Data Protection and Freedom of Information

EU - First BCR Authorisation Under The Mutual Recognition Procedure

Hyatt Hotels Corporation has received authorisation for its binding corporate rules. They allow Hyatt to make international transfers of personal information within the Hyatt Hotels & Resorts business in compliance with the Data Protection Directive.

Authorisation from the UK Information Commissioner

The authorisation, from the UK’s Information Commissioner, is the first to use the new mutual recognition procedure. Once a set of simple administrative steps are taken, Hyatt will receive automatic approvals in a number of other European states.

The mutual recognition procedure was launched in October 2008 by the Article 29 Working Party, the panel of EU data privacy regulators. It provides a “one-stop” shop for BCR applications covering 17 EEA member states including France, Germany, Italy, Spain, the Netherlands and the UK.

A more streamlined approach?

The procedure significantly speeds up the application process for binding corporate rules. Hyatt’s application, which forms part of a compliance programme in 45 countries, took 12 months from start to finish, significantly less than earlier applications conducted under the old “co-operation” procedure. Previous applications had taken several years to complete. The recent streamlining of the application documents should in our view reduce that time still further, making an approval time that is measured in months credible for the first time. As a result, for the right organisation, binding corporate rules have now become a credible and achievable means to legitimise international transfers of personal data.

BCRs are not the only means of achieving compliance with the data export obligations in the Data Protection Directive, but they are the most flexible. Alternative approaches, which may suit some organisations better, include the use of intra-group agreements and the US Safe Harbor. For the right organisation, however, BCRs may now claim to be the quickest approach to achieving compliance.

Media

EU - Advocate-General’s Google AdWords Opinion Leaves Questions For The ECJ

France - The Hadopi Law and France’s Controversial Fight Against Piracy

Spain - New Broadcasting Regulations

France - Piecing Together The Online Gambling Jigsaw

Outsourcing

EU - Managing Contracts In Challenging Times
Linklaters LLP assisted Hyatt Hotels Corporation with this process and is working on a number of other binding corporate rules applications, with further authorisations expected in the near future.

The Binding Corporate Rules Authorisation is available here

By Richard Cumbley, London

France - CNIL Issues Its Investigation Programme For 2009

The French data protection authority (Commission Nationale de l'Informatique et des Libertés - “CNIL”) has published its investigation programme for 2009 on its website www.cnil.fr. In its announcement of 11 June, the CNIL describes the programme as “ambitious” and one forms part of its policy to “give priority to on-the-spot investigations”.

Overview

The programme is important because it gives a clear idea of the CNIL’s enforcement priorities over the next year. Such investigations are also an increasingly important part of the CNIL’s enforcement strategy. The CNIL sets out on its website that of the 218 investigations made in 2008 “almost 40 per cent of them were carried out in accordance with its annual investigation programme”. For such investigations, the CNIL has access between the hours of 6 a.m. to 9 p.m. to the facilities hosting the data processing operation. Pursuant to article 44 of the French Data Protection Act, an investigation may only start after prior notification to the public prosecutor and, in the event of any opposition by the tenant of the facilities, after authorisation from the President of the first instance court (Tribunal de Grande Instance).

Although the CNIL’s clear intention is to take enforcement action across the “whole of France”, it seems likely that most of it will focus on Paris and the surrounding region (except for investigations of local authorities). Indeed, at the 5th Data Protection Officers’ Conference, the CNIL’s representatives acknowledged it was difficult to police other regions without additional resources.

Enforcement Priorities

The programme targets both the public and private sectors. In the “private sector”, the following areas are targeted for further investigation:

- **Electronic voting systems** – Whether these systems are used by public or private entities.

- **Security** - The CNIL will look into the “security measures implemented” for “data processing of national importance in both the private and public sectors”.

- **Marketing** - The CNIL has decided to look into “new techniques”, (the CNIL refers to “Bluetooth marketing” as an example), as well as the selection methods used for targeting new groups of people or “communities”, used by businesses and more specifically websites.

- **Medical data** - The CNIL intends to review the data processing activities carried out by a variety of “organisations in the healthcare sector” (and, in particular, the “security measures” applied to those activities).
- **Sport** - Football clubs will be under review with a particular focus on “the banning of supporters from football stadiums, including through the use of “video surveillance with biometric recognition”.

- **Private intelligence** - The CNIL intends to continue checking the data processing activities carried out by private investigators.

- **Labour/Recruitment** - The CNIL intends to check the “data processing activities of recruitment operations” of “important companies” along with recruitment websites and agencies.

- **Insurance and Transport** - Activities such as GPS “tracking of car policyholders” (géolocalisation) by insurance companies and the use of “electronic tickets” by public transport operators will be reviewed.

**Sanctions**

Since 2004, the CNIL has had the power to use a wide array of sanctions (article 45 of the French Data Protection Act) including issuing a warning, a formal demand, an administrative fine of up to €150,000, or up to €300,000 in cases of a repeated breach (within a limit of 5 per cent of the turnover), and/or an order to cease processing. Finally, in urgent proceedings the President of the CNIL can order that appropriate security measures be taken. Breaches may also lead to criminal proceedings.

