Linklaters

November 2012

Technology Media and Telecommunications.

Data Protection

EU – Update on the proposed General Data Protection Regulation

In January 2012, the European Commission proposed a major reform of the European data protection law. It released a policy communication, a draft General Data Protection Regulation and a draft Directive on protecting personal data in criminal and justice matters. As the year draws to a close, we review the progress of the draft Regulation and consider if it is still likely to be adopted in late 2013 or in the first half of 2014 before the election of the European Parliament.

Progress so far

The draft Regulation is progressing under the co-decision procedure, being the ordinary process for such legislation. It has already attracted substantial comment and numerous opinions.

Jan Philipp Albrecht, who is the European Parliament rapporteur of the Committee for Civil Liberties, Justice and Home Affairs ("LIBE"), issued a timetable during the summer setting out the main steps remaining to complete the adoption of the Regulation. The key dates in that timetable are set out in the table below together with a number of important opinions issued to date.

The timetable anticipates that, by summer 2013, the Regulation should be ready for the trilogue involving the Parliament, the Council and the Commission, and that the Regulation should be put to a final vote in the plenary session of the European Parliament in late 2013 or early 2014. Assuming the two year implementation period in the draft Regulation is retained, this would result in its coming into force in late 2015 or early 2016.

However, there are already concerns about whether this timetable will be met, particularly given the time taken by the European Council to review the draft Regulation. A further complication is that, if the draft Regulation is not passed in early 2014, it might have to wait until after the European Parliament elections in June 2014. This could push the adoption of the Regulation back

Contents

to 2016 which, assuming the two year implementation period is retained, might mean it only comes into force around 2018.

Timeline	
January 2012	Publication of the draft Regulation
March 2012	First Article 29 Working Party Opinion
March 2012	Opinion of the European Data Protection Supervisor
May 2012	Opinion of the European Economic and Social Committee
October 2012	Second Article 29 Working Party Opinion
October 2012	Opinion of the Committee of the Regions
November 2012[1]	Presentation of the draft report
December 2012	Deadline for tabling amendments to LBIE report
Late January/February 2013	Discussion of amendments in LIBE Committee
February 2013	Discussion with Opinion Committees
March/April 2013	Orientation vote LIBE Committee
Summer 2013 (?)	Trilogue with Parliament, Council and Commission
Late 2013 - Early 2014 (?)	Vote in plenary

Potential areas of change

The draft Regulation was introduced, in part, to achieve higher levels of harmonisation across the European Union and to make data controllers more responsible for their processing through the introduction of the principle of "accountability".

Whilst there is general consensus on some aspects of the draft Regulation, such as retaining the current data protection principles, a number of other aspects of the Regulation have been more controversial. For example:

> *Regulation*: The choice of a Regulation over a Directive has caused some concern. A Regulation is directly effective in all Member States whereas a Directive must be implemented into each Member States national law, thus allowing those States some flexibility in its implementation. However, the European Commission has been

[1] According to various sources, this likely to be delayed until December 2012.

pushing hard for a Regulation because it provides greater harmonisation.

> *Delegated Powers*: The draft Regulation gives the European Commission delegated powers over many aspects of the Regulation. Whilst these delegated powers do provide a flexible means to ensure harmonisation of the Regulation, their presence also means that the Regulation, when passed, would still be largely incomplete; this would leave many data controllers in a difficult position, not knowing what to do to comply with these new rules but subject to heavy sanctions if they do not. There have been proposals that these delegated powers should either be set out in the Regulation itself, subject to soft law guidance by the new European Data Protection Board, or simply omitted because they are not required. Vice President Viviane Reding has recently expressed her willingness to review the delegated acts and to limit them only to those which are really necessary.

> *Accountability*: The new proposals also mark a shift from a notification regime to the use of "accountability". Under the accountability principle, data controllers will have to take the necessary measures to ensure compliance and maintain documentation demonstrating that these measures continue to be effective. One major concern is that, whilst this is intended to simplify the current regime through the removal of the notification requirement, it could in fact result in an even higher burden than under the current framework and create more uncertainty.

> *Data Breach*: The draft Regulation reinforces the security obligations placed on data controllers which should generate more trust from consumers, particularly when transacting over the internet. However, this obligation also includes a heavily criticised obligation to notify data breaches to regulators as it is not subject to a de minimis threshold, i.e. it applies regardless of the size of the breach (no threshold) and existence of any risk of harm for data subjects.

Next steps

It is interesting to note that Ireland holds the presidency of the European Council during the first half of 2013, when many crucial negotiations will take place.

Ireland is, of course, a popular European base for technology companies like Intel, Facebook and, more recently, Twitter, so should be in an ideal position to wrestle with the problems of creating a data protection law fit for the digital age. Whether it can progress those negotiations fast enough to allow the draft Regulation is to be passed in late 2013 or before the European Parliament elections of 2014 remains to be seen.

By Tanguy Van Overstraeten and Alana Van Caenegem, Brussels

EU – *UsedSoft v Oracle*: ECJ approves sale of 'used' software

On 3 July 2012, the ECJ handed down its landmark decision in *UsedSoft GmbH v Oracle International Corp* (C-128/11), ruling that the owner of copyright in software cannot prevent a perpetual licensee who has downloaded the software from the internet from selling his 'used' licence. This decision has significant implications for the software and other digital industries.

Background

Oracle develops and markets computer software, most of which is downloaded by its customers from the internet. Each customer's right to use the software is governed by a licence agreement which provides that, in return for payment of a one-off fee, the customer receives a non-exclusive, non-transferable right to use the software for an unlimited period. Pursuant to a separate maintenance agreement, customers can also download updates and patches (programs for correcting faults) from Oracle's website.

UsedSoft deals in second-hand software. It began to offer for sale 'used' Oracle licences, stating that these were 'current' in the sense that the maintenance agreement between the original licence holder and Oracle was still in force.

Oracle obtained an injunction from the Munich Regional Court restraining UsedSoft from carrying out these activities. UsedSoft appealed to the German Federal Court which referred a number of questions on the interpretation of Directive 2009/24/EC on the legal protection of computer programs (codifying Directive 91/250/EEC) (the "**Software Directive**") to the ECJ. The relevant provisions of the Software Directive are summarised below:

> Article 4(1): the computer program rights holder has the exclusive right to do or authorise: (a) the reproduction of the program; (b) the translation or other alteration of the program; and (c) any form of distribution to the public of the program.

