## Contents

**EUROPE**
- Court of Justice finds that selective distribution agreements prohibiting the sale via internet unlawfully restrict competition and cannot benefit from a block exemption
- European Commission issues evaluation report on the Data Retention Directive
- Article 29 Working Party issues a working document on the EU personal data breach framework
- Article 29 Working Party issues opinion on the definition of consent

**BELGIUM**
- Constitutional Court rules on the lawfulness of the revised provisions for online gambling of the Gaming Act of 7 May 1999
- Court of Appeal of Antwerp finds that The Pirate Bay website must be blocked
- Court of Appeal of Brussels finds that unsolicited e-mails sent by a political party violate privacy law
- Court of First Instance of Nivelles acknowledges the enforceability of Creative Commons licenses under Belgian law
- Privacy Commission issues recommendation on smart grids and smart metering
- Privacy Commission and Ministry of Justice conclude protocol simplifying the authorization procedure for binding corporate rules

**THE NETHERLANDS**
- Supreme Court interprets Dutch Privacy Act in accordance with Article 8 ECHR
- Court of Appeal of Leeuwarden finds that the registration of one’s general practitioner is allowed
- Court of Appeal of the Hague upholds exoneration clause KPN
- District Court of Leeuwarden finds that a new award decision entails a new Alcatel deadline
- District Court of Almelo finds that even in case of a resolution time in service level agreements a notice of default can be required
- District Court of Amsterdam finds that a bank is liable for investment losses due to a TradeBox system breakdown
- Dutch government revokes security certificates from its sole provider
- Dutch Security and Justice Minister addresses Parliamentary questions regarding American companies having access to European cloud data under the US Patriot Act
- Cookie icons appear in advertisements
- National Prosecutor’s Office finds that KPN’s use of Deep Packet Investigation is not a criminal offence

**LUXEMBOURG**
- Legislator implements ePrivacy Directive
EUROPE

EU - Court of Justice finds that selective distribution agreements prohibiting the sale via internet unlawfully restrict competition and cannot benefit from a block exemption

In a judgment of 13 October 2011, the European Court of Justice (ECJ) ruled on the lawfulness of a clause in selective distribution agreements prohibiting distributors from selling the products via the internet.

Pierre Fabre Dermo-Cosmétique is a member of the Pierre Fabre Group which manufactures and markets cosmetics and personal care products and has several subsidiaries, such as the Klorane, Ducray, Galénic and Avène laboratories. Their cosmetic and personal care products are sold mainly through pharmacists on the markets of France and other EU Member States. The products in question are not classified as medicines and are, therefore, not covered by the pharmacists’ monopoly laid down by French law. However, distributions agreements provide that the products may be sold only in a physical space and in the presence of a qualified pharmacist. All forms of selling via the internet are thus prohibited.

In October 2008, following an investigation, the French Competition Authority decided that, because of the de facto ban on all internet sales, the distribution agreements amounted to anti-competitive agreements contrary to both French law and European Union competition law. The Competition Authority found that the ban on internet selling necessarily had as its object the restriction of competition and could not benefit from a block exemption. However, a selective distribution system is compatible with EU competition law if distributors are chosen on the basis of objective criteria of a qualitative nature, laid down uniformly for all potential distributors and not applied in a discriminatory fashion. Furthermore, the characteristics of the product in question must necessitate such a distribution network in order to preserve the product’s quality and ensure its proper use. Finally, the criteria laid down may not go beyond what is necessary.

First, the ECJ repeated its earlier case law that selective distribution agreements necessarily affect competition and that, if there is no objective justification, these are to be considered restrictions “by object”. However, a selective distribution system is compatible with EU competition law if distributors are chosen on the basis of objective criteria of a qualitative nature, laid down uniformly for all potential distributors and not applied in a discriminatory fashion. Similarly, the ECJ now found that the need to maintain the prestigious image of Pierre Fabre’s products is not a legitimate aim for restricting competition.

Second, the ECJ recalled that block exemptions do not apply to vertical agreements which have as their object the restriction of active or passive sales to end-users by members of a selective distribution system operating at the retail level of trade. According to the ECJ, a contractual clause which de facto prohibits the internet as a
method of marketing at the very least has as its object the restriction of passive sales to end-users wishing to purchase online and located outside the physical trading area of the relevant member of the selective distribution system. The ECU consequently found that the block exemption does not apply to that contract.