The CNIL’s 2008 annual report and website sets out financial sanctions previously imposed. Significant fines have been imposed for:

- Abusive registration by banks of several clients in the Banque de France file which, for example, resulted in the first use of an administrative fine in June 2006 for €45,000.

- Abusive marketing via email, telephone and fax - for example, in November 2008 there were two fines of €30,000 each.

- Creation and use of a database showing the racial and ethnic origins of people, which resulted in a fine of €15,000 in January 2008.

- Injurious comments in employees’ files, which resulted in a fine of €40,000 in December 2007.

- Various breaches of the French Data Protection Act by debtor research companies in relation to which a fine of €10,000 was imposed in October 2007 and another of €50,000 in June 2007.

Quotes are drawn from the website of the CNIL to which you can refer for the full text: www.cnil.fr. All rights (including copyrights) being reserved by the CNIL.

*By Stéphanie Faber, Paris*
Germany - Amendments to the Federal Data Protection Act

On 3 July 2009, the German Bundestag passed the Federal Data Protection Act Amendment Law (Novelle des Bundesdatenschutzgesetzes) the majority of which entered into force on 1 September 2009. The amendment is a result of various high profile data scandals as well as the attempted sale of marketing data for millions of individuals.

Legislative history

By the spring of 2009, the Federal Data Protection Act Amendment Law had become the subject of strategic manoeuvring by political parties in the run-up to the German Bundestag elections in September 2009. Various provisions were discussed heatedly and were the subject of intense lobbying, in particular the deletion or restriction of the so-called list privilege for marketing measures. However, the home affairs committee was able to agree a compromise in its last meeting before the summer break and the Bundestag thus passed the Federal Data Protection Act Amendment Law.

The final text did not include some of the other more controversial provisions, such as additional protection for employee data. Instead, it only includes a brief, generally worded provision relating to employee data incorporated in the newly created section 32 of the Federal Data Protection Act, while the introduction of additional protection was, again, postponed to the next legislative term. The German Bundestag also abandoned the proposed data protection audit law, which would have allowed for audits of companies by certified auditors. Finally, the new law also does not contain the highly controversial right of associations to institute legal action.

Key amendments

The changes to the Federal Data Protection Act are still significant. A detailed summary of the changes is available here and includes:

- an requirement for new detailed wording in data processor contracts;
- breach notification requirements;
- expanded powers to intervene for supervisory authorities; and
- increased fines, including potential confiscation of profits.

An increase in enforcement?

The risk of security breaches and illegitimate transfers has therefore increased considerably. Once a data controller has made a notification about the breach (and endured the associated media coverage) it can then expect an investigation by the competent data protection supervisory authority (who now has expanded powers of intervention), followed by an enhanced punishment (which could now include retrospective confiscation of profits).

From a risk management perspective, both the potential damage and consequences of breach of data protection law have increased as a result of the amendments to the Federal Data Protection Act. These risks are further exacerbated by the increased public attention to, and media coverage of, data protection infringements by large corporates since 2008.

By Dr Konrad Berger, Munich, and Dr Daniel Pauly, Frankfurt
UK - Is Data Protection More Than Just Data Security?

Christopher Graham has recently reached the 100-day mark as Information Commissioner and many will want to understand his vision for the future development, promotion and enforcement of data protection legislation in the United Kingdom. One issue in particular is whether the data protection agenda, or at least the enforcement agenda, has become too focused on data security.

It’s useful to consider this issue in light of the enforcement activity taken by his office over the last couple of months (set out in the table below).

<table>
<thead>
<tr>
<th>September 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing Pharmacy Ltd</td>
</tr>
<tr>
<td>NHS Grampian</td>
</tr>
<tr>
<td>NHS Education for Scotland</td>
</tr>
<tr>
<td>Ipswich Hospital NHS Trust</td>
</tr>
<tr>
<td>Sandwell Borough Council</td>
</tr>
<tr>
<td>Wigan Council</td>
</tr>
<tr>
<td>Matthew Single</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>August 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Borough of Sutton</td>
</tr>
<tr>
<td>Repair Management Ltd</td>
</tr>
<tr>
<td>East Cheshire NHS</td>
</tr>
<tr>
<td>Dr Paul Thomas</td>
</tr>
<tr>
<td>UPS Ltd</td>
</tr>
<tr>
<td>Various construction firms (14 in total)</td>
</tr>
</tbody>
</table>

Laptops and memory sticks

It is clear that the majority of the enforcement action is still directed at data security and, in particular, personal information on laptops and memory sticks. It is inevitable that these devices will be lost or stolen from time to time, so full disk encryption is essential to ward off any subsequent enforcement action. This is reflected in the Information Commissioner’s guidance: “There have been a number of reports recently of laptop computers containing personal information which have been stolen … where such losses occur and where encryption software has not been used to protect the data, enforcement action will be pursued”.

"the use of password protection (i.e. using a BIOS or Windows password is insufficient ... Password protection was in place in many of the cases but did not prevent enforcement action"
The Information Commissioner also considers that the use of password protection (i.e. using a BIOS or Windows password) is insufficient. Password protection may prevent the laptop from being activated but it is still very easy to just take the hard disk out of the laptop and access the data on it using another computer. Password protection was in place in many of the cases in the table but did not prevent enforcement action.

