Simmons & Simmons

ICT Horizons by Simmons & Simmons

Summer 2019

Introduction

This document is split into two parts. The first part is intended to guide in-house counsel who cover Information, Communications & Technology (**ICT**) and Commercial law as part of their remit:

- on the material legal and regulatory developments affecting their organisations since the last edition of ICT Horizons; and
- provide related recommendations that are designed to support counsel in addressing the issues raised by the developments.

The second part is a commentary at a high level, on the spread of types of matters that we are advising on for clients now by comparison with prior periods to give an indication of what other in-house ICT counsel are needing assistance with, and to what extent.

Our contact details are provided at the end of the document should you wish to discuss the impact of any of these developments further.

Part One: Developments

Liquidated Damages Clauses – recent developments

It is a well-known concept of English law that a liquidated damages ("LDs") clause is enforceable regardless of the actual loss suffered by a party, provided the amount payable is not a penalty. This turns on whether the amount agreed was not out of all proportion to the legitimate interest of the innocent party in the enforcement of the primary obligation to which the LDs relate. Additionally, it is also generally accepted that where the amount specified in a liquidated damages clause is a genuine attempt to pre-estimate the loss caused, this will provide strong evidence that the clause is not a penalty.

In *Triple Point Technology v PTT Public Company Ltd* a contractor achieved the first stages of an IT project 149 days late. When the customer refused to make payments for further stages, the contractor suspended work and left the site. The contractor sued on its unpaid invoices and the customer counterclaimed for LDs under the contract.

The Court held that although the LDs were described in the contract as a "penalty", this did not make the clause unenforceable because the amount specified nevertheless represented a genuine pre-estimate of loss that could arise from the delay. The wording of the LDs clause focused on the period between the contractual completion date and the date of actual completion meaning that the clause could not apply where completion never occurred. As a result, LDs were only available for the stages completed late and not for stages never completed, in respect of which a separate claim in damages for breach of contract would be needed.

Recommendation: The significance of this case is that the courts will continue to enforce LDs clauses only where they represent a true attempt to pre-estimate loss. Where drafters are contemplating using a LDs clause in order to compensate for delay in delivery of services or projects, they will need to exercise caution when pre-estimating associated losses.

AI and Machine Learning – recent developments

Building on the work of a group of independent experts appointed in June 2018, the European Commission is launching a pilot phase to ensure that its current "ethical guidelines" for AI development and use can be implemented in practice. The Commission has also now invited different industry specialists, research institutes and public authorities to test the detailed assessment list drafted by the High-Level Expert Group, which further complements the guidelines.

In addition, the UK's Information Commissioner's Office ("ICO") has published an exploratory piece discussing how organisations can ensure that human involvement within automated decision-making activities can be made more "meaningful" so as to avoid the stricter requirements under Article 22 of General Data Protection Regulation ("GDPR"). Article 22 of the GDPR establishes conditions on AI systems making solely automated decisions that have legal effects (or substantially similar effects) on individuals to ensure that a human review of such decisions is available, where necessary. This adds to guidance already issued by the ICO and the European Data Protection Board which states that human review must be involved in automated decision-making where any individual objects to such decision making. Generally, market participants have been seeking further clarification on how such human reviews can be made more than purely a "token" gesture whilst not stifling the increased efficiency brought about by AI and machine learning technologies.

Recommendation: Organisations should seek to explore the elements of the guidance that demonstrate how to make a human review of an automated decision more "meaningful". Examples within the guidance include regularly involving human reviews in checking an AI system's recommendations and not "routinely" applying the results of automated decisions to individuals. Organisations should also seek to implement a process that reduces "automation bias" when integrating AI into business processes, i.e. with a view to preventing human users from routinely relying on the results generated by AI systems without ever questioning their outputs.

ICO enforcement notice against HMRC in relation to biometric data – recent developments

During January 2017, HMRC adopted a voice authentication / recognition service which asked individual callers to some of their existing helplines to record their voice as a form as password recognition. A complaint from "Big Brother Watch", a non-profit civil liberties and privacy organisation, subsequently revealed that users were not given any further information about their voices being recorded and no clear option to not register for the voice recognition services. HMRC's use of these technologies involved the recording and storing of voice biometrics in relation to 7 million users.

The ICO found that HMRC had not collected adequate consents based on the fact that customers were purely asked to repeat "my voice is my password" and were not given any clear option to not register for the voice biometrics service. In response to the complaint, the ICO has issued an enforcement notice against HMRC instructing it to delete any voice biometrics data that it holds for individuals who did not provide an adequate consent.

The case highlights the following important issues in relation to the processing of biometric data: controllers should always consider conducting a data protection impact assessment ("**DPIA**") when there is wide-scale processing of special categories of data and, when attempting to rely on consent as a legal basis for processing of biometric data, controllers should remember that such data will be defined as "special category" personal data under the GDPR and therefore any consents relied upon will need to be "*explicit*". It is also notable that the ICO's decision considered the fact that a large number of data subjects were involved and that there was a significant imbalance of power between the data subject and HMRC given that many / all were using HMRC to ensure that they were complying with their tax obligations.

Recommendation: When integrating internal or client facing processes that use biometric or genetic data (including, for example, voice biometrics recognition or facial recognition technologies), organisations will need to actively consider the ways in which they are able to collect "explicit" consent in line with the more stringent provisions surrounding such consents within the GDPR. Given the fact that biometric data is considered as "special category" data under the GDPR, it is likely that the increasingly widespread use of facial recognition and voice biometric technologies will be the subject of greater regulatory scrutiny by the ICO in the future. Organisations should carry out DPIAs and, more broadly, look to pro-actively integrate "privacy by design" compliance measures before adopting such technologies.