> Article 4(2): the first sale of a copy of a program by the rights holder or with their consent in the EU exhausts the distribution right of that copy within the EU (such that the rights holder loses its right to rely on its copyrights to oppose the resale of that copy).

> Article 5(1): unless the contract specifies otherwise, the acts of reproduction and translation (under Article 4(1)(a) and (b)) do not require authorisation by the rights holder where they are necessary for the use of the computer program by a lawful acquirer.

The German Federal Court asked the ECJ whether:

> the right to distribute a copy of a computer program was exhausted under Article 4(2) where the acquirer had made a copy with the rights holder's consent by downloading the program from the internet; and

> an acquirer of the user licence was a "lawful acquirer" within the meaning of Article 5(1) such that it could rely on the exhaustion rule under Article 4(2) to run the program on its own systems.

ECJ's decision on exhaustion: what is a 'sale of a copy'?

The ECJ ruled that in order for a copyright holder's distribution right to be exhausted under Article 4(2) in respect of a copy of software (such that the copyright holder can no longer oppose the resale of that copy), the transaction between it and its customer must amount to a 'sale of a copy' of the program. Where a customer downloads a copy of Oracle's software and enters into a licence agreement under which it receives the right to use that copy for an unlimited period in return for payment of a fee, such a transaction amounts to a 'sale' for the purposes of Article 4(2) and involves a transfer of the right of ownership in that copy.

This broad interpretation of Article 4(2) is necessary as otherwise the effectiveness of the rule of exhaustion would be undermined since suppliers would merely have to call the contract a "licence" rather than a "sale" in order to circumvent it.

The ECJ said that the term 'sale of a copy' in Article 4(2) encompasses all situations in which there is a grant of a right to use a copy of a computer program for an unlimited period in return for payment of a fee, and any such 'sale' would trigger the exhaustion provisions of the Software Directive. Therefore, even if the licence agreement prohibits further transfer, the copyright holder can no longer oppose the resale of that copy.

It is immaterial whether the computer program is made available in some physical form (e.g. a CD or DVD) or by way of internet download; in either case the transaction is a 'sale' of the relevant copy of the software.

Moreover, the exhaustion of the distribution right extends to any corrections or updates made by the copyright holder under a maintenance agreement. Even if the maintenance agreement is for a limited period, the functionalities corrected, altered or added on the basis of such an agreement form an integral part of the copy originally sold and which can be used by the customer for an unlimited period.

Restrictions on the reseller

In order for a resale not to infringe, the original licensee must render his own copy unusable at the time of its resale. The ECJ said that it would be permissible for the copyright holder to make use of technical protective measures (e.g. product keys) to ensure that this is the case. This preserves the right of reproduction of the program which is not exhausted by the first sale.

If the licence acquired by the first acquirer is in a "block" and relates to a greater number of users than he needs, that acquirer is not authorised by the effect of the exhaustion of the distribution right to divide the licence and resell only part of it.

Is a second acquirer a 'lawful acquirer'?

Since the copyright holder cannot object to the resale of a copy of software for which that rights holder's distribution right was exhausted, a second acquirer of that copy (and any subsequent acquirers) were "lawful acquirers" for the purposes of Article 5(1) who could download that copy from the copyright holder's website and copy it as required to use it on their own systems.

How should the software industry respond?

This is a landmark decision which effectively creates a secondary market for licensed software, regardless of the terms of the licence agreement. However, the judgment contains a number of important qualifications which should be borne in mind by software providers and resellers alike:

> *Limited term licences* - The ECJ placed a lot of emphasis on the fact that the Oracle licences were not limited in time, and for this reason concluded that a 'sale' of the copy of the program had occurred. This leaves it open for software providers to argue that they have not exhausted their distribution rights in software which is licensed for a limited time *via* a rental model. However, any such time limits are likely to have to be real and enforced, not merely nominal or formal, as courts (at both national and European level) are unlikely to allow the doctrine of exhaustion to be circumvented by mere formalities. For the same reason, very long licences (e.g. 99 years) are unlikely to persuade the courts that the arrangement is not in substance a 'sale' for the purposes of the Software Directive.

> *Contracts for services* - The ECJ was clear that the doctrine of exhaustion does not apply to maintenance agreements and contracts for services. We may therefore see more reliance on software being provided through online services such as 'the cloud' where the arrangement is less likely to be tantamount to a 'sale of a copy' of software.

> *Multi-user licences* - The principle of exhaustion does not allow licensees to divide and sell parts of multi-user licences. This may discourage software providers from 'selling' their software under block licences for small numbers of (or even individual) users, which would presumably be more readily tradable on the secondary market than single enterprise licences.

> *Technical protective measures* - Any acquirer who resells its licence must make his own copy unusable prior to the resale. The ECJ said expressly that copyright holders may make use of technical protective measures (e.g. product keys) to ensure that this is the case. Software providers may therefore wish to investigate the technical solutions available to them to monitor and police usage in this regard to avoid a free-for-all in respect of their software. It is not clear to what extent software providers can put measures in place to use technology to prevent the transfer of software - although given the free movement of

goods principles behind the ruling, it appears unlikely that the courts would be sympathetic to such practices.

The judgment also leaves a number of questions unanswered, perhaps most significantly: what usage terms apply to a second acquirer of software? The ECJ observed that, in considering whether a 'sale' had occurred, the downloading of a copy of a computer program and the conclusion of a user licence agreement form an "*indivisible whole*". Further, the rights acquired under Article 5(1) are those necessary for use of the computer program by the lawful acquirer "*in accordance with its intended purpose*" - which could only be ascertained by reference to the original licence terms. So it seems likely that the usage right transferred to the second and any subsequent acquirers will be limited by the scope of the permissions set out in the original user licence. However, there is nothing in the judgment that suggests that any other contractual obligations should apply as between the software provider and any new acquirer. Moreover, the ECJ was clear that any separate agreements such as maintenance and support agreements will not be transferred as these are not subject to the doctrine of exhaustion. As such, it is unlikely any new acquirer could demand any future patches, upgrades or support from the software provider without entering into a new agreement with the software provider directly.