A wider data security agenda

The data security agenda is, however, wider than just lost data on mobile devices. For example, undertakings were sought from Billing Pharmacy Ltd for theft of an unencrypted desktop computer containing medical details. The information was sensitive (in every sense of the word) and so deserved a high degree of protection, but the enforcement raises a question of whether encryption now ought to be applied to desktops as well as laptops. This would certainly now seem prudent if the desktop is used to store substantial amounts of personal information.

Other evidence of a wider security agenda comes from the enforcement action against NHS Grampian. They were subject to a range of security breaches, including emailing a patient’s medical details to over 50 other members of staff without any proper reason to do so. Screening software provides some protection against inappropriate email disclosures but there still is no technological silver bullet or substitute for comprehensive staff training on proper data handling.

Finally, insecure disposal of information is also likely to lead to enforcement action. Dr Paul Thomas had to give undertakings after a server containing medical information about his practice’s patients was found in a skip. At a minimum, the hard discs in any computer should be overwritten using specialist software before their disposal. A hammer and nail is a good solution for particularly sensitive information.

Future focus

Enforcement action was taken for other reasons in two cases: the prosecution of Matthew Single for leaking the BNP membership list and the enforcement notices served against construction companies for use of a secret employee blacklist. However, data security is still the main area of enforcement and it seems likely this will remain the case for the near future. There are a number of reasons for this:

- poor data security can lead to real consumer harm as a result of identity theft and invasion of consumer privacy;
- the Information Commissioner receives a steady stream of data breach notifications from data controllers (currently there are about 20 notifications a month from the public sector and 10 notifications a month from the private sector), providing rich pickings for subsequent enforcement activity; and
- in some cases, the security measures taken by data controllers are simply not good enough.

A more interesting point is whether the means of enforcement will change. The “undertaking” was extremely effective when it was first deployed and those on the receiving end could expect significant adverse publicity. However, undertakings have now largely lost their sting and the frequency
with which they are now issued means they do little to “name and shame” the offending organisation.

The Information Commissioner may instead be looking forward to April 2010 and the ability to issue monetary penalty notices. Many serious security breaches are likely to satisfy the threshold criteria for such notices - i.e. (i) there is a serious breach of the data protection principles, (ii) that is likely to cause substantial damage or substantial distress, and (iii) the breach is deliberate or reckless - so while data protection may be more than just data security, data security is likely to remain in the headlines for some time to come.

By Julian Cunningham-Day and Peter Church

UK - Utilities and Freedom of Information

The Government has recently announced that it is “attracted to” applying the Freedom of Information Act 2000 (the “Act”) to utility companies. This is a potentially burdensome and intrusive development and is likely to result in significant lobbying by the utility sector.

What is the effect of the Act?

The Act entitles any person to request information held by, or on behalf of, a public authority. The public authority must provide that information unless it falls within a statutory exemption. There is no need to justify the request and, with certain limited exceptions, the identity and motive of the person making the request is irrelevant. The Act is therefore potentially burdensome and intrusive.

Who is caught by the Act?

The Act applies to “public authorities”. They are persons:

- listed in Schedule 1 to the Act. This includes a vast range of public sector and quasi-public sector bodies, from the Financial Services Authority to Sir John Soane’s Museum;

- wholly owned by the Crown or a public authority listed in Schedule 1; or

- designated as a “public authority” by the Secretary of State under section 5. A designation can be made if that person: (a) appears to the Secretary of State to “exercise functions of a public nature”, or (b) is “providing under a contract made with a public authority any service whose provision is a function of that authority”.

A consultation on the third limb was issued in October 2007. The Government finally issued a response to that consultation in July 2009 setting out whether further designations should take place.

Who is now likely to become a public authority?

The response indicates that, subject to further consultation, the following entities will be designated as public authorities under section 5:

- academy schools;

- The Association of Chief Police Officers;
Will the utilities also become public authorities?

The response considers a range of other bodies, including professional regulators, charities and public service contractors. In general, it concludes that designation of these bodies is not currently appropriate.

However, the position is different for the utility sector. The Government states “it is attracted to bringing such utilities within the Act. While it does not propose to include utilities in the first section 5 order, it will carry out a further consultation with the bodies concerned to assess whether it would be appropriate to include some or all of them in a subsequent section 5 order, or to extend the scope of the Act to cover them in a different way”.

This will potentially be of concern to many utility companies, who may wish to prepare for this further consultation process, for example by considering if they are likely to perform a function of a public nature (using case law developed under the Human Rights Act 1998) and if there are wider human rights arguments that could be deployed against any such designation.

The utility sector is also quite diverse so the utility companies should be aware that the Government may employ different approaches to different types of utility. By way of example, the arguments for designating telecoms companies are likely to be particularly weak.

The response to the consultation is available here

By Peter Church, London

UK - A Strict Approach To Sensitive Personal Data?

Last year the House of Lords considered the interaction between freedom of information and data protection. Lord Hope concluded that there was no presumption in favour of disclosing personal data and, in the case of sensitive personal data, it is not appropriate “for the statutory language to be construed liberally in favour of the release of information … If none of the conditions [for processing sensitive personal data] can be met, so be it.”

This article considers three recent decisions by the Information Tribunal on the disclosure of sensitive personal data. It also consider the practical implications from a wider data protection perspective.