Third, the ECJ found that such a contract may, however, benefit from an individual exemption. It is, however, up to the national courts to examine whether the conditions for an individual exemption set forth in Article 101(3) TFEU are met. (FDE)

The case can be found on http://curia.europa.eu, case No. C-439/09

EU – European Commission issues evaluation report on the Data Retention Directive

On 18 April 2011, the European Commission issued a report in which it evaluates Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (the “Data Retention Directive”). This Directive requires providers of publicly available electronic communications services and of publicly available telecommunications networks (the “Providers”) to retain communications traffic data and location data for a period between six months and two years. The Data Retention Directive, which allows law enforcement agencies to use communications traffic data for the prosecution of serious crimes, was enacted following a vigorous debate among privacy advocates, telecom operators and law enforcement agencies. As a result of this debate, the European legislator provided that the impact of the Data Retention Directive had to be evaluated by 15 September 2010. In this evaluation report, the European Commission concluded that there are some substantial inadequacies in the Data Retention Directive. According to the European Commission, one of the most important inadequacies of the Data Retention Directive is that it provides for ambiguous wording on certain crucial provisions of the directive. As an example, the European Commission states that the notion “serious crimes” as used in Article 1 of the Directive is not sufficiently defined. Due to this ambiguity, some Member States allow the use of retained communications traffic data for the investigation and prosecution of almost all criminal offences, whereas other Member States only allow data retention for the prosecution of a limited number of crimes. The evaluation report also addresses the financial aspects of data retention. According to the European Commission, the obligation to retain communications traffic data represents a substantial cost to Providers. Since the Data Retention Directive does not provide for a regime relating to the allocation of the costs of data retention, some Member States provide that Providers will be reimbursed for the retention of communications traffic data whereas other Member States do not provide for such a regime. Given that these differences in national reimbursement schemes might adversely affect some smaller Providers, the European Commission will consider ways of providing consistent reimbursement schemes that are applicable to all Providers.

As a general conclusion, the European Commission concludes that the Data Retention Directive failed to generate a harmonized approach towards data retention in the European Union. In order to create such a harmonized approach, the European Commission proposes to revise the current data retention framework. In its evaluation report, the Commission proposes to revise the Data Retention Directive on the basis of the following criteria:

• the purpose for which data retention can be used must be clearly defined in the revised directive;
• the periods during which the data is to be retained must be shortened and harmonized; and
• the revised directive must clearly specify which law enforcement agencies are entitled to have access to retained communications traffic data.

Prior to enacting a revised Data Retention Directive, the European Commission will consult all relevant stakeholders including law enforcement agencies, privacy advocates and the telecommunications sector. On the basis of its findings, the European Commission will
draft an impact assessment on data retention, which will be used as a basis for the revised Data Retention Directive. (LDA)


EU – Article 29 Working Party issues a working document on the EU personal data breach framework

On 5 April 2011, the Article 29 Working Party issued a working document in which it reviewed the manner in which the different Member States have transposed the data breach provisions of Directive 2009/136 of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the “ePrivacy Directive”).

The ePrivacy Directive provides that Member States should oblige providers of publicly available electronic communications services (i.e. internet service providers) to notify the authorities and the individuals concerned if a breach of security leads to the accidental or unlawful disclosure or access to personal data of such individuals (also known as a data breach).

Although the ePrivacy Directive had to be transposed into national law by 25 May 2011, the Article 29 Working Party concludes that currently not a single Member State has transposed the ePrivacy Directive. According to the Working Party, the delay in the transposition of the ePrivacy Directive in the different Member States mainly results from a lack of awareness of this subject-matter in some Member States. In order to adequately address this issue, the Article 29 Working Party proposes to establish a sub-group which raises awareness regarding data breach notifications by exchanging knowledge between the different Member States and by developing harmonized procedures on this matter. In addition, the Article 29 Working Party also proposes that the sub-group will coordinate the data breach notifications procedures in case of cross-border data breaches.

