EU Privacy and Complex Cloud Contracting

The greatest pleasure, and the greatest challenge, of being a privacy lawyer is the need to be both an ethicist and a pragmatist. Oftentimes, we find ourselves advising companies not just on what is the legal thing to do, but what is the right thing to do (and, no, the two aren't always one and the same); while, on other occasions, our task is to find solutions to real or imagined business impediments presented by the law.

The dichotomy introduced by cloud deals

Nowhere is this dichotomy more apparent than when advising on cloud deals. The future is cloud and mobile, as someone once said. So it seems an oddity that privacy laws are all too often interpreted in ways that impair cloud adoption and utilization. This oddity is perhaps most apparent when negotiating cloud deals, where two parties who are in commercial agreement and want to realize the benefits of a cloud relationship are unable to reach contractual agreement over basic data protection terms.

This failure to reach contractual agreement is so often due to a misunderstanding, or (sometimes) a perverse interpretation of, EU data protection requirements, that we thought we'd use this note to set the record straight.

Some questions to ask

The following is necessarily broad brush, but hopefully paints a picture of the key things to consider in cloud deals and how to address them:

1. **What data protection terms does the law require?** In most cloud relationships, the service provider will be a "data processor" and its client the "data controller". In this type of relationship, the client is legally obligated to impose two key requirements on the service provider – first, that the service provider must act only on its instructions; second, that the service provider must have in place "appropriate" security. There's no point negotiating these. Just accept them as a legal necessity and move on.

2. **What about Germany?** Germany is a huge market for Cloud contracting, but its data privacy laws are notoriously strict. If you're a cloud provider rolling out a pan-EU service, you have to address German data privacy requirements as part of your offering or risk not doing business in a major EU market. In addition to the two requirements just described above, Germany also mandates the need for precise "technical and organisational" security measures to be in place for the cloud service and the granting of audit rights in favour of the cloud client. These need to be addressed either within the standard EU ts&cs for the cloud service or, alternatively, by way of bespoke terms just for German deals.

3. **Should there be audit rights?** Yes, that's right. Certain EU territories, like Germany, expect that cloud clients should have audit rights over their cloud providers. To most cloud providers, the idea of granting audit rights under their standard terms is an anathema. Imagine a provider with thousands of clients – you only need a small fraction of those clients to exercise audit rights at any one time for the business disruption to be overwhelming. Not only that, but allowing multiple clients onsite and into server rooms for audit purposes itself creates a huge security risk. So what's the solution? A common one is that many cloud service providers have these days been independently audited against ISO and SSAE standards. Committing in the contract to maintain recognised third party audit certifications throughout the duration of the cloud deal – possibly even offering to provide a copy of the audit certification or a summary of the audit report – will (and rightly should) satisfy many cloud clients.

4. **And data residency?** The old "European data center" chestnut. We've been in more than a few negotiations where there's been a mistaken belief that the cloud service provider needs to host all data in Europe in order for the service to be "legal" under European data protection law. This is a total fallacy. Cloud service providers can (and, make no mistake, will) move data anywhere in the world – often in the interests of security, back-ups, support and cost efficiency. What's more, the law permits this – though it does require that some manner of legal "data export" solution first be implemented for data being transferred out of Europe. There are a number of solutions available – from model clauses to safe harbor to Binding Corporate Rules. Cloud clients need to check their service providers have one of these solutions in place and that it covers the data exports in question but, so long as they do, then there's no reason why data cannot be moved around internationally for service-related reasons.

5. **Is there adequate security?** The law requires cloud clients to ensure that their service providers have implemented "appropriate" security. The thing is, cloud clients often aren't best able to assess whether their cloud provider's security is or is not "appropriate" – one of the commonly cited reasons for outsourcing to the cloud in the first place is to take the benefit of the greater security expertise that cloud providers offer. To further complicate matters, some territories – like Germany, Poland and Spain – have precise data security rules. It's highly unlikely that a cloud provider will ever tailor its global IT infrastructure to address nationally-driven requirements of just one or two territories, so outside of heavily-regulated sectors, there's little point trying to negotiate for those. Instead, cloud clients should look to other security assurances the cloud

provider can offer – most notably, whether it maintains ISO and SSAE certification (see above!).

6. **And what about subcontracting?** Cloud suppliers subcontract: it's a fact of life. Whether to their own group affiliates or externally to third party suppliers, the likelihood is that the party concluding the cloud contracting will not be (solely) responsible for performing it. The question inevitably arises as to whether the supplier needs its client's consent to subcontract: the short answer is, generally, yes, but there's no reason why a general consent to subcontract can't be obtained upfront in the contract. At the same time, however, the cloud customer will want assurances that its data won't be outsourced to a subcontractor with lax data protection standards, so any such consent should be carefully conditioned on the cloud provider flowing down its data protection responsibilities and committing to take responsibility for managing the subcontractor's compliance.

7. **What other terms should be in a cloud contract?** In addition to the points already discussed, it's critical that cloud providers have in place a robust data breach response mechanism – so that they detect security intrusions asap and inform the cloud client promptly, giving it the opportunity to manage its own fallout from the breach and address any legal data breach notification requirements it may be under. In addition, cloud providers should be expected to inform their clients (where legally permitted to do so) about any notices or complaints they receive concerning their hosting or processing of their client's data – the client will generally be on the hook for responding to these, so it's important it receives these notices promptly giving it adequate time to respond.

So there's no reason that data protection should be holding those deals up! All of the issues described above have straightforward solutions that should be palatable to both cloud clients and providers alike. Remember: good data protection and good business are not mutually exclusive – but realistic, compatible goals.

"Further afield in the US, Phil Lee in the Palo Alto office "ranks among the finest practitioners" on data privacy and online regulation, with a particular specialism in behavioural profiling, cookies, data transfers and binding corporate rules."

Quotation from
Who's Who Legal—Information Technology

Observers say the firm *"provides an exemplary service to clients, combining urgency with an accurate eye for detail."*

Quotation from
Chambers & Partners 2013

Contacts

Phil Lee
Partner - Palo Alto

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

Mark Webber
Partner - Palo Alto

E: mark.webber@fieldfisher.com
T: +1 (650) 513 2684

Nick Holland
Partner - London

E: nick.holland@fieldfisher.com
T: +44 (0)20 7861 4977