O’Connell v Information Commissioner & Others EA/2009/0010

This decision arose out of the conviction of one of the members of the Guildford Four, Patrick Armstrong. The Guildford Four successfully appealed against their convictions and were released in 1989. Subsequently, in 1993, three of the police officers involved in the investigation were tried for conspiracy to pervert the course of justice and, as part of that trial, various documents were put before the jury, including counsel’s defence brief for Patrick Armstrong.

Mr O’Connell made a request for a copy of that original defence brief to the Crown Prosecution Service under the Freedom of Information Act 2000
The request was refused and the matter came before the Information Tribunal. It found that information in the defence brief constituted sensitive personal data about Patrick Armstrong, one of the members of the Guildford Four, as it related to the alleged commission of offences by him.

This meant the defence brief could only be disclosed under FoIA if, amongst other things, a condition for processing (i.e. disclosing) sensitive personal data could be established. No processing condition could be found, despite the fact that it is publicly known that Patrick Armstrong had been convicted and then acquitted. The information was therefore exempt under FoIA.

Heath v Information Commissioner EA/2009/0020

This decision also relates to criminal proceedings. A man killed a young girl in 1968. He was sentenced to life imprisonment, with the trial judge apparently expressing the view that the killer should never be released. Later, in 1992, a 10-year tariff was applied to the killer’s sentence.

Mr Heath made a freedom of information request for a copy of that tariff certificate. The request was refused and eventually came before the Information Tribunal. It decided that the information in the tariff certificate was sensitive personal data about the killer. This was because it related to the commission of offences and the sentence of the court.

Again, the certificate could therefore only be disclosed if, amongst other things, a condition for processing sensitive personal data could be established. No such condition could be found in this case, despite the fact the information about the sentence imposed on the killer was already known to Mr Heath.

Riniker v Information Commissioner & Others EA/2007/0132

The final request related to a freedom of information request by Ms Rinker which, amongst other things, asked for copies of petitions made to the Visitor of London University. The petitions had been brought by students of the University of London about their exam or PhD results. The Information Tribunal found that the petitions contained personal data and, in many cases, also contained sensitive personal data such as racial origins, political opinions or religious beliefs.

Ms Riniker asked that the information be redacted so that it could be released to her in an anonymised format. However, this was not possible. Whether the information is in fact anonymised (i.e. relates to identified individuals) must to be assessed from the perspective of the person disclosing the information. In this case, the public authority would have been able to identify the individuals concerned from the redacted petition from other information it holds (i.e. the unredacted petitions) even if Ms Riniker could not. This follows the House of Lords decision in Common Services Agency v Scottish Information Commissioner [2008] UKHL 47.

Accordingly, even if the petitions were released to Ms Riniker in a redacted format, it would still be necessary to satisfy a condition for sensitive personal data in respect of any sensitive personal data in that petition. No processing conditions were applicable, so the petitions were exempt under FoIA.

A new approach?

The outcomes of the cases are quite curious. For example, Mr O’Connell was not entitled to the defence brief because it revealed Patrick Armstrong’s
alleged involvement in the Guilford bombings - despite his conviction and subsequent acquittal being public knowledge. Ms Riniker could not see sensitive personal data in petitions lodged with the Visitor to the University of London, even if those petitions were redacted so as to be anonymised in her hands.

This strict approach may reflect the fact that a disclosure under FoIA is effectively a disclosure to the public at large and accordingly the hurdle for disclosure must be higher than that for a disclosure to a limited number of people.

However, applying a similar literalistic approach outside the FoIA context could cause real practical difficulties, especially as redaction or pseudo-anonymisation may not be sufficient to take information out of the data protection framework and a broad interpretation of sensitive personal data has been taken in the past (e.g. the decision in Murray v Express Newspapers [2007] EWHC 1908 that a picture of a child was sensitive personal data as it revealed his ethnic origin). While a more pragmatic approach to the interpretation of the processing conditions for sensitive personal data and/or enforcement of the Data Protection Act 1998 may resolve some of these issues, those disclosing sensitive personal data should continue to do so with caution.

O’Connell v Information Commissioner EA/2009/0010 is available here

Heath v Information Commissioner EA/2009/0020 is available here

Riniker v Information Commissioner & Others EA/2007/0132 is available here

By Peter Church, London
EU - Advocate-General’s Google AdWords Opinion Leaves Questions For The ECJ

Google’s use of its AdWords tool cannot in itself amount to trade mark infringement. So considered Advocate-General Poiares Maduro, assistant to the European Court of Justice, in an opinion delivered on 22 September 2009 following a reference to the Court by the French Cour de Cassation (Joined Cases C-236,7,8/08, Google France and ors v Louis Vuitton Malletier and ors). The Court usually - although not always - follows the Advocate-General’s opinion, which is thus a strong indication of the way in which the Court will finally rule.

Keywords

Google (along with other search engine providers) supplies a keyword sponsorship product (in Google’s case, AdWords) which enables advertisements to be displayed, alongside “natural” results, in response to designated inputted keywords. Advertisers select keywords so that their ads are displayed in response to the input of those keywords and pay Google on the basis of the frequency with which users click on the ads’ links. A number of trade mark owners, including Louis Vuitton, sued Google France for trade mark infringement in France on the basis of the use of their marks as sponsored keywords.