In addition, the Article 29 Working Party also welcomes the European Commission’s initiative to extend the scope of the data breach notification obligation. This initiative implies that the obligation on the data breach notification, which currently only applies to providers of publicly available electronic communications services, will be made applicable to all data controllers. (LDA)


EU – Article 29 Working Party issues opinion on the definition of consent

On 13 July 2011 the Article 29 Working Party issued an opinion on the concept of consent in the Data Protection Directive (the “Privacy Directive”) and in the e-Privacy Directive. The opinion is issued in response to a request from the European Commission as part of the ongoing review of the Privacy Directive. It provides a thorough analysis of the key elements of the definition of consent and clarifies the various aspects of the legal framework to ensure an easier application and understanding of the concept for all stakeholders involved.

Consent of a data subject is one of the six grounds which allows for legitimate processing of personal data. Consent, if adequately given, allows the data subject to fully control the processing of his personal data. However, the Article 29 Working Party notes that consent data does not provide a controller with a carte blanche to process the data, and the controller will still have to comply with all other requirements of the Privacy Directive.
The Privacy Directive defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." In addition, consent has to be "unambiguous" and "explicit" for special categories of data. For each of these elements, the opinion provides numerous examples of valid and invalid consent. In addition, the Working Party provides that, in an online context, consent can never be validly based on an individual's lack of action or silence. Moreover, the Working Party specifies when consent is considered to be valid if the data subject is underage or lacks legal capacity.

In light of the European Commission’s request, the opinion also contains some recommendations for the review of the Privacy Directive. As such, the Article 29 Working Party recommends to:

• clarify the meaning of "unambiguous" consent and explain that only consent based on statements or actions to signify agreement can constitute valid consent;
• require data controllers to put in place mechanisms to prove consent (in the context of a general accountability obligation);
• include an explicit requirement regarding the quality and accessibility of the information on which consent is based. (LCE and CLI)

The full text of the opinion of the WP 29 can be found on its website: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

BELGIUM

BE – Constitutional Court rules on the lawfulness of the revised provisions for online gambling of the Gaming Act of 7 May 1999

On 14 July 2011, the Constitutional Court issued a judgment in which it decided that the revised rules for operating online gambling services in Belgium are non-discriminatory and do not violate the European principle of free movement of services. The revised Gaming Act (the “Act”) intends to modernize the Belgian gambling and betting legislation. The Act was promulgated on 10 January 2010 and entered into force on 1 January 2011. In light of this modernization, the scope of the Act was expanded to sports betting, online gambling and betting, and media games. The new rules provoked an elaborate debate on the lawfulness of the new provisions. Where before 1 January 2011 all online gambling and betting was forbidden, the Act now partly allows it under strict requirements:

• the operator of online gambling services must hold a license for a casino, a gaming arcade or a betting service in Belgium (“land-based”); and
• his servers are permanently located in a permanent establishment in Belgium.

Telebet NV, Betfair International and the Remote Gambling Association challenged the lawfulness of these new provisions before the Constitutional Court. They argued that the new provisions of the Act violated the constitutional principle of non-discrimination by creating an unreasonable discrepancy between online and land-based gaming service providers. They claimed that this discrepancy emerged because the new provisions of the Act constituted a non-permitted deviation from the European principle of non-discrimination by creating an unreasonable discrepancy between online and land-based gaming service providers. They claimed that this discrepancy emerged because the new provisions of the Act constituted a non-permitted deviation from the European principle of non-discrimination as laid down in Article 56 of the Treaty on the Functioning of the European Union.

In its judgment, the Constitutional Court found that the new provisions did indeed constitute a restriction of the free movement of services. However, the Court underlined that Member States are allowed to introduce restrictions on the exploitation of gaming services if (1) this is necessary for reasons of
In its decision, the Court followed the reasoning of the preparatory acts of the Act which provide that a strict control of gambling services is necessary to combat the negative consequences of betting and gambling. In light thereof, the legislator opted for a “solution of canalization” which means that (i) only a few betting and gambling service providers are allowed to legally operate on the Belgian market, and (ii) all other gambling and betting activities are forbidden. To optimize the supervision capacities on online gambling of the Gaming Commission, the legislator implemented a land-based license scheme for online gambling. The Court concluded that the new provisions of the Gaming Act are thus both necessary and proportional. In addition, the Court concluded that the consequences of the new provisions are reasonable and do not cause any discrimination between online and land-based gaming service providers. 

The case can be found on http://www.juridat.be

On 3 October 2011, the Court of Appeal of Antwerp issued a judgment in cease-and-desist proceedings between a non-profit association established by Belgian video manufacturers, the Belgian Anti-Piracy Federation (“BAF”), and the internet service providers Telenet and Belgacom. BAF based its claim on Article 87 §1, par. 2 of the Copyright Act which provides that a court can issue a cease-and-desist order against internet intermediaries if its services are used by third parties for actions in violation of copyright.

The Court of Appeal rescinded the decision of the Court of First Instance of July 2010 (see our ICT Law Newsletter No. 39 of November 2010) which found that immediate interim measures to block the website The Pirate Bay were not strictly necessary and that BAF’s claim was disproportionate, especially since the website has been active for many years without the BAF having initiated any legal proceedings in the past.

First, contrary to the opinion of Belgacom and Telenet, the Court of Appeal found that there was no need to defer the judgment until the European Court of Justice would rule on the question whether a measure ordering an internet service provider to install a system for filtering and blocking electronic communications in order to protect intellectual property rights infringes fundamental rights (see our ICT Law Newsletters No. 37 of March 2010 on the Scarlet case and No. 39 of November 2010 on the Netlog case) since in this case BAF only requested the Court to order removal of the website The Pirate Bay.

In addition, Belgacom and Telenet argued that a cease-and-desist order would impose a general monitoring obligation, whereas, according to Article 21 §1 of the Belgian E-Commerce Act, such obligation is prohibited. The Court of Appeal, however, considered that a duty that could be fulfilled by a one-off technical change, such as to disable routing of a particular Internet Protocol address, does not involve monitoring. In the current case, the Court of Appeal has ordered Belgacom and Telenet to implement, under penalty of a daily fine of EUR 1,000 within 14 days after the notification of the judgment, a Domain Name System (DNS) blocking measure, i.e. changing the ISP service that translates domain names (e.g. www.example.com) into IP addresses (e.g. 192.0.32.10). At the same time, the Court acknowledged that circumvention is technically possible but in this particular case Belgacom and Telenet will not be held liable for any users who would circumvent this technique. 

The case can be found on http://www.juridat.be
BE – Court of Appeal of Brussels finds that unsolicited e-mails sent by a political party violate privacy law

In a recently published judgment of 17 March 2010, the Court of Appeal of Brussels condemned a political party for illegal processing of personal data without the data subject's consent. This case concerned the political party's sending of e-mails to someone who did not give his consent to such processing. The Court found that the political party did not demonstrate having obtained such consent. Hence, the political party was held to have committed a criminal offence and was condemned to pay a fine of EUR 550, while the Court awarded EUR 1 to the civil party. The Court also ordered the publication of that judgment in three national newspapers at the choice of the individual, but at the political party's expense.

In addition, the Court found that, even though the data subject radically disapproved of the opinions of the political party, sending unsolicited e-mails could not be considered as “critically” threatening the peace of mind of that particular data subject, as prohibited by Article 442bis of the Belgian Criminal Code which provides for a punishment on harassment caused to a person. Also, there was no violation of Article 14 of the E-commerce Act which prohibits the use of e-mails for marketing purposes without the prior, free, specific and informed consent of the addressee since a political party does not pursue a commercial, industrial or craft activity nor does it exercise a regulated profession as required by Article 2 of the E-commerce Act defining marketing. (NRO)

The case can be found on http://www.juridat.be

BE – Court of First Instance of Nivelles acknowledges the enforceability of Creative Commons licenses under Belgian law

On 26 October 2010, the Court of First Instance of Nivelles issued a judgment regarding Creative Commons licenses, acknowledging their enforceability under Belgian law.

Creative Commons licenses constitute a set of copyright licenses intended to expand the range of creative works available in the public domain. Creative Commons licenses offer an alternative to the traditional "all rights reserved licenses" by creating a more flexible copyright model with “some rights reserved”. Creative Commons licenses allow creators to distribute their content under a pre-defined license framework and all licensees may use the works in a flexible manner without being required to contact the author first. There are four major types of Creative Commons licenses which the author can select:

- attribution (“BY”): author's name has to be mentioned;
- share alike (“SA”): derivative works can only be distributed under the same or a similar license;
- non-commercial (“NC”): restriction of distribution to non-commercial purposes;
- no derivative works (“ND”): restriction of distribution to the original work.

In this case, a Belgian band, unaffiliated to the Belgian Society of Authors SABAM, uploaded songs on a freely accessible music website under a Creative Commons license “BY-NC-ND”. A Belgian theater company used one of its songs as background music in an advertisement broadcasted on several national radio channels. According to the band members, all three license conditions were violated by the theatre company as the band’s authorship was never mentioned, the song was used to serve a commercial purpose and the use of the song as background music is to be considered as a derivative work. Therefore, the band sought indemnification in court and requested the publication of the judgment in a specialized magazine.

By referring to a judgment of 9 March 2006 from the District Court of Amsterdam recognizing the validity of Creative Commons licenses in the Netherlands, the Court confirmed the enforceability of this type of licenses in Belgium too. Failure to comply with the terms of Creative Commons licenses can, according to the Court, lead to the payment of damages for each of the violated provisions.

On the amount of the indemnification, the judge stated that, in principle, the authors have a right to compensation of their prejudice irrespective of the fact that their work has been distributed under a free license. Nevertheless, the Court ruled
that artists who have chosen in favor of a non-commercial regime such as Creative Commons licenses cannot claim a higher financial indemnity than the usual rates as applied by SABAM. Finally, the Court did not order the publication of the judgment in the absence of any damage to the band’s reputation.

Consequently, further to this judgment, it appears that the creators who opted for the Creative Commons licenses regime can assert their rights in Belgian courts and obtain compensation in case of violation of such licenses. (SCO and TLE)

The case can be found on http://www.juridat.be

BE – Privacy Commission issues recommendation on smart grids and smart metering

On 15 June 2011 the Privacy Commission published a recommendation on smart grids and smart metering and the legal principles that have to be complied with in this respect.

This recommendation closely follows opinion 12/2011 of the Article 29 Working party on smart metering adopted on April 4, 2011.

A “smart grid” is an intelligent supply network for the energy and water industry, which processes detailed information of consumers. A “smart meter” is a part of this grid and ensures a bidirectional real-time communication over a network. Smart meters allow amongst others to remotely read the meter and to provide detailed information about the energy consumption of consumers.

In the EU, the implementation of smart meters is strongly encouraged: Directive 2006/32 of 5 April 2006 on energy end-use efficiency and energy services takes steps to achieve energy saving and efficiency, including more accurate metering techniques.

However, the implementation of smart meters raises several questions on the protection of privacy because this technology allows a far reaching view on the activities of a household. Therefore, the Privacy Commission states that it is of utmost importance that all involved actors (regulators, distribution service operators, energy suppliers and service suppliers) carry out a social cost-benefit analysis for each target group. This analysis should take into account the impact on privacy in the long run, and should list all basic modalities, scenarios and privacy risks concerning smart metering before any legislation concerning smart metering is elaborated.

The Commission also provides recommendations on how to comply with these privacy principles when drafting new legislation on smart meters. For example, the Commission proposes to apply a “double green light” mechanism to establish sufficient legitimacy before the data can be processed. The processing of the data will thus depend on both the prior agreement of the data supplier concerned (e.g. the energy supplier concerned) and the independent government service, which has to verify if the concerned data manager and the data processor comply with the data protection legislation.

In addition, the Commission highlights the importance of transparency: neutral, thorough and clear information will give the data subject confidence and will enable him to make an informed decision about whether or not he wants to release his personal data. (LCE and CLI)

The opinion can be found on http://www.privacycommission.be

BE – Privacy Commission and Ministry of Justice conclude protocol simplifying the authorization procedure for binding corporate rules

Binding corporate rules (“BCRs”) are internal codes of conduct drafted for use in multinational companies which cover the international transfer of personal data within their corporate group in order to
ensure an adequate level of data protection. Once signed by all entities of the group and approved by the various national data authorities involved in the (flow) stream, the BCR have to be observed by all entities and employees. In Belgium, the authorization process can only be considered final when a Royal Decree of approval has been issued by the federal Government.

On 13 July 2011, the Belgian Privacy Commission signed a Protocol with the Ministry of Justice to streamline the authorization procedure for such internally binding compliance measures under Belgian law. The Protocol contains (1) the minimum requirements for the BCR; (2) the new procedure for approval that has been agreed upon by the Commission and the Ministry of Justice; (3) an explanatory note; and (4) a pre-approved standardized template for the Royal Decree of approval.

In practice, the most significant improvements are:

- the strict term of 60 days within which the Commission has to issue its advice to the Ministry of Justice after all documents have been collected and the file can be considered as complete;
- the automatic approval of the BCR by the Ministry of Justice if the Commission’s advice is favourable. As approval, the Minister of Justice will sign the Royal Decree of approval which will be published in the Official Gazette. As a template is used, the individual Royal Decrees do not require prior review by the Finance Inspection and the Belgian Council of State. (NRO)

The Protocol can be found on www.privacycommission.be

---

**THE NETHERLANDS**

**NL – Supreme Court interprets Dutch Privacy Act in accordance with Article 8 ECHR**

In a judgment of 9 September 2011, the Dutch Supreme Court confirmed an appellate decision of the Court of Appeals Arnhem concerning the reporting of a minor default payment by a bank to the national registry of debtors (“Bureau Kredietregistratie” or “BKR”).

In this matter, the claimant had ignored minor invoices on a loan. Its lender, Santander Consumer Finance Benelux B.V., collected the outstanding invoices and reported the claimant as a defaulter to the BKR. The claimant wanted to be removed from the registry and contended that Santander breached the provisions of the Data Protection Act (“DPA”) when it registered the claimant in the first place.

Santander argued that it did not need to perform any type of test on the necessity of registering the claimant as a defaulter, since the claimant had given his prior consent to the processing of his personal data by Santander in accordance with Santander’s privacy policy.

According to the Supreme Court, a request by a data subject to be removed from a registry must be interpreted in accordance with the right to privacy set forth in Article 8 of the European Convention on Human Rights. Consequently, any type of processing of personal data should not be disproportionate in comparison to the aim of such processing. The Supreme Court confirmed the need for the controller to perform a proportionality and subsidiarity test under specific circumstances in all instances. The fact that there would be a legal requirement to process the data (in this case, report them to the BKR), provided insufficient justification according to the Supreme Court. Moreover, in the event the data subject would inform the controller that it had not sufficiently considered the interests of the data subject, then the controller should still make such consideration based on the then current facts and circumstances. (SG)

This case can be found on http://zoeken.rechtspraak.nl, LJN=BQ8097

---

*Stibbe* ICT Law Newsletter No. 42 – November 2011
In its judgment of 12 July 2011, the Court of Appeal of Leeuwarden found that the registration of one’s general practitioner is allowed.

In its judgment of 12 July 2011, the Court of Appeal of Leeuwarden found that the Foundation for Name Registration (“Stichting Inschrijving op Naam” or “ION”) was not required by law to remove the claimant’s personal data registration that contained the name and address of her physician.

In the Netherlands, the ION registers the name and address of Dutch citizens’ physicians. This practice was introduced by the new Health Insurance Act in 2006. ION’s data registration of Dutch citizens’ physicians can be accessed by health insurance companies and general practitioners, and the main purpose of said data register is the prevention of double entries (and payments).

In this case, a citizen objected against her registration with ION. The Leeuwarden’s Court of Appeal dismissed the Dutch citizen’s arguments. According to the Court, the processing by ION was required in light of the fact that ION had a legitimate interest to process the data, because it was prescribed by law to manage these data. After having performed a proportionality and subsidiarity test required pursuant to the DPA, the Court ruled in favor of ION. The Court reached this outcome in view of the limited sensitivity of having one’s general practitioner registered, vis-à-vis the legitimate interest of ION for registering these data.

This case can be found on http://zoeken.rechtspraak.nl, lJN=Br5585.
acknowledged KPN’s interest to make use of exoneration provisions in general and also takes into consideration that the delay in this particular case had not been material. Given the fact that the exoneration clause was fully applicable, the question whether KPN was in default in the first place did not have to be addressed, and, even if it were to be addressed, KPN would still not be liable on the basis of the exoneration clause. (CvM)

This case can be found on http://zoeken.rechtspraak.nl, lJN=BQ7876

**NL – District Court of The Hague finds that a new award decision entails a new Alcatel deadline**

In a recently published judgment of 1 June 2011, the District Court of The Hague found that contracting party HTM Personenvervoer N.V. (a public transport company for the The Hague region) had insufficiently justified their procurement award decision and that it would be unreasonable if a new award decision would be issued without a new ‘Alcatel deadline.’ The ‘Alcatel deadline’ is a mandatory 15 day stand-still period introduced by the Court of Justice of the European Union (ECJ) in its ‘Alcatel judgment’ (C-81/89) of 1999 which enables third parties to request nullification of an award decision before the decision is made final. After the ‘Alcatel judgment’, this stand-still period was laid down in the Public Procurement Decree and the Public Procurement Decree for special sectors. The latter Decree is applicable in this case.

The claimant in the interlocutory proceedings was the unsuccessful tenderer Construcciones y Auxiliar de Ferrocarriles S.A. (“CAF”). CAF raised objections to the transparency of the award criteria and the justification of the award decision. The contracting party HTM had announced the award criteria and the subcriteria, but had failed to disclose the related assessment factors. Instead, the assessment factors had remained in the custody of a civil-law notary. Despite CAF’s request, HTM had refused to disclose the assessment factors. Furthermore, CAF argued that HTM had modified the award criteria upon announcement.

In its judgment, the Court ruled that HTM should re-assess the tenders of the tenderers based on the initially announced award criteria. First, it held that securing objectivity by depositing information at a civil-law notary was insufficient, because it did not result in transparency, in such a way that it allowed tenderers to take the assessment factors into account when drawing up their tenders. Second, it held that it was not allowed to make interim changes to the award criteria and the assessment criteria after they were announced.

The subsequent renewed award decision required a new 15 days stand-still period. (FF)

This case can be found on http://zoeken.rechtspraak.nl, lJN=BQ6916

**NL – District Court of Alkmaar holds that even in case of a resolution time in service level agreements a notice of default can be required**

On 3 August 2011, the District Court of Alkmaar rendered a judgment on contractually agreed resolution times in a so-called service level agreement (“SLA”). A resolution time is the period of time, following a notification of a breakdown or defect in the software, within which the problem has to be solved. This means that there is an obligation for the supplier to achieve a result within this period. By failing to do so the supplier will automatically be in default, unless he can prove that the failure to meet the resolution time is not his fault. In principle, there is no obligation to send a notice of default in case there is a violation of a resolution time or a result obligation. As a result, damages can be claimed immediately.

This case focused on the question whether the following clause had to be considered a resolution time/result obligation: “Within 48 hours of a report of a breakdown, Fleetlogic will provide on-site services, unless a later date is agreed upon in writing.”

The Court held that this clause did not establish an obligation to achieve a result; this clause concerned providing services and, according to the Court, did not extend to a period of time within which the problems had to be solved. Consequently, the clause had to be considered a best efforts obligation. In this case, the Court found that a notice of default was required.
Furthermore, the Court stated that, even if this clause was considered an obligation of result, a notice of default could be required because it concerned a continuous maintenance obligation by Fleetlogic for several systems with different customers. As such, according to the Court, even if parties have agreed on resolution times and result obligations in service level agreements, a notice of default can be required in order to claim penalties or damages. (SG)

This case can be found on http://zoeken.rechtspraak.nl, LJN=Br4997

**NL – District Court of Amsterdam finds that a bank is liable for investment losses due to a TradeBox system breakdown**

On 13 April 2011, the District Court of Amsterdam held the ABN AMRO bank liable for investment losses due to a breakdown in one of the bank’s systems.

In the events leading to this case, a blockade occurred in the TradeBox system of ABN AMRO. As a consequence, one of its clients could not trade stock options for a significant period of time.

The Court found that ABN AMRO could not invoke the applicability of its general terms and conditions – which contained a disclaimer of liability. As a result, the client could successfully invoke the nullification of the general terms and conditions including the limitation of liability section.

According to the Civil Code, general terms and conditions should be made available to the other party electronically, before or upon conclusion of the contract. In addition, the party claiming applicability should ensure that the general terms and conditions can be saved by the other party on a data carrier.

The court held ABN AMRO liable for the client’s damages. (ND)

This case can be found on http://zoeken.rechtspraak.nl, LJN=BQ7598

**NL – Dutch government revokes security certificates from its sole provider**

In August 2011, DigiNotar, a company issuing SSL (secure socket layer) certificates for numerous websites operated by the Government, admitted that hackers had illegally obtained such certificates.

These SSL certificates are used as a qualified electronic signature within the meaning of the Electronic Signatures Directive to authenticate the person using this certificate. The hack extended to the google.com domain. It was established that Gmail accounts of Iranian citizens had