By Kathy Berry, London

EU – *SAS v WPL:* When can you copy software without infringing copyright?

The ECJ has given its ruling in *SAS Institute Inc. v World Programming Ltd* (C-406/10), confirming that the functionality of software is not protected by copyright. The ECJ also clarified the extent to which the terms of a licence agreement can prevent a licensee from studying licensed software in order to develop competing programs.

Background

SAS Institute developed a set of integrated computer programs enabling users to carry out various data processing tasks. The SAS system enables users to write their own applications, in a programming language proprietary to SAS, in order to adapt the SAS system to work with their own data.

WPL perceived a market demand for alternative software capable of executing applications written by users in the SAS programming language. It produced a rival system which emulated the functionality of the SAS system so that, as far as possible, the same inputs produced the same outputs. Users were able to run the applications they had developed for the SAS system on the WPL system.

In order to create the WPL system, WPL obtained and studied a version of the SAS system known as the "learning edition", supplied under licence from SAS. However, it was common ground that WPL did not have access to SAS's source code.

SAS alleged that:

> WPL had copied the manuals for the SAS system when creating the WPL system, thereby infringing its copyright in the manuals;

> by copying the manuals, WPL had indirectly copied SAS's software and had infringed its copyright in the software;

> WPL had used the learning edition of the SAS system in contravention of its licences, thereby acting in breach of contract and infringing copyright in the learning edition; and

> WPL had infringed copyright in the SAS manuals by creating its own manual.

SAS sought to challenge the existing view of the English courts that it is not an infringement of copyright in the source code of a computer program for a competitor to study how the computer program functions and then write its own program to emulate that functionality.

Arnold J in the English High Court referred a number of questions on the interpretation of the Software Directive and the Information Society Directive to the ECJ. In Arnold J's view, it was not *acte clair* whether the functionalities of a computer program were to be regarded as the expression of the computer program (thus qualifying for copyright protection pursuant to the Software Directive), or whether they are merely ideas and principles

underlying the computer program (in which case they would be outside the scope of protection).

The ECJ's decision - Copyright protection for functionality

The ECJ confirmed that Article 1(2) of the Software Directive must be interpreted as meaning that neither the functionality of a computer program, the programming language, nor the format of the data files used in it, constitute a form of expression of that program and, as such, are not protected by copyright under the Software Directive.

The ECJ agreed with Advocate General Bot that allowing that the functionality of a computer program to be protected by copyright would amount to making it possible to monopolise ideas, to the detriment of technological process and industrial development.

However, muddying the waters somewhat, the ECJ indicated that whilst the SAS Language and the format of SAS's data files were not eligible for protection under the Software Directive, they might be eligible for protection as copyright works under the Information Society Directive if they amounted to their author's own intellectual creation. So, whilst it is clear that emulating the functionality of software is legitimate, this should be read with the caveat that reproducing a copyright work consisting of a programming language or data file format could still infringe.

Observing, studying and testing licensed software

The ECJ also clarified that, under Article 5(3) of the Software Directive, a person who has obtained a copy of a computer program under a licence is entitled, without the authorisation of the owner of the copyright, to observe, study or test the functioning of that program so as to determine the ideas and principles which underlie any element of it, provided that those acts did not infringe the copyright in the program.

Authorisation for such acts, to the extent that these included loading and running the program, was not required were they were necessary for the use of the program by the lawful acquirer in accordance with its intended purpose, including for error correction. The ECJ expressly confirmed that licensing arrangements cannot be used to try to protect the ideas and principles underlying any element of the program: any contractual terms seeking to prevent the studying, observing and testing of licensed software are unenforceable.

Protection for user manuals

As regards the use of user manuals, the ECJ ruled that computer manuals will be protected by copyright to the extent that they are the expression of the intellectual creation of the author. Their reproduction in other computer programs or manuals could amount to copyright infringement if the reproduction constitutes the expression of the intellectual creation of the author. This would be a matter for national courts to decide.

The ECJ did not consider that keywords, syntax and commands in isolation would be sufficient intellectual creations to attract copyright, but the choice, sequence and combination of those words, figures or mathematical concepts could be protectable as copyright works. It was for the national courts to decide whether the reproduction of those elements in WPL's manual of software constituted the reproduction of the expression of the intellectual creation of the author.

Comment

The ECJ's decision that the functionality of a computer program cannot be protected by copyright is unsurprising as it endorses the approach previously adopted by the English courts (for example *Navitaire Inc v EasyJet Airline Co Ltd* [2004] EWHC 1725 and *Nova Productions Ltd v Mazooma Games Ltd* [2007] EWCA Civ 219) and by the Advocate General.

There is now little doubt that non-textual copying of software that merely emulates the functionality of a computer program in another computer program, with no reference to the underlying source code, will not amount to copyright infringement.

Somewhat unhelpfully however, the ECJ also acknowledged the possibility that whilst programming languages and/or data files were not protected under the Software Directive, they could be capable of copyright protection under the Information Society Directive. Whilst the scope of this qualification is not yet clear, it remains possible that reproducing a copyright work consisting of a program language or data file format may also amount to copyright infringement.

Finally, this decision also confirms that copyright owners can not contractually restrict their licensees from observing, studying and testing their computer program, provided that any reproduction of the program by the licensee does not go beyond that resulting from the normal loading and running of the program and does not infringe the exclusive rights of the owner in that program.

By Kathy Berry, London

EU – *Football Dataco v Sportradar:* ECJ rules on database right and location of infringement

The ECJ has given its ruling in *Football Dataco v Sportradar* (C-173/11), finding that where a website operator targets members of the public in one Member State, and provides them with material infringing *sui generis* database rights from a server located in another, the act of infringement occurs "at least" in the Member State where the recipients are located. The ECJ did not decide whether infringement also occurs at the source of the service.

Background

The Database Directive (96/9/EC), implemented in the UK by the Copyright and Rights in Databases Regulations 1997, obliges Member States to provide for two separate forms of protection for databases: copyright and a *sui generis* database right. The *sui generis* database right gives the maker of a qualifying database the right to prevent the unauthorised "extraction and/or re-utilisation" of the whole or a substantial part of its contents.