Opinion of the Advocate-General

The Advocate-General drew a clear distinction between the use as such in AdWords of keywords corresponding to trade marks and the use of trade marks in advertisers’ sites or the products sold on those sites; the reference concerned only the legality of the former; the legality of the latter forms of use could only be assessed on their own terms. The Advocate-General broke keyword use down into two elements:

(a) the offer by Google to advertisers of keywords to sponsor; and

(b) the display of ads in response to the input of keywords.

He found no infringement in relation to (a) since the use of the trade marks as keywords was not made in relation to the goods for which the trade marks were registered, for example, leather goods, but in relation to Google’s own AdWords service. He also found no infringement under (b) on the basis that searches were unlikely to be confused into thinking that the results of a search inputting a particular trade mark necessarily linked to the trade mark owner (or an economically related undertaking). In addition, the selection by advertisers of keywords to sponsor could not amount to infringement since in this context the advertisers were acting privately as consumers and not in the course of trade.

The Advocate-General’s analysis under (b) appears to be deficient: it is not necessary to demonstrate a likelihood of confusion when seeking to establish infringement on the basis of use of an identical mark in relation to identical goods and services, for example, where a link to a leather goods retailer is displayed following the input of, say, Louis Vuitton as a search term. The question that the Advocate-General arguably had in mind was whether the display of ads in response to the input of keywords was liable to affect the functions of the trade mark, in particular, whether it would be interpreted by
consumers as a designation of origin of the goods covered by the mark and thus infringing. By including the need to show a likelihood of confusion as part of the test, the Advocate-General may have set too high a bar for trade mark owners when seeking to establish infringement.

In the context of the additional protection conferred by trade mark law on marks with a reputation, such as the Louis Vuitton mark, the Advocate-General adopted a broad approach and considered that Google’s use of such marks as keywords could not be prevented, as the need for freedom of expression and commerce outweighed the need to protect the investment that goes into such marks. If followed by the Court, this balancing exercise would likely represent a development of the law in the trade mark sphere.

Unsurprisingly, the Advocate-General rejected the suggestion that Google could be liable for contributing to infringing acts by third party websites whose links were displayed in response to inputted keywords; questions of joint liability are not addressed by EU legislation and fall to be determined as a matter of national law.

Hosting exemption

Finally, the Advocate-General opined that if Google were found liable for infringement, it would not be able to rely on the E-Commerce Directive (2000/31/EC) to exempt it from such liability. Although he considered Google’s search engine and provision of hyperlinks under AdWords to be covered by the Directive (as information society services), its activities could not be described as mere hosting and thus susceptible to exemption, since it did not remain neutral in its operation of AdWords; it retained an interest in users clicking on links to the ads.

Questions for the ECJ

While the opinion may not on the whole be favourable to brand owners, it still raises a number of questions for the Court to consider. Moreover, since the rules on joint liability fall to be decided on a national basis, it may be unrealistic to expect courts across the EU to be consistent in their decisions on liability of search engine providers in this area, in the short term at least.

By Marianne Schaffner and Lorraine Sautter, Paris

France - The Hadopi Law and France's Controversial Fight Against Piracy

Internet piracy is on the rise in France. A report by the French National Assembly indicates that over the last five years the music industry has lost a staggering 50% in both sales and overall profit, record labels have experienced a 30% drop in employment, and the number of new artists signed has fallen by 40% per year. Video production companies have also felt the sting, with industry turnover diminished by 35% over the same period. All in all, the impact that piracy had on the entertainment sector as a whole was estimated at a Euros 1.2 billion in 2007 and resulted in the direct loss of approximately 5,000 jobs.

In order to address these concerns, French legislators introduced the Creation and Internet Law (the Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet or “HADOPI 1”) in June 2009. The objective of this law is twofold:

"over the last five years the music industry has lost a staggering 50% in both sales and overall profit"
to provide a gradual response to the growing piracy problem; and

to encourage the development of legal content available for download.

After part of this law was annulled by the French Constitutional Court, a second complementary law was introduced in order to rectify the constitutionality issues. The Law for the Protection under Criminal Law of Artistic and Literary Works on the Internet ("HADOPI 2") was adopted by the National Assembly in September 2009.

A new administrative body

HADOPI 1 created an independent administrative body (the "Authority") to deal with protection of online works of art. In order to perform this function, the Authority is granted the power to recommend any legislative or regulatory modifications that it deems necessary, and may be consulted by the government regarding any bill or decree involving the protection of literary and artistic property.

Illegal downloading: Three strikes and you’re out

Under Article L. 336-3 of the Intellectual Property Code, individual Internet subscribers have a duty to ensure that their accounts are not accessed in order to reproduce, misrepresent, make available or communicate copyrighted artistic works without the prior consent of the owner of the works (the "duty to supervise"). The Authority’s progressive warning procedure ("riposte graduée") is set out in Article L. 331-26 and takes a “three strikes” approach.

