Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Banking in the cloud: Part 3 – contractual issues

W. Kuan Hon [a,*], Christopher Millard [b,c,**]

[a] Privacy, Security and Information Group at Fieldfisher, London, UK
[b] Centre for Commercial Law Studies, Queen Mary University of London, London, UK
[c] Bristows LLP, London, UK

Keywords:
Cloud computing
Cloud providers
Cloud contracts
Banks
Financial institutions
Financial services regulation
Banking regulation
Data protection
EU
European Union

ABSTRACT

This paper looks at EU banks' use of public cloud computing services. It is based primarily on anonymised interviews with banks, cloud providers, advisers, and financial services regulators. The findings are presented in three parts. Part 1 of this paper explored the extent to which banks operating in the EU, including global banks, use public cloud computing services. Part 2 of this paper covered the main legal and regulatory issues that may affect banks' use of cloud services.

Part 3 looks at the key contractual issues that arise in negotiations between banks and cloud service providers, including data protection requirements, complexities caused by the layering of cloud services, termination, service changes, and liability. It also presents the overall conclusion derived from the studies conducted, as set out in the three parts of the paper.

All three parts of the paper can be accessed via Computer Law and Security Review's page on ScienceDirect at: http://www.sciencedirect.com/science/journal/02673649?sdc=2. The full list of sources is available via the same link and will be printed at the end of this part of the article.

1. Introduction

This paper considers the key contractual issues that arise in negotiations between banks and cloud service providers. It first reviews data protection requirements in relation to banks' use of cloud, with a focus on data localisation. It then considers how the layering of cloud services creates complexities for contracts between banks and cloud services providers. In this respect, it considers cloud providers' layered service models (IaaS, Paas, and Saas), as well as the role of integrators. It then reviews the key contractual issues around termination of contract, service changes, and liability.

Finally, the article sets out the overall conclusions derived from the studies presented in all three parts of the paper. It concludes that, while some barriers to cloud adoption by banks are internal and some external, cloud is still misunderstood, and further educational efforts are needed to ensure regulatory approaches and guidance are sufficiently cloud-aware to strike the appropriate balance between risk management on the one hand, and efficiency and innovation, on the other, across the European Economic Area.

* *Corresponding author.* Fieldfisher, Riverbank House, 2 Swan Lane, London EC4R 3TT, UK.
E-mail address: kuan.hon@fieldfisher.com (W.K. Hon).
** *Corresponding author.* Centre for Commercial Law Studies, Queen Mary University of London, Northgate House, 67-69 Lincoln's Inn Fields, London WC2A 3JB.
E-mail address: c.millard@qmul.ac.uk (C. Millard).

https://doi.org/10.1016/j.clsr.2017.11.007
0267-3649/

2. Data protection and data location

2.1. Overview

2.1.1. Data protection compliance concerns

Data protection compliance is a major issue for cloud customers, including banks. EU data protection laws can be strict (Hon et al., 2013d), with different rules in different Member States, and will become stricter under the GDPR. One bank commented that privacy was "too big a problem". Many providers had offered to solve the problem, but regulators need to propose something workable that could reach critical mass, otherwise "it's really a no-go".

The biggest data protection issue arising in cloud (other than security) is data location. According to one provider, data security and location were the top issues raised by its customers and it was "constantly" discussing data location with clients. Another provider said 40% of its customers raise data location, particularly banks. According to a third provider, unless the bank had a good legal team that understood cloud, "the first question everyone asks is location": a big "obstacle".

An adviser commented: "when asked about data residency, those [providers] who can tell you [in] which datacentre [the customer's data is processed], even rack, have a real [advantage]; [certain customers] would [dismiss] others [providers] even if cheaper". Data location is particularly problematic with personal data in cloud (Hon and Millard, 2013c). The problem is compounded in multi-jurisdictional situations, particularly for global banks who need to address privacy and data protection laws in non-EU countries as well.

2.1.2. Data transfers, model clauses, and the Privacy Shield

Data protection regulators such as the Article 29 Working Party (A29WP) interpret restrictions on "transfer" of personal data outside the European Economic Area (EEA) as requiring personal data to be *physically located* in the EEA, i.e. in EEA-located equipment. Remote access from outside the EEA, such as by US support staff, to EEA-located personal data is also generally considered to involve a "transfer". There are exceptions to the transfer restriction, e.g. for national security and law enforcement purposes and some limited derogations, such as unambiguous consent provided by the individuals whose data are to be transferred.

Many cloud providers and their customers have relied on European Commission-approved standard contractual clauses, also known as 'model clauses', to provide "adequate safeguards".[1] However, the Irish Data Protection Commissioner has challenged the validity of the Commission-approved clauses, and the Irish High Court has decided to refer the issue to the Court of Justice of the EU (CJEU) for a preliminary ruling.[2]

Companies may also be able to transfer data under a scheme agreed between the EU Commission and the US Government for transfers to subscribing US organisations. The first such scheme, known as Safe Harbor, went into effect in 2000, but was invalidated by the CJEU in 2015.[3] In July 2016, the Commission adopted the Privacy Shield (C(2016) 4176 final) to replace Safe Harbor. In 2017, the European Commission and the US Government conducted the first annual review of the Privacy Shield, concluding that the scheme provided "a high level of data protection for EU individuals".[4] However, the validity of the Privacy Shield is currently subject to legal challenge in two cases before the CJEU,[5] and this has created further uncertainty to the future of standardised mechanisms for EU-US data transfers.

Following the Snowden revelations of mass surveillance/data collection by US intelligence authorities, transferring data to the US has become a sensitive issue. Some consider it "essential" for cloud customers to know where their cloud provider's servers are based. Even before Safe Harbor's demise, several US providers who had subscribed to Safe Harbor nevertheless offered model clauses that customers could opt in to online, as an alternative (especially in Germany where data protection regulators doubted Safe Harbor's adequacy), or as an addition to Safe Harbor, as "belts and braces".

One provider stated that for certain cloud offerings it always relied on model clauses. This marks a change of approach, as one bank commented that "three years ago, providers wouldn't agree to any data protection language or model clauses; that has changed; model clauses are now [widely-offered], which is better".

The Article 29 Working Party's letter about Microsoft's model clauses arrangements (A29WP, 2014a) may have kickstarted this change. While the letter was positive, the Working Party was careful not to endorse Microsoft's solution. Legal complexities still mean it is difficult for banks to get comfortable that the arrangements will meet regulatory requirements, especially for customer data, a bank said. It took "high jumps" just to aggregate data from certain Member States into one datacentre given their "excessive" requirements, even within the same group, so if negotiating with a third party they'd "leave the table".

Many EMEA countries have their own specific approaches to data localisation and "once you get comfortable with that, you find the regulator going back the other way". For instance, Russia has required the use of local infrastructure (Hon et al., 2016). As noted in part 2 of this paper, regulatory fragmentation can be a barrier to cloud adoption. Accordingly, a

[1] See *Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC* [2001] OJ L181/19; *Commission Decision 2004/915/EC of 27 December 2004 amending decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries* [2004] OJ L385/74; *Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council* [2010] OJ L39/5.

[2] See *The Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems*, 2016/4809P, Judgment of 3 October 2017.

[3] *Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650.

[4] Joint Press Statement from US Secretary of Commerce Ross and Commissioner Jourová on the EU-U.S. Privacy Shield Review, 21 September 2017. Available from: http://europa.eu/rapid/press-release_STATEMENT-17-3342_en.htm.

[5] See cases in progress: *Digital Rights Ireland v Commission*, Case T-670/16 and *La Quadrature du Net and Others v. Commission*, Case T- 738/16.