Football Dataco maintains and exploits a database of information relating to professional football matches in England and Scotland. Sportradar GmbH offers a rival service *via* its website betradar.com, using servers located in Germany and Austria. Sportradar's customers include betting service providers targeting the UK market (e.g. Stan James and bet365).

In April 2010, Football Dataco brought proceedings against Sportradar in the English High Court, claiming that Sportradar had copied its database and alleging, *inter alia,* infringement by Sportradar of its *sui generis* database right.

Sportradar challenged the English High Court's jurisdiction to hear the case. The High Court held that it did have jurisdiction to hear the action in so far as it concerned the joint liability of Sportradar and its UK customers, but that it did not have jurisdiction in relation to Sportradar's primary liability. The Court's reasoning was that it would only have jurisdiction where the harmful event had occurred within its jurisdiction, and here, the harmful event (i.e. the primary infringing act of "re-utilisation" of the database) took place only where the server was based (i.e. outside the UK), and not where the transmission was received (by end users in the UK).

Both parties appealed to the Court of Appeal, which referred questions to the ECJ relating to the concepts of extraction and re-utilisation and the location of infringement.

The ECJ's decision

Re-utilisation - The ECJ held that the concept of "re-utilisation" must be understood broadly, extending to any unauthorised act of distribution to the public. The nature and form of the processes used are irrelevant. Re-utilisation therefore includes sending, by means of a server, to another computer, at that person's request, data previously extracted from a database protected by the *sui generis* right.

Location of infringement **-** The ECJ said that re-utilisation by means of a server is characterised by a series of successive operations, ranging from placing data online to the transmission of that data to the public, which may take place in a different Member State.

The ECJ noted the ubiquitous nature of websites and held that the mere fact that a website containing the relevant infringing data is accessible in a particular territory is not sufficient to conclude that the website operator is performing an act of re-utilisation in that territory. It could not be correct that website operators should be subject to the laws of each state in which their website is technically accessible, even if the website is obviously targeted at persons outside that state. Instead, the localisation of an act of re-utilisation depends on evidence of an intention to target end users in a particular territory.

In this case, the fact that Sportradar agreed to provide access to its server to companies offering betting services in the UK was a relevant factor, provided that Sportradar was aware of the ultimate destination of the data. It could also be relevant if the contract price took account of the actual and projected amount of business that those companies did in the UK. Finally, the language in which the data was made available could be relevant supporting evidence. Where such evidence is present, the national court is entitled to consider that an act of re-utilisation occurs in the Member State in which the recipient of the data is located.

The ECJ dismissed Sportradar's argument that re-utilisation takes place only in the Member State in which the server is located. Such an interpretation would mean that a defendant could escape the national laws of a Member State, even one at which its website is specifically targeted, merely by locating its server elsewhere. This would make it too easy to circumvent the *sui generis* right.

In the light of these considerations, the ECJ held that where a website operator intends to target members of the public in one EU Member State, and provides them with material infringing *sui generis* database rights from a server located in another, the act of infringement occurs "at least" in the Member State where the recipients are located. The ECJ did not decide whether infringement also occurs at the source of the service.

Comment

This decision is generally good news for rights holders, ensuring that digital infringers who target end users in a Member State cannot escape infringement proceedings in that Member State merely by locating their servers outside it. (The English High Court in this case had found that re-utilisation happens only in the country of emission, i.e. the country in which the server is located.)

However, the ECJ left some important questions open, primarily whether infringement *also* occurs in the country of emission. This may be implied from the ECJ's comment that infringement occurs "at least" in the country of transmission, but the ECJ declined to specifically address the point.

The introduction of the requirement for evidence of intent is consistent with ECJ case law relating to trade marks (e.g. *1-800 Flowers* and *Euromarket Designs*), but may not always be easy to prove. The nature of the evidence required may depend on the facts of each particular case, but is likely to include the language of the website and the data; currency; payment methods; domain names and keyword advertising. Other relevant factors may include the presence or absence of website disclaimers and/or technical measures to block access to end users in certain jurisdictions.

Whilst this decision concerns only the *sui generis* database right, it is also likely to be relevant to copyright, in particular in the context of an infringing communication to the public of copyrighted content. As such, the decision could be relevant to all who make content available *via* the internet.

By Kathy Berry, London

Hong Kong – Privacy Ordinance amended to deal with direct marketing, data processing, due diligence and enforcement

Hong Kong's main data protection law (the Personal Data (Privacy) Ordinance) has been amended to introduce important new requirements for companies who collect personal information in Hong Kong. The changes:

> impose new restrictions on the use and disclosure of personal information for direct marketing purposes;

> clarify the obligations on entities who use outsourced data processors;

> clarify how personal information may be disclosed and used during due diligence in M&A transactions; and

> strengthen the powers of the Privacy Commissioner to investigate data breaches, take enforcement action and impose penalties.

The new requirements introduced to the Ordinance are discussed in further detail below.

Use of personal data for direct marketing

A company may not use personal information of an individual for direct marketing purposes unless that individual has given his or her informed consent. This approach is a significant change from the 'opt-out' position under the previous law. However, there are exemptions for:

> companies in respect of data collected prior to commencement of these new provisions; and

> direct marketing companies who use personal information at the direction of a third party who has notified them that all required consents have been obtained.

When using an individual's personal information for direct marketing for the first time, a company must expressly tell the individual that he or she may revoke their consent at any time. The company must cease using the individual's personal data for direct marketing on request by that individual. These requirements reflect the existing 'opt-out' regime in the Ordinance.

A breach of any of these new requirements will constitute an offence attracting fines of up to HK$500,000 and up to three years' imprisonment, which is significantly harsher than previous penalties under the Ordinance.

Disclosure/sale of personal data to third parties for direct marketing

A company may not provide a third party (for consideration or otherwise) with personal information of an individual for the purposes of direct marketing unless that individual has given his or her informed consent, which may be revoked at any time.