First strike - When the Authority has reason to believe that an Internet subscriber is in breach of the duty to supervise use of their account, it may send electronically a “recommendation” to the subscriber reminding them of this duty. Along with the reminder, the notice must also contain information regarding legal sources of online cultural content, tools that allow the subscriber to better secure their Internet account in order to avoid illegal downloads, and even the negative impact that illegal downloading has for the advancement of artistic creation and the economy in the artistic sector.

Second strike - If a second breach is detected within the six months following the first recommendation sending date, the Authority can send a second recommendation repeating the same information as the first one.

Third strike - Under Article L. 331-27 of the Intellectual Property Code as per HADOPI 1, if the subscriber fails again to properly supervise use of their account within the year following the receipt of a recommendation, the Authority could, after an administrative hearing and in relation to the gravity of the conduct, pronounce one of the two sanctions as follows:

- suspend internet access for between two months and a year, during which the subscriber is prohibited from entering into a service contract with any other internet service provider; or

- order the subscriber to implement security measures designed to prevent the reoccurrence of illegal downloads, with penalty fees for non-compliance.
Finally, HADOPI 1 also set forth a procedure by which the Authority, on its own initiative, could propose a settlement to the subscriber who undertook to rectify their behaviour in certain cases.

Article L. 331-30 of the Intellectual Property Code clarifies that suspension of access in no way affects the contract between the sanctioned subscriber and the internet service provider nor any bundled service (i.e. television, phone). Furthermore, the subscriber would have to pay if they terminated their contract during the suspension period.

Cancellation by the French Constitutional Court

In June 2009, the Constitutional Court declared that certain provisions of HADOPI 1 were unconstitutional, including those giving the Authority the power to suspend Internet access for up to one year.

The Court considered this sanction to be a disproportionate infringement on freedom of expression and communication, a fundamental right guaranteed by the Constitution. While it didn’t go as far as classifying Internet access as a fundamental right in itself, the Court nonetheless emphasised that freedom of expression and communication implies access to online communication services. As such, only a judicial, and not an administrative, body should have the jurisdiction to impose such a sanction.

The Constitutional Court also took issue with the fact that HADOPI 1 placed the burden of proof on the Internet subscriber, who had to demonstrate that they were not responsible for the alleged piracy (e.g. by demonstrating that they properly secured their Internet access or that a third party was in fact responsible for said piracy). This results in a presumption of guilt on the Internet subscriber which infringes the presumption of innocence, a principle constitutionally guaranteed under French law.

Finally, HADOPI 1 was challenged for not striking the right balance between the protection of copyright and privacy rights (see the ECJ decision in Promusicae v Telefonica (C-275/06)). Under HADOPI 1, the Authority issued warnings on the basis of data (the IP addresses of Internet subscribers) provided by sworn agents (designated by entities representing the copyright holders). The Constitutional Court held that processing by these sworn agents, and the transmission of related data to the Authority, is not an unwarranted infringement of subscribers’ privacy rights.

New law: HADOPI 2

As a result of the decision of the Constitutional Court, a new bill (“HADOPI 2”) was introduced to complete HADOPI 1 and address the concerns of the Constitutional Court. This bill has been finalised but is subject to review by the Constitutional Court.

HADOPI 2 will remove the Authority’s power to impose sanctions directly on the Internet subscribers, only a judge having this power. Instead, the Authority’s function is now:

- to monitor illegal internet downloading; and
- to warn individuals when detecting illegal downloads made from their accounts.
Under HADOPI 2, a subscriber’s Internet access may be suspended not only for failing to secure access to an Internet account (as provided for in HADOPI 1) but also for copyright infringement over the Internet.

HADOPI 2 also allows a judge to suspend access to the Internet, as a form of “supplementary sentence” for copyright infringement over the Internet. Infringement actions can also be conducted using a streamlined procedure under which a single judge can issue a criminal order (ordonnance pénale) without a hearing on an ex parte basis. The order can result in either a discharge or the imposition of a fine or additional penalties. The Internet subscriber may, however, challenge this criminal order and ask that the case be reheard in inter partes proceedings.

The judge may also suspend a user’s Internet access for up to one month for gross negligence (négligence caractérisée) in the supervision of access of their Internet account. Therefore, the owner of an Internet account may be liable even if they are not illegally downloading material themselves. Under HADOPI 2, gross negligence is established if illegal downloads are detected within one year of a user receiving a recommendation from the Authority asking them to implement security tools for their account.

Technological arms race

The French Government introduced HADOPI 1 and HADOPI 2 to control Internet piracy and deter users from downloading copyright material. However, the laws may already be outdated as Internet users use new technology to circumvent their requirements.

For example, Internet pirates can mask their identity with relative ease by using an anonymous proxy or a VPN server that conceals the end user’s IP address, allowing copyrighted content to be downloaded without leaving a trace.

New means and measures will have to be adopted to fight this type of Internet piracy. However, HADOPI 1 and 2 should still deter the average Internet subscribers, which is their main objective.

The road ahead

On 28 September 2009, a group of Parliament members filed an application to annul HADOPI 2 before the Constitutional Court. They are challenging the constitutionality of the entire law and, in particular, the use of the aforementioned ex parte criminal procedure.

France is not the only country to adopt a repressive approach vis-à-vis Internet piracy. For instance in Sweden, a law dated 1st April 2009 provides that the copyright holder is granted the right to obtain the IP address of the alleged infringer. Furthermore, the Swedish courts recently took decisive action against the operators of The Pirate Bay. Will HADOPI lead to equally spectacular decisions in France?

The French National Assembly Report n° 1841 On the Protection of Literary and Artistic Property under Criminal Law, 16 July 2009 is available here

The Constitutional Court decision n° 2009- 580, 10 June 2009 on HADOPI 1 is available here

By Grégory Sroussi, Paris
Spain - New Broadcasting Regulations

The Spanish Government continues to update and amend the regulation of the broadcasting sector. The most recent changes affect pay-TV, advertising and media ownership. Other amendments are under discussion and could be approved during 2010.

Pay-TV and advertising

Private TV operators will now be able to broadcast one of their channels on a subscription basis. This has dramatically changed the broadcasting landscape, particularly with regard to premium contents such as football matches. Public TV will no longer be allowed to carry advertising and must be available free-to-air. As a consequence, a new system to finance public TV has been put in place, whereby:

- private TV operators will contribute 3 per cent of their earnings from free to air TV and 1.5 per cent in the case of pay TV; and
- telecom operators will contribute 0.9% of their earnings.

The new system to finance public television is currently under close scrutiny by the European Commission. A number of telecom and TV operators may also challenge the new system of finance.

Media ownership

Restrictions on the ownership of television channels have been relaxed. It will now be possible to hold a significant stake (defined as being more than 5 per cent) in more than one nationwide private TV broadcaster, or even to merge them. However, certain conditions must be met when the significant stake is acquired:

- the joint market share of the affected TV broadcasters must not have exceeded 27 per cent during the previous year; and
- there must be at least three distinct broadcasters to ensure a variety of media sources.

While corporate transactions have been expected for a number of months, none have taken place, and none of the various rumoured combinations of TV operators have yet materialised.

Future changes

Other changes will take place if the Bill on the General Act for Audiovisual Communication is approved. This includes the creation of a watchdog that would, among other things, ensure that TV operators comply with the Audiovisual Media Services Directive. There will also be a new enforcement system that would lead to severe penalties for infringements. In addition, spectrum trading will be clearly regulated and new regulations on the acquisition of premium contents would be approved.

The Government is hoping the General Act for Audiovisual Communication will be approved during the course of 2010. However, this is not the first attempt to regulate the media sector as a whole, and all previous attempts have ultimately encountered insurmountable obstacles.

By Carmen Burgos and Beatriz Pavón, Madrid
France - Piecing Together The Online Gambling Jigsaw

The French self-regulatory organisation for advertising (Autorité de Régulation Professionnelle de la Publicité or “ARPP”) issued a Note of Guidance on advertising for gambling and lotteries in June 2009. This note will come into effect in October 2009.

This Note of Guidance applies to both internet and “bricks and mortar” gambling, and has clearly been prepared to complement the draft law on internet gambling currently being discussed by the French Parliament.

Draft bill on internet gambling

France has decided to enact a new law that will “open” the gambling and betting market in response to pressure from EU competition authorities and to fight against the numerous overseas online betting and casino sites used by French gamblers. However, the draft bill still focuses more on regulating the market rather than encouraging competition.

French law currently prohibits lotteries and games which are open to the public and involve a “monetary” payment from the participant in return for an expectation of a gain based, even partially, on chance. The main exceptions are:

- monopolies on lotteries and betting services granted to specific bodies and, in particular, the state owned Française des Jeux, which has the gambling monopoly on football and on lotteries. Some of these bodies also provide lottery and betting services on the internet;
- licences granted to “brick and mortar” casinos. These casino operations are highly regulated; and
- private gaming circles (cercles de jeux). These are non-profit-making associations where gaming is only an ancillary activity. They also require authorisation from the relevant ministry.

The bill has been criticised because of its very limited scope (online horse and sports betting and online poker) and the numerous constraints imposed on the operators. These include deletion of information held by applicants on former French customers (to avoid any springboard effect when entering the market), limitation on gamblers’ returns, taxation and royalties due to the relevant sporting event organisers.

Nonetheless, a number of gambling operators are preparing themselves for this opening to secure market share in the hope of further liberalisation or, in the much longer term, harmonisation on gambling regulations at EU level.

Other preparatory steps

Pending the official creation of the online gambling regulator (Autorité de régulation des Jeux en Ligne or “ARJEL”), an interim group has been appointed to start working on the future specifications and filing formalities with the aim of being “ready” to meet the target date to implement the new gambling law.

Indeed, the intention of the French legislator is to issue the law ahead of the 2010 Football World Cup in South Africa. The bill was originally presented in March 2009 and has been just adopted by the Assemblée Nationale in
October 2009 (available here). It will now be submitted to the Sénat. To keep to the current deadline it may be necessary to use the urgency procedure.

Meeting the deadline will also require all the secondary legislation and other materials, including application decrees and specifications, to be ready at the date of enactment of the law. The interim ARJEL team members are therefore working hand in hand with various other bodies such as, *inter alia*, the Ministry of Economy, the ARPP and the French data protection authority (the CNIL) to ensure they are ready.

**Ethical standards for gambling advertising**

During a seminar on the future law on internet gambling in October, the President of the ARPP indicated that compliance with the Note of Guidance will be a vital part of any application for an online gambling licence with the ARJEL. This is the case even though ARPP is only a self-regulatory organisation and the Note of Guidance is unlikely to be a statutory obligation nor even an official specification. This statement was not contradicted by the proposed President of the ARJEL who was also present at the seminar (as were gambling regulators of several other countries and senator Trucy, who is also member of the French gambling commission).

Indeed, applicants under the new gambling law must provide guarantees and information on how they intend to comply with the technical, legal, financial and internal process specifications currently under preparation. This will include measures to fight against gambling addiction, protect children and, more generally, ensure corporate responsibility. An undertaking to comply with the ethical recommendations of the ARPP, by way of becoming one of its members, would fulfil one of the many requirements.

The June 2009 Note of Guidance is similar to the rules for gambling advertising of the UK Advertising Standards Authority.

This is only one piece of the jigsaw puzzle and obviously all players are waiting for the final version of the law, the decrees and the specifications.

The Note of Guidance is available on the ARPP’s internet site, here

*By Stéphanie Faber, Paris*
Telecoms

Poland - Telecoms Law Amended to Meet EU Requirements

The Polish telecommunication law was amended in July 2009 to bring it into line with the EU Common Regulatory Framework. A key reason for introducing these amendments was the pending infringement proceedings by the European Commission. As a direct result of the new law’s implementation, the Commission has closed three out of six cases against Poland in the telecom sector. A summary of the main changes is set out below.

"As a direct result of the new law’s implementation, the Commission has closed three out of six cases against Poland in the telecom sector."

Strengthening the independence of the Polish regulator

The new law reinstates earlier provisions specifying the duration of the chief regulator’s term in office and limiting the circumstances in which the chief regulator can be removed. These provisions had been removed in 2006 and the Polish Prime Minister’s unfettered power to dismiss the chief regulator was heavily criticized – especially as the regulator is in permanent dispute with the partly state owned incumbent operator.

The regulator’s powers have also been extended to cover the fulfilment of new obligations imposed on operators. Finally, the law introduces the right to appeal from the regulator’s decisions regarding a relevant market’s definition. The lack of effective appeal on this point has been questioned several times by the European Commission.

Pro-consumer changes

There are a number of significant pro-consumer amendments in the new laws. Prior to the amendments a customer was obliged to refund all the discounts granted at the date of signing a contract upon termination of that contract. This has been changed so that this obligation to refund discounts will be calculated on a pro rata basis, i.e. the longer the time span of the contract before termination, the smaller the discount to be paid back. Given that promotions based on discounts (e.g. subsidised handsets for long service contracts) were extremely common, the new law will be very popular with consumers.

Service providers are now obliged to inform customers in detail of any changes to the terms and conditions or tariffs and the customer has a right to terminate the contract without the payment if those changes are not acceptable. However, the right of free termination does not apply if:

- the adjustments were forced by legal or regulatory changes and were not proposed by the operator; or

- the changes in prices are favourable for customers.

Before the new amendments, customers had the right of termination without a penalty each time the operator changed the conditions of its services and adjusted the by-laws or contracts (even if they were favourable for customers). This made the operators very reluctant to introduce any changes and customers keen to use any such changes as a justification for an early withdrawal from obligations vis-à-vis operators.
Data retention

The amendments also implement the Data Retention Directive. Providers of publicly available telecommunications services are now obliged to keep customers' data for a period of 24 months (this covers such data as end users' ID and location, and the date, time and length of communication). The operators must protect the data and only make it available to authorised entities. The data retention obligation may also be fulfilled through a cooperation agreement with other operators or through an outsourcing contract with a third party outsourcer. Furthermore, the regulator will take over the data and keep them stored in the event of an operator's insolvency.

Overseas companies

Finally, EEA telecom companies wanting to provide their services in Poland without setting up a subsidiary under Polish law may now register themselves in the register of telecommunication entrepreneurs kept by the regulator, which is a prerequisite to providing telecommunications services in Poland. Until now, this was practically impossible because the documents that must be filed during the registration process required the prior establishment of a legal entity under Polish law.

By Magdalena Bartosik, Warsaw
Outsourcing

EU - Managing Contracts In Challenging Times

Good contract management is more important than ever in the current challenging economic market. Many organisations are taking a fresh look at their contracts and, in some cases, trying to exit or renegotiate them. Taking this sort of decisive action is fraught with risk if the contract has not been properly managed.

Linklaters therefore asked Pierre Audoin Consultants to survey senior contract managers from 50 top multi-national organisations to see how some of these issues are being addressed in practice.

Overall, the picture is very positive. Most of these organisations take a rigorous approach to contract management by investing in the contract management process, utilising change control procedures and keeping track of correspondence. However, in many cases there is still room for improvement. For example, of those surveyed:

- 6 per cent do not keep formal minutes of meetings;
- 12 per cent do not use a formal change control procedure;
- 22 per cent do not have any formal procedures for storing emails and other correspondence relating to a contract; and
- 26 per cent say there is little or no continuity between their contract negotiation team and contract management team.

However, these are the exception rather than the rule and, overall, the survey indicates an increasingly confident and professional approach to contract management. The full survey is available here

By Marly Didizian, London