European Banking Authority Guidelines – upcoming developments

The European Banking Authority ("**EBA**") has recently finalized its guidelines on outsourcing contracts (the "EBA Guidelines"). Subject to each national authority incorporating the Guidelines into national regulatory frameworks, the Guidelines will take effect from 30 September 2019. Additionally, there is a backstop date for updating pre-existing contracts to comply with the Guidelines by 31 December 2021.

The Guidelines provide a detailed framework of requirements relating to outsourcing, which take into account or are consistent with current requirements for relevant financial services firms, such as the Capital Requirements Directive and MiFID II. In essence, the Guidelines set out obligations with respect to end-to-end governance over an organisation's outsourcing and the contractual arrangements it has with outsourcers.

In summary, the Guidelines introduce the following key changes: further examples of when an arrangement comprises an outsourcing, guidance on whether those outsourcings should be considered "critical and important", requirements for a comprehensive outsourcing policy and on monitoring an outsourced service provider's performance, designation of senior staff to oversee outsourcing arrangements, enhanced expectations around intra-group outsourcings and arrangements, and information flows to be put in place where one group entity exercises group wide management functions in relation to the outsourcing.

Recommendation: As a preliminary point, organisations need to assess whether the Guidelines apply to them. This is not always a straightforward question as it depends not only on an individual entity's activities but also on its group's activities. If the Guidelines apply, organisations should consider the Guidelines in relation to both their current and future outsourcing activities. This may mean updating key governance structures regarding outsourcing management functions to handle the heightened compliance obligations brought about the Guidelines. Further documentation will also need to be considered to ensure that organisations create or update existing outsourcing policies for all relevant entities. This will include ancillary documentation which supports the outsourcing policy such as vendor due diligence questionnaires, business continuity plans, and exit plans.

The GDPR – one year on

On 30 May 2019, the ICO published a paper, "GDPR: one year on", summarising its findings on the impact of the GDPR a year after its implementation on 25 May 2018. A main theme of the paper revolves around the general uptick in workload for the ICO, which has seen its workforce increase from 505 to more than 700.

The ICO received around 14,000 notifications of personal data breaches in the first year of the GDPR (a notable increase from around 3,000 during the year preceding GDPR). Around 82% of cases were closed without any action being taken. Of the remaining cases, only around 17.5% required remediation action from the organisation, while less than 0.5% resulted in a monetary penalty or improvement plan. The number of data protection complaints from the general public has also increased dramatically, almost doubling to around 41,000. Data subject access requests are the most common complaint, accounting for around 38% of the complaints received. The ICO has also been making use of its new enforcement powers. Previously, companies had to agree to a data protection audit under the DPA 1998, but under the GDPR the ICO can issue assessment notices that allow it to carry out inspections. The ICO states that it has issued 15 such notices under the GDPR since it came into force in May 2018.

The ICO has also outlined its regulatory priorities going forward, which include: cyber security; AI, big data and machine learning; web and cross-device tracking for marketing purposes; children's privacy; the use of surveillance and facial recognition technology; data broking; the use of personal information in political campaigns; and freedom of information compliance. It is likely that we will see further guidance and codes of practice in these areas, typified by the ICO's recent consultation on a draft code of practice on "Age Appropriate Design" which is intended to provide further guidance on protecting children against online harms.

Recommendation: The ICO's statistics on personal data breach notifications and data subject access requests bear out our own experience that these aspects of compliance are among the most prevalent and challenging for our clients. As a result, we recommend that organisations focus on ensuring that their compliance policies and procedures in these areas are as robust and readily implementable as they can be, alongside considering whether any of the ICO's other regulatory priorities may have an impact on them.

Part Two: Comment on spread of types of matters

We have the following comment on the spread of types of matters (and on informal conversations with our clients during the period covered):

- over the past 12-18 months we have seen a marked increase in transactions involving large financial institutions relating both to a shift to digital banking and an expansion upon traditional financial services product and service offerings. We see this trend continuing with a number of projects of this nature in the pipeline;
- a year on from the date on which the GDPR entered into effect, clients are reflecting on the effectiveness of their compliance measures, with many taking the opportunity to enhance them; and
- investment decisions that were postponed earlier in the year due to the uncertainty of the UK's position on Brexit are now being revisited, with a series of new outsourcing transactions starting in recent months.

Other ICT Commercial knowhow publications

ICT: http://www.elexica.com/en/Legal-Topics/Information-Communication-and-Technology

Data Protection & Privacy: http://www.elexica.com/en/Legal-Topics/Data-Protection-and-Privacy

Brexit: http://www.elexica.com/en/Legal-Topics/Brexit

EU Data Protection Regulation Microsite: http://www.elexica.com/en/Resources/Microsite/European-Data-Protection-Regulation

Contacts

Alexander Brown
T +44 20 7825 4954
E alexander.brown@simmons-simmons.com

Lawrence Brown
T +44 20 7825 3053
E lawrence.brown@simmons-simmons.com

Tom Wheadon
T +44 20 7825 3603
E tom.wheadon@simmons-simmons.com

James Cotter
T +44 20 7825 3194
E james.cotter@simmons-simmons.com

Hinal Patel
T +44 20 7825 2080
E hinal.patel@simmons-simmons.com

George Morris
T + 44 20 7825 4046
E george.morris@simmons-simmons.com