Breach of these provisions can result in fines of up to HK$1,000,000 and up to five years' imprisonment, if the disclosure of data was for consideration, or

up to HK$500,000 and up to three years' imprisonment, in other cases. Again, this is a significant increase to the previous penalty provisions in the Ordinance.

Obligations relating to data processors

The new Ordinance does not place new obligations on data processors, however it does require companies that outsource data processing to adopt means (contractual or otherwise) to:

> prevent the data processor from keeping personal data for longer than is necessary; and

> prevent unauthorised or accidental access, processing, erasure, loss or use of personal data.

Due diligence

The new Ordinance clarifies that personal data may be disclosed to another entity for the purpose of due diligence on a company or assets, provided that:

> the disclosure is no more than necessary for the purpose of the due diligence;

> on completion of the proposed transaction to which the due diligence relates, the acquirer will continue to carry on the same or a similar business to the business for which the target company had collected and used the data; and

> it is not practicable to obtain consent from the individual for the disclosure.

Any entity who receives personal data through due diligence may only use that data for the due diligence. It must return the personal data at the end of the due diligence and delete any copies that it may have retained.

Other changes

The new Ordinance also includes provisions that increase the Privacy Commissioner's investigative and enforcement powers and sets out a new scheme for individuals to seek legal assistance to pursue claims of data breach.

In addition to the penalties for breach of the new direct marketing provisions, the new rules impose penalties of up to HK$1,000,000 and five years' imprisonment if a person:

> for profit or to cause loss to an individual, discloses to a third party personal information about that individual that was obtained from a data user without consent (whether or not for the purpose of direct marketing); or

> discloses to a third party personal information about an individual that was obtained from a data user without consent where that disclosure causes psychological harm to the individual.

The amended Ordinance also imposes heightened penalties of up to HK$50,000 and two years' imprisonment for a first conviction, and up to HK$100,000 and two years' imprisonment, for subsequent convictions, if a data user contravenes a notice of the Privacy Commissioner directing it to remedy a breach of the Ordinance.

Next steps

All companies which collect data from individuals in Hong Kong should ensure that their methods of data collection, use and disclosure are in line with the new Ordinance. In particular, companies wishing to use personal information to market their products or third party products to individuals must satisfy themselves that they have the required consents to undertake these activities. If not, criminal penalties may apply.

The amendments to the Ordinance will come into effect in phases. The majority of provisions came into effect on 1 October 2012. However, the new provisions about direct marketing will come into effect at a later date (expected to be early to mid 2013) to give businesses the opportunity to prepare for the impact of the changes.

By Adrian Fisher, Shanghai

Hong Kong – New outsourcing guidelines for insurers

From 1 January 2013 authorised insurers in Hong Kong must comply with new guidelines issued by the Hong Kong Insurance Authority (the "**HKIA**") and obtain the approval of the HKIA if they wish to outsource certain of their functions to third party service providers.

Application of the guidelines

The guidelines apply to all arrangements under which a service provider (whether located in or outside of Hong Kong and whether or not an independent party or a related party of the insurer) undertakes to perform a service which the insurer would otherwise carry out itself. The guidelines set out some examples of what may be considered outsourcing for the purposes of the guidelines, including application and claims processing, policy administration, human resources management, marketing and research, IT systems management and risk management services.

The guidelines clarify that certain services are not outsourcing for the purposes of the guidelines, particularly sales of policies by insurance agents or brokers and medical examinations for assessing insurance claims. Common business services like banking, printing, mail and telecommunications services are also excluded.

An insurer should follow the guidelines to the extent necessary considering the materiality of the outsourcing. If an outsourcing is material to the insurer's business, all issues outlined in the guidelines must be addressed.

Key requirements of the guidelines

The guidelines set out requirements covering the following 10 areas:

> **Outsourcing policy**: Insurers must have in place a board-approved policy on outsourcing. The policy should establish the insurer's framework for assessing the materiality of a proposed outsourcing and the risks involved in that outsourcing, as well as the monitoring and control requirements in respect of an outsourcing. Staff of the insurer who are involved in any outsourcing arrangement must be made aware of and have training about the insurer's outsourcing policy.

> **Materiality assessment**: In line with its outsourcing policy, an insurer must have in place a framework to assess the materiality of a proposed outsourcing arrangement. The guidelines make clear that the assessment of the materiality of an outsourcing arrangement is qualitative and depends on the particular facts of the outsourcing. An insurer must continually monitor the materiality of its outsourcing arrangements.

> **Risk assessment**: Prior to entering into, renewing or renegotiating an outsourcing arrangement, an insurer must conduct a comprehensive risk assessment, including by assessing the financial, operational, legal and reputational risks involved in the outsourcing.

> **Service provider**: An insurer must conduct sufficient due diligence on the provider of a proposed outsourced service.

> **Outsourcing agreement**: The guidelines set out a number of provisions that an insurer should consider when negotiating an outsourcing services agreement, including about: (a) description of services; (b) service standards; (c) monitoring and reporting obligations; (d) restrictions on subcontracting; (e) business continuity and disaster recovery; (f) termination rights; and (g) audit rights. The guidelines state that all outsourcing agreements should preferably be governed by Hong Kong law.

> **Information confidentiality**: An insurer must ensure that its outsourcing arrangements comply with Hong Kong's data protection laws (ie the Personal Data (Privacy) Ordinance). An insurer must also ensure that it and its service provider have in place appropriate data security and confidentiality safeguards. Any breach of confidentiality or unauthorised access to data that affects the insurer or its customers must be notified to the HKIA.

> **Monitoring and control**: An insurer must have resources and processes in place to monitor and control its outsourcing arrangements. The guidelines are not exhaustive in explaining how this can be achieved, but do require an insurer, for example, to conduct regular reviews or audits of its outsourcing arrangements and to have in place escalation processes to expedite resolution of any issues in the outsourcing arrangements. Significant problems that may materially affect the insurer must be notified to the HKIA.

> **Contingency planning**: An insurer must have, and ensure that its outsourced service providers have, adequate business continuity and disaster recovery procedures in place. These procedures must be regularly reviewed and tested.

> **Overseas outsourcing**: If an insurer intends to outsource any of its functions to an overseas service provider, it must consider issues such as any country risks posed by the jurisdiction from where the services will be provided, confidentiality or data protection implications of transferring information to that jurisdiction and the extent to which the HKIA is able to continue to access information of the insurer to fulfil its statutory responsibilities.

