COMPUTER LAW & SECURITY REVIEW 34 (2018) 928–932

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Legal aspects of cloud security

*Richard Kemp**

Kemp IT Law, London, UK

ARTICLE INFO

Article history:

Keywords:
Cloud computing
Information security
Cloud security
Data protection
GDPR
Cloud contracts
Cloud governance
Standards

ABSTRACT

Enterprise (large organisation) computing workloads are moving from 'on-prem' to 'in-cloud' increasingly quickly, and the cloud is forecast to account for almost half of enterprise IT by 2026, up from 10% today. But the benefits of the enterprise cloud need to be weighed against increasingly burdensome duties around cloud and data security. This comment piece provides a checklist of the sources of enterprise cloud security duties and a checklist of best practices to manage them.

After the demanding bow wave of GDPR readiness legal work in the run up to 25 May 2018, IT lawyers may be forgiven for thinking that the biggest change is now behind them. However, GDPR heralds rather than ends a period of broadly based structural change in technology adoption, business transformation and IT law and regulation. Nowhere is this better shown than in the legal aspects of the rapidly developing area of cloud security.

A central feature of this change is the epic migration now well underway in enterprise (large organisation) computing from 'on premise' – traditional IT infrastructure at the user – to 'in-cloud' – open access to the public cloud, the more dedicated resources of the private cloud and their hybrid cloud combination. The development of the enterprise cloud is as significant as the migration of electricity generation out of the factory to the UK national grid in the 1930s but with many more facets, as each component of computing – power, processing, network, memory, storage and software - gets the cloud's 'as a service' treatment.

Aggregating the elements of the private cloud and Infrastructure (IaaS), Platform (PaaS) and Software (SaaS) in the public cloud, and comparing their projected development over the next ten years with 'traditional' enterprise computing, open source IT research organisation Wikibon is forecasting that the cloud's share of enterprise computing will grow from around 10% today to 45% by 2026.[1]

For enterprise users, the cloud provides a range of benefits and opportunities, including provisioning flexibility, access to new services, assisting digital transformation, speed of deployment and cost efficiencies. However, enterprise-scale organisations operate in a business environment that increasingly emphasises the criticality of cloud and data security - the legal, technical, operational and governance controls that an organisation puts in place to ensure desired information security outcomes.

As IT workloads migrate to the cloud, the benefits of cloud provisioning need to be weighed and balanced against security risks and duties. Organisations are therefore establishing cloud security and compliance governance procedures

* Kemp IT Law, 21 Napier Avenue, London SW6 3PS, UK
E-mail address: richard.kemp@kempitlaw.com

https://doi.org/10.1016/j.clsr.2018.06.001
0267-3649/

Table 1 – Checklist of enterprise cloud security duties and liability sources.

A.	**ENTERPRISE - REGULATORY DUTIES**
1.	**Sector specific regulation**
(a)	Example 1: UK financial services firms regulated by the Financial Conduct Authority (FCA) • European Banking Authority March 2018 (EBA/REC 2017/03): Cloud Outsourcing Recommendations[2] • FCA July 2016 (FG16/5): Guidance for enterprises outsourcing to the 'cloud' and other third party IT services[3] • FCA Handbook SYSC Rule 8 (General outsourcing risk management controls)[4] and DTR (Disclosure and Transparency Rules)[5] • Directive 2009/138/EC (Solvency II) for insurers: Articles 38 and 49 (outsourcing)[6]
(b)	Example 2: UK law firms authorised by Solicitors Regulation Authority (SRA) • SRA high-level Principles[7] • SRA Code of Conduct[8] - Outcome 7.10: outsourcing requirements (applies to cloud services)
2.	**Generally applicable security/data regulation**
(a)	Data protection/privacy – GDPR (Regulation 2016/679)[9] •controller must comply with Art. 5 personal data processing principles, including 'ensuring appropriate security … using appropriate technical or organisational measures' (Art 5(1)(f)) • controller 'shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with' GDPR (Art 24(1)) • controller must 'implement appropriate technical and organisational measures designed to implement data-protection principles' (Art 25(1)) • controller 'shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures' so that processing complies with the GDPR (Art 28(1))
(b)	Security of network and information systems (duties applicable to CSPs) NIS (Directive 2016/1148)[10] • a cloud service provider (CSP) 'must identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems on which it relies to provide its service' (Reg 12(1) implementing Directive, Art 16(1))[11] • those measures must 'prevent and minimise the impact of incidents … and take into account (i) the security of systems and facilities, (ii) incident handling, (iii) business continuity management, (iv) monitoring auditing and testing and (v) compliance with international standards' (Reg. 12(2), implementing Art 16(1)) Communications Act 2003[12] (CA 2003) Privacy and E-Communications Regulations 2003[13] (PECR) • notification requirements/notifications in relation to a breach of or failure to take appropriate organisational and technical measures, etc: ◦ by a CSP as a public electronic communication network (PECN) under S.105(A) CA 2003 or in relation to a security breach under S.105B CA 2003; ◦ by a CSP as a public electronic communications service (PECS) provider under Reg 5 PECR;
(c)	Data sovereignty – Investigatory Powers Act 2016[14] • regulates powers for interception and to retain and access communications data • interception is interfering with or monitoring a communication in the course of transmission by which its 'content' (message and envelope) is made available to other than sender or recipient[15] • communications data is 'the 'who', 'when', 'where' and 'how' of a communication, but not the content, not what was said or written'[16]
(d)	Data residency/domiciliation and related requirements • EU: unauthorised international transfers of personal data are unlawful (GDPR, Art 44) • Growing number of countries (including Russia, China and Vietnam) with data domiciliation laws
(e)	UK criminal law Official Secrets Act 1989 • Crown servants and UK government contractors disclosing of or failing to secure information damaging to the UK's interests may commit offences Computer Misuse Act 1990 • hacking (as unauthorised access) and DDOS (distributed denial of service attacks) and various cyber activities can be offences UK Terrorism Acts 2000-2015 • introduces terrorism offences in relation to cyber security UK Fraud Act 2006 • phishing/identity theft (dishonestly and knowingly making a false representation intending gain or loss) can be an offence
3.	**Relevant generally applicable business regulation** • public companies' governance requirements under the Companies Act 2006 (CA 2006) • company law duty to retain accounting/general records • directors' CA 2006 duties to exercise reasonable skill, care and diligence in carrying out role • litigation procedure duties relating to document discovery

(*continued on next page*)