training, vendor management, complaints handling and audit processes.

The concept of BCRs was originally developed by the EU's Article 29 Working Party in order to allow multinational corporations, international organizations and groups of companies to make intra-organizational transfers of personal data across borders in compliance with EU Data Residency requirements. Critically, BCRs must be reviewed and approved by EU data protection authorities, meaning that companies that have successfully achieved BCRs have demonstrated to the regulators a rigorous approach to data protection compliance throughout the organization. A list of companies that have achieved BCRs as at the date of this Report can be found at *http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm*

While BCRs are recognized as a valid way to export data from European Union countries to non-EU countries, a natural question to ask is whether other, non-EU countries recognize and permit the use of BCRs to export personal data in compliance with their local Data Residency rules? This acceptance might, for example, be either through express legislative wording authorizing the use of BCR, or alternatively an 'implicit' acceptance where BCRs are aligned with local Data Residency standards (even if not expressly called out in local legislation) and therefore tolerated by the local regulatory authority.

Of the countries analysed, **42 out of the 47 currently expressly or implicitly recognise BCRs as a valid means to transfer personal data internationally within an organisation**. Such widespread acknowledgement of BCRs demonstrates that they provide a common, one size fits all standard for global businesses needing to transfer data internationally in compliance with national Data Residency rules. **Despite being an EU-originated solution, BCRs have clearly developed to attract much wider recognition and appeal on the global stage.**

What are the enforcement risks?

42 out of the 47 countries analysed have data protection regulators with powers to impose sanctions for failure to comply with Data Residency rules.

The United States, India, Israel, South Africa and New Zealand were the only countries analysed where the regulator currently lacks the ability to sanction Data Residency breaches. With regard to India, the regulator does not have the power to sanction. With regard to Israel, the enforcement powers of the Database Registrar are somewhat unclear and, as of yet, there has not been a case to test its ability to enforce Data Residency rules. The examples of South Africa and New Zealand are discussed above.

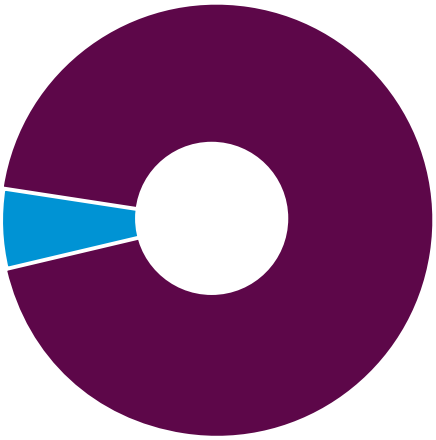
Thus far, regulatory enforcement of Data Residency rules (with the exception of Russia) has been limited. However, due to increasing regulatory sensitivities concerning international exports of data, it is highly likely the cross-border transfer of personal data will be subject to closer scrutiny by data protection authorities going forward.

Perhaps more significantly, businesses that do not have appropriate solutions in place for their exports of international data will increasingly find it difficult to conclude deals and do business in territories with Data Residency requirements. This is already proving the case for many US companies who, in light of ongoing EU tensions about the future of the US-EU Safe Harbor framework, increasingly find EU customers insist upon alternative data export solutions such as Standard Contractual Clauses or BCR.

2. For the purposes of this Report, we have not explored additional sectoral restrictions that may exist under, for example, national financial services or life sciences regulatory regimes.

How many countries have Data Residency rules in place?

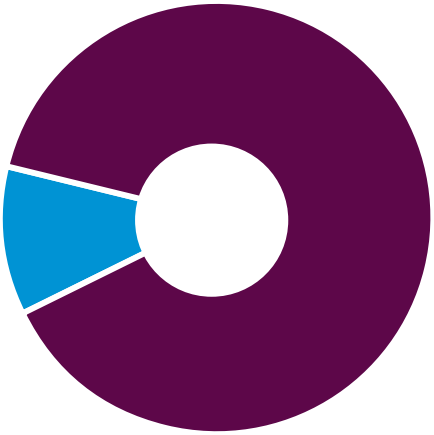
6% of countries analysed do not have Data Residency rules in place



94% of countries analysed have Data Residency rules in place.

Are BCRs recognised as a lawful means of transferring personal data abroad?

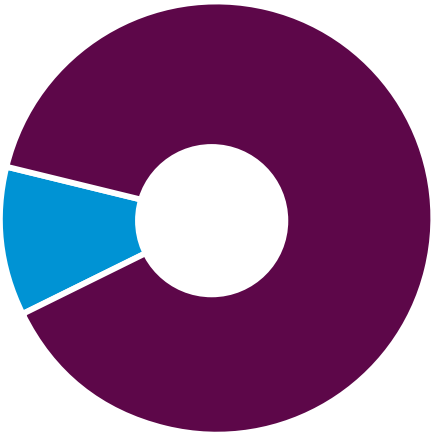
11% of countries analysed do not recognise BCRs as a lawful means of transferring personal data abroad.



89% of countries analysed expressly or implicitly recognise BCRs as a lawful means of transferring personal data abroad.

How many countries have a regulator which can impose sanctions for breaches of Data Residency rules?

11% of countries analysed do not have a regulator which can impose sanctions for breaches of Data Residency rules.



89% of countries analysed have a regulator which can impose sanctions for breaches of Data Residency rules.

Authors

Phil Lee
Head of US Office and Partner, Privacy and Information Law Group
Fieldfisher

m: +1 (650) 842 0821
e: phil.lee@fieldfisher.com
follow: @euprivacylawyer.com
connect: http://uk.linkedin.com/in/phillee77/

Hazel Grant
Head of Privacy & Information Law Group
Fieldfisher

t: +44 (0)20 7861 4217
m: +44 (0)7775 728838
e: hazel.grant@fieldfisher.com

Michael Brown
Solicitor, Privacy and Information Law Group
Fieldfisher

t: +44 (0) 207 861 4843
e: michael.brown@fieldfisher.com
connect: https://www.linkedin.com/pub/michael-brown/39/a56/638

Acknowledgements

Fieldfisher would like to acknowledge and extend its sincere thanks to the following privacy experts whose contributions were invaluable to the creation of this report: Argentina (Gustavo Tanus of TSKS), Brazil (Renato Opice Blum of Opice Blum Advogados Associados), Canada (Kris Klein of nNovation LLP), China (Marissa Dong of Jun He Law Offices), Israel (Omer Tene), India (Jyoti Virmani of Fox Mandal Little), Malaysia (Foong Cheng Leong of Foong Cheng Leong & Co), New Zealand (David Clarke of Russell McVeagh), Russia (Pavel Savitsky of Borenius) Singapore (Lee Xin Mei of Rajah & Tann), South Africa (Dario Milo of Webber Wentzel), South Korea (Chun Y Yang of Kim & Chang), Switzerland (David Rosenthal of Homburger AG), Uruguay (Martin Pesce of Ferrere Attorneys at Law).

Unlocking the value of data

fieldfisher

The amount of data being generated in today's world is phenomenal. Companies are able to understand much more about their customers and business than ever before. This can be crucial to their success. These changes bring risk however, and the need to meet increasingly complex regulations. We help our clients to manage these risks and help them find ways to generate value from the data they hold.

We can help you to:

- Ensure your business complies with data protection laws & minimises any risks.
- Generate value from your data to drive innovation and create operational efficiencies.

What we do

Global data transfers

Many companies benefit from the ability to move and access information globally. It is easy to become an 'accidental exporter' for example when a customer accesses your website from across the world. We help our clients to remain compliant in their global data transfers. From initial auditing through to policy creation and regulatory clearance, we have the expertise to help. We specialise in Binding Corporate Rules, data transfer and sharing agreements, data protection registrations, whistleblowing compliance and compliance assessments.

Compliance with new technologies and e-marketing

We ensure your e-marketing campaigns and new technology products, such as the launch of a new app, are compliant with data privacy laws. We do this through Privacy Impact Assessments to identify needs for improvement or the impact of 'cookie consent' laws for example. We can help with Privacy by Design to ensure the development of your product considers privacy laws from the start to save time and money.

Liaising with regulators

We can help you to liaise with data protection regulators throughout the EU. Our experience means we can help you to take the right approach and communicate in the most effective way in order to get the results you need.

Minimise risks of an incident

Data security incidents are inevitable. Either as consequence of human error or through malicious third party hacking. We help many of our clients to prevent and manage data security incidents. We can help you make regulatory notifications and help minimise the consequences of data breaches.

Negotiations on data protection

We can help to quickly and efficiently settle data privacy negotiations between parties where an agreement cannot be easily met. We take a practical and logical approach to ensure a deal can be agreed on time and on budget.

What we deliver

Peace of mind

We have an exceptional track record of getting it right. We always deliver – on time and on budget.

Managed risk

Our size, reach and experience helps our clients navigate through the turbulence of an increasingly complex regulatory environment. Our approach quickly identifies areas where you could be at greatest risk, and provides you with the best and most efficient solutions.

Efficient implementation

We deliver global data privacy programmes ensuring our clients are compliant regardless of jurisdiction. Our network of privacy specialists in more than 50 countries across the world means we can provide you with the right team and most tailored solutions.

Value generation

Our knowledge and experience means we not only provide legal expertise, but how your business can get the most value out of your data.

About us

fieldfisher

Fieldfisher has a market-leading data privacy practice that is consistently ranked in the Top Tier for data protection in the legal directories. We have a truly international team of specialist lawyers and are rated by buyers of our services as the "go to firm" for expertise, commerciality and client care.

We have worked with some of the biggest brands in the world, advising them on all types of privacy, data protection and security projects. This means that we have a unique perspective of how data protection issues are dealt with by different organisations. Our clients recognise us as thought leaders in this area, and trust us to advise them on the most complex of problems. We provide excellent value for money, advising not only on legal matters but on ways to get the most value out of your data.

We can support you on all aspects of the law, from the development of global or local data protection strategies through to strategy execution, analysis of risk and risk mitigation. We are also adept at handling troublesome regulatory problems, disputes and litigation. We are at our best when faced with new issues.

Our clients

AdRoll
Amazon
Box
Everything Everywhere
Expedia
Netflix
Philip Morris International
RadiumOne
Telenor
Total
VMware
Zendesk

Key facts

18 dedicated privacy lawyers across Europe & the US

A further **50** specialist privacy lawyers in our network around the world

Over **80%** of our data privacy work is international in nature

Led **20%** of all Binding Corporate Rules applications in the world

Our data privacy group is ranked **number 1** in the Chambers legal directory.

Top 4 firm for quality of legal advice
2014 Legal Week Client Satisfaction Survey

Contacts

Hazel Grant
Head of Privacy - London

E: hazel.grant@fieldfisher.com
T: +44 (0)20 7861 4217

I advise on data protection compliance strategies as well as the implementation of privacy-compliant technologies and processes. My experience means I can help you to consider how you can get the best value out of the data you hold.

Felix Wittern
Privacy Partner - Germany

E: felix.wittern@fieldfisher.com
T: +49 (0)40 87 88 69 8 114

I work with our clients to find practical solutions to implementing their EU data protection requirements so they are not only legally compliant, but so that they can use the data in the best way for their business needs.

Phil Lee
Privacy Partner - United States

E: phil.lee@fieldfisher.com
T: +1 (650) 513 2769

I provide "real time" European data protection advice to our US clients. I advise on new technologies, including the cloud, mobile and ad tech. We are the only Privacy and Information Law practice that is able to provide "on the ground" EU data protection advice to our US clients during their working day.

Antonis Patrikios
Privacy Director – London & United States

E: antonis.patrikios@fieldfisher.com
T: +44 (0)20 7861 4354

I work between the UK and US advising our clients on huge and complex global compliance programmes. I help them to manage and mitigate risks, liaise with regulators and law enforcement authorities and deal with data breaches.

fieldfisher