> **Sub-contracting**: The guidelines do not prohibit an outsourced service provider from sub-contracting outsourced services, but responsibility is placed on the insurer to maintain control over any sub-contracting arrangements. If the service provider wishes to sub-contract, the insurer must ensure that the service provider complies with the guidelines as if it were the insurer and the sub-contractor were the outsourced service provider.

Notification and approval requirements

An insurer must notify the HKIA at least three months prior to entering into or significantly varying a material outsourcing arrangement to which the guidelines apply. The insurer must provide a copy of any outsourcing agreement with this notification.

Although the guidelines refer to this as a 'notification' requirement, it is effectively a requirement to obtain the HKIA's approval to a new or varied material outsourcing, as the HKIA may raise objections and require an insurer to remedy areas of concern about the outsourcing. The HKIA may also extend the three month 'notification period' if more time is needed to address these areas of concern to the HKIA's satisfaction. The notification regime does not apply to an outsourcing that is not material.

If the HKIA does not respond to the insurer within three months of it notifying the HKIA of the new or varied outsourcing arrangement, the HKIA is deemed to have approved the arrangement.

Transition period

The guidelines introduce a transition period for those outsourcing arrangements (whether or not material) entered into prior to 1 January 2013 and that will not expire before April 2013. Under these transitional arrangements, the insurer must: (a) provide the HKIA with information about the outsourcing arrangement before 1 February 2013; (b) conduct materiality and risk assessments on the outsourcing arrangement before 1 April 2013; and (c) remedy any deficiencies in the outsourcing arrangement before 1 January 2014.

By Adrian Fisher, Shanghai

UK – Supreme Court orders website to disclose users' data

Viagogo, the online ticket exchange site, has been ordered to hand over the identities of individuals who have used the site to re-sell international rugby tickets at more than face value and in breach of the conditions attaching to those tickets. The Supreme Court decided disclosure of that personal data to the RFU was proportionate. In making that assessment, it was not necessary to take a narrow approach focusing on the benefit derived from obtaining information about each individual user in insolation. Instead, the Supreme Court was able to consider wider policy factors such as the RFU's desire to maintain ticket prices at affordable levels and deter others from selling them at inflated prices.

An order for disclosure of ticket sellers

The RFU (Rugby Football Union) is the governing body for rugby union in England and the owner of Twickenham stadium. The RFU alone is responsible for issuing tickets for rugby matches at Twickenham. There is huge demand for these tickets so the RFU imposes conditions on their use to prevent ticket prices inflating and to ensure tickets are allocated in a manner which develops the sport of rugby and enhances its popularity. In particular, the ticket remains the property of the RFU at all times and any resale of the ticket above its face value is a breach of contract rendering the ticket null and void.

Viagogo (who have recently changed their name to Consolidated Information Services) operated a website allowing people to re-sell tickets anonymously to various sporting and other events, including rugby matches at Twickenham. Viagogo received a percentage of the price paid for those tickets.

The RFU conducted a number of test purchases on the Viagogo website, which revealed that the tickets were frequently sold above their face value, sometimes significantly so. The RFU sought disclosure of the identity of the sellers from Viagogo under Norwich Pharmacal principles. Both the High Court and Court of Appeal ordered the disclosure of the sellers' identities, finding that there was a good case that the sale of tickets amounts to and led to arguable wrongs (breach of contract and trespass) and there was no readily available alternative means to discover the sellers' identities. Moreover, any interference with the personal data of the sellers was justified and proportionate given the RFU's legitimate objective in obtaining redress for arguable wrongs.

Litigation and data protection

Viagogo appealed to the Supreme Court, claiming that the order breached data protection laws and Article 8 of the European Charter of Fundamental Rights.

Article 8 of the Charter of Fundamental Rights provides that everyone has the right to the protection of their personal data. The Charter itself is directly effective in Member States when implementing EU law. The rubric

"implementing EU law" is interpreted broadly and included the order against Viagogo to disclose the details of the sellers, as it relates to the processing of personal data for the purposes of the Data Protection Directive - a matter within the material scope of EU law.

That being said, the protection provided under Article 8, and under the Data Protection Directive, is not absolute. For example, the rights under the Charter can be limited where it is necessary to do so in order to protect the rights and freedoms of others.

These limitations are reflected in Article 13 of the Data Protection Directive which allows Member States to adopt legislative measures to protect the rights and freedoms of others. This includes legislation allowing the disclosure of personal data in civil proceedings where it is necessary to enable a person with a viable course of action to pursue that action in the courts (as confirmed by the European Court of Justice in Promusicae C-275/06). Indeed, the UK has specific provisions in section 35 of the Data Protection Act 1998 which allow for the disclosure of personal data where required by law or made in connection with legal proceedings.

Approach to proportionality

However, before the Court makes an order for the disclosure of personal data, it must consider in the balance the potential value of that information to the party seeking the material against the interests of the relevant individual whose personal data will be disclosed. Whilst this general principle was agreed, the way the balancing act should be approached was not and formed the main thrust of Viagogo' appeal.

Viagogo sought to argue that the proportionality assessment should be approached on a narrow basis, considering, on an individualised basis, the impact that the disclosure would have on the individual concerned and weighing it against the value of information about that individual being disclosed – expressed in simple terms the question is: "*What value will the information about this particular individual have to the RFU*?"

The Supreme Court roundly rejected this assertion. The assessment of proportionality need not take place in a "hermetically sealed compartment" and instead the wider context in which disclosure was sought could be considered.

RFU's motives make disclosure proportionate

In this case, it was entirely proper to consider the RFU's "worthy motive" of maintaining ticket prices at an affordable level and the clear breach by sellers of the terms of those tickets. Moreover, the fact that disclosure of this information was likely to deter others from selling tickets at inflated prices in the future was also a relevant factor in this assessment. Taking these broader factors into account, the Supreme Court was in no doubt that the disclosure should be ordered.

However, the Supreme Court made it clear that there is no presumption that an order will be granted and that the Court of Appeal may have overstated its

position by suggesting it will “generally be proportionate” to make an order where there is arguable wrongdoing and no other means to obtain the identities of the wrongdoers. Each case depends on its facts.

For example, the Supreme Court supported the decision to only order partial disclosure in *Goldeneye v Telefonica* [2012] EWHC 723. That case involved a Norwich Pharmacal order against Telefonica and other internet service providers for disclosure of the identities of customers whose internet connections were used to share files, including pornographic films, using peer-to-peer file sharing software. The Supreme Court agreed that only partial disclosure was justified as the information was highly personal and not all of those customers would have actually uploaded those works (for example, others might have hijacked their internet connection). As a result, some customers might feel obliged to pay compensation for any copyright infringement just to avoid the embarrassment of being associated with pornography rather than as a result of any wrongdoing on their part. This contrasts starkly with the case in hand in which all that was sought were the names and addresses of sellers who had bought and sold tickets in clear contravention of the rules of those tickets.

See *The Rugby Football Union v Consolidated Information Services (formerly Viagogo Limited)* [2012] UKSC 55

By Alastair Walford, London

UK – *E-Nik v DECC*: Does contextual interpretation still allow for summary judgment?

In a recent dispute, the High Court had to consider if a short point on construction could be resolved on summary judgment. The modern contextual approach to interpretation requires the court to interpret clauses in light of the contract as a whole and the wider commercial background. Despite the uncertainties raised by this purposive approach, the court was still able to decide that the defendant's position was unarguable and give summary judgment to the claimant.

This decision thus provides a useful example of the limits of the modern approach to construction as well as considering a number of other points of interest – for example, whether it is possible to imply a term that prices are exclusive of VAT and whether "take or pay" clauses are a penalty.

IT consultancy services

The case of *E-Nik Ltd v DECC* [2012] EWHC 3027 arose out of a short consultancy agreement. The term was 2.5 years terminable on 12 months' notice. It was not drafted by lawyers and, in the judge's own words was "*not always elegant or apt*". The dispute centred on the following clause:

> *"The Authority hereby undertakes to purchase [a] minimum of 500 days of Consultancy from the Supplier per year based on project requirement, additional days will be required once the purchased days have been exhausted"*

The essence of the dispute was whether this created a binding obligation on DECC to purchase a minimum of 500 days' consultancy each year or whether this commitment ceased to apply if there was no "project requirement" for such work.

Application for summary judgment

E-Nik brought an action for summary judgment. This required it to show that DECC's position had no real prospect of success. E-Nik put forward a number of points relating to the other provisions of the contract or commercial background in favour of its interpretation. This included:

- that there was no definition of "project" and therefore no clear requirements that could be used to assess any amendment to the minimum purchase requirement;
- the 12 month termination period would be pointless if DECC could simply cease calling off services at any time;
- there was another provision in the agreement requiring E-Nik to provide a spreadsheet with the "number of days remaining", thus indicating a minimum commitment; and
- E-Nik was to invoice yearly in advance which could only be consistent with a minimum commitment on behalf of DECC.

To the extent that there was ambiguity in the provision, E-Nik relied on certain correspondence that occurred prior to the agreement being formed. Ultimately, the court was prepared to decide the point in E-Nik's favour without a full trial. As a matter of construction:

> the word "*minimum*" in the clause would be deprived of any meaning unless there was a fixed commitment; and

> it was perfectly satisfactory to construe the words "*based on project requirement*" as showing how the minimum of 500 days had been arrived at. The clause did not say, or mean, "*subject to project requirements*". In any event, even if there was an alternative construction, it was less commercially likely (*Rainy Sky v Kookmin Bank* [2011] 1 WLR 2900).

The decision follows earlier decisions, such as *Khatri v Raiffeisen-Boerenleenbank* [2010] EWCA Civ 397. In that case, the Court of Appeal emphasised that the commercial background is key to the construction of any contract. However, if there is no real conflict of evidence, the court should only decline to resolve a matter of interpretation on summary judgment where a full trial (with discovery, evidence and cross-examination) is likely to discover facts that make a real difference to the construction of that contract.

The final half year

The next point for the court was how the minimum commitment of 500 days per year applied to the last half year of the contract. Should the commitment to be pro-rated to 250 days? Alternatively, could the 500 days be spread over the whole third calendar year meaning that those 500 days could be allocated to the second half of the year after the contract had terminated?

Again, the court was happy to decide the point in E-Nik's favour as a matter of commercial common sense without the need for a full trial. DECC's construction, that no pro-rating was to take place, was uncommercial given the purpose of the contract was to ensure the availability of E-Niks services.

Was this "take or pay" clause a penalty?

The contract therefore contained a "take or pay" provision under which DECC had agreed to pay for 500 days of consultancy even if not ordered. Burton J referred to his earlier judgment in *M & J Polymers v Imerys Minerals* [2008] 1 All ER 893 that such a clause might qualify as a penalty clause.

However, in this case there was a clear commercial justification for the clause. E-Nik had kept resources available to provide consultancy services at commercially advantageous rates. Moreover, the clause was negotiated and entered into by parties of comparable bargaining power and there was no oppression. Accordingly, the minimum commitment was not a penalty.

Was there an implied term that the charges were exclusive of VAT?

The only reference to VAT in the agreement was an obscure statement that E-Nik would "*comply with all the requirements of VAT legislation*". DECC therefore claimed that the £850 should be inclusive of VAT, following the

position set out in section 19 of the VAT Act 1994. This position is also consistent with previous case law in which the courts have been reluctant to imply a term that prices are VAT exclusive.

E-Nik countered by arguing that a term should be implied that the charges were exclusive of VAT. The main thrust of its argument was that there was a course of conduct between the parties whereby all prices were exclusive of VAT. This somewhat hopeful argument was supported by:

> an assertion that a daily rate of £850 inclusive of VAT would result in the charges being lower than those for E-Nik's lowest grade of staff, whereas they were intended to provide a blended rate averaging out different staff charge out rates;

> the possibility that the rate of VAT might change meaning that the underlying charge out rates would vary in way beyond E-Nik's control; and

> the fact that invoices had been paid by DECC on a VAT exclusive basis. However, subsequent conduct by the parties cannot be used in the construction of a contract and no case on variation or estoppel was made or sustainable.

None of these factors were sufficient to persuade Burton J that there was any agreement that VAT should be added to the £850 per day charge and judgment was given on that point in favour of DECC.

By Caitlin Moor, London

UK – Will the Courts cut your indemnity down to size?

Commercial parties often try to rely on broadly worded indemnities to protect their position. But how much protection do they provide in practice? Two decisions earlier this summer suggest that broadly worded indemnities may be interpreted narrowly in a manner that reflects the underlying commercial purpose of the agreement.

An indemnity against "all consequences and liabilities"

The first decision by the Supreme Court arose out of the charter of The MT Kos (*Petroleo Brasileiro v ENE Kos* [2012] UKSC 17). The charterparty for the vessel allowed the owner to withdraw the vessel if the charterer failed to make payment when due. There was no "anti-technicality" clause in the charterparty so no need to warn the charterer of the impending withdrawal.

Accordingly, when the charterer missed a payment on 31 May 2008, the owners served notice to withdraw the vessel on 2 June 2008. At the time the vessel was withdrawn it was in port and had just completed loading a parcel of cargo in accordance with the charterer's orders. The charterer first tried to persuade the owner to withdraw the notice and then unloaded the cargo, that process completing 2.6 days after the vessel was withdrawn.

The owners sued the charterers for use of the vessel during that 2.6 day period. The basis for the claim was under the law of bailment and under the indemnity set out below:

> "*charterers hereby indemnify owners against all consequences or liabilities that may arise from the master, charterers or their agents signing bills of lading or other documents, or from the master otherwise complying with charterers' or their agents' orders*"

This indemnity is common to most modern time charters. It is a necessary part of such arrangements – if the owner is to surrender control of the vessel and put it under orders of the charterer, there is nothing unreasonable in wanting a complete indemnity in return.

However, as Lord Sumption observed in the lead judgment, whilst the indemnity is "*very wide ('all consequences or liabilities that may arise') … it is not "complete", nor is it unlimited*". In fact, the Supreme Court's decision places a number of restrictions on the scope of the clause. For example, the indemnity would not apply:

- "against things for which [the owners] are being remunerated by the payment of hire"; and
- "to risks which the owners have contractually assumed, which will usually be the case where they arise from, for example, their own negligence or breach of contract or consequences such as marine fouling which are incidental to the service for which the vessel was required to be available".

Having set these limits on the indemnity, the Supreme Court decided that the detention of the vessel was, in fact, within the scope of the indemnity as it

was "*not an ordinary incident of the chartered service and was not a risk that the owners assumed under the contract*". The charterers were therefore obliged to pay for use of the vessel during that 2.6 day period.

The case does, however, highlight the constraints that are likely to be placed upon a broadly worded indemnity and the need to interpret it in light of the wider commercial background.

Indemnities against third party claims

A similar contextual analysis was used to take a third party claim out of the scope of two indemnities in *Waite v Paccar Financial* [2012] EWCA Civ 901. This case arose out of the lease of a Foden A3-6M lorry by Paccar to Mr Waite.

At the end of the agreement, the lorry was sold for eventual use by a Mr Jones for £15,000. Mr Jones subsequently claimed that the lorry was not fit for purpose and lacked pulling power and issued proceedings seeking £42,000 in damages. Paccar entered into a settlement with Mr Jones for £7,000.

Paccar then sought to recover £18,918 from Mr Waite for the cost of the settlement and associated legal costs. The claim was brought under the following indemnities in the original lease agreement:

Clause 4 - "*You will*

> *i) as an obligation surviving termination of this Agreement, indemnify us against any loss, damage, or other expense we incur,(including legal costs on a full indemnity basis and as a result of any third party claim or otherwise),arising directly or indirectly out of the state, condition or use of the Vehicle or in any way arising out of our having entered in this Agreement,(except in the case of death or personal injury caused by our negligence);….*
>
> *iii) be responsible, at your own cost, for keeping the vehicle in good condition (allowing for fair wear and tear) and in full working order* …."

Clause 8 - "*we may at our discretion appoint you as our sales agent for the Vehicle on the following terms*: …

> *iii) the vehicle must be sold for business use without the benefit of any warranty, representation or condition on our part (save that we can pass good title);*
>
> *iv) you must indemnify us against all losses, damage, costs, claims and expense arising out of the sale (including legal fees) on a full indemnity basis in connection with any proceedings against us brought by any purchaser*; .."

Despite the broad wording of these clauses, Paccar's claim failed. Neither indemnity applied to its claims. The indemnity in Clause 4(i) was not applicable for a number of reasons:

- the provisions of Clause 8 dealt with the sale of the vehicle and provided a complete code for liability attached to that sale. Clause 4 was not applicable;
- in any event, the indemnity only covered acts and omissions by Mr Waite during the period of his hire of the lorry and not the sale which took place afterwards (though clearly any ongoing liability under that indemnity would survive); and
- the indemnity in clause 4(i), read in context, did not apply where Mr Waite had kept the vehicle in good condition in accordance with Clause 4(iii).

The indemnity in Clause 8(iv) was similarly not applicable when read in light of the earlier Clause 8(iii). This stated that the sale was to be made without any warranty as to the condition of the vehicle. The lorry was "sold as seen" and Mr Jones should have had no right to bring an action for its alleged lack of pulling power. Accordingly, Paccar's decision to settle the claim was therefore a free-standing decision outside the terms of the contract and the indemnity given by Mr Waite.

Commercial interpretation

It is trite law that contractual clauses must be interpreted in light of the other provisions of that contract and the wider commercial background. However, these cases provide a useful illustration of how that process applies to broadly drafted indemnity clauses and the possibility that their meaning might be narrowed dramatically.

By Peter Church, London

Author: Peter Church

Contacts

For further information please contact:

Tanguy Van Overstraeten
Partner

(+32) 2501 9405

tvanover@linklaters.com

Peter Church
Solicitor

(+44) 20 7456 4395

peter.church@linklaters.com

One Silk Street
London EC2Y 8HQ

Telephone (+44) 20 7456 2000
Facsimile (+44) 20 7456 2222

Linklaters.com

A15846426/0.5/26 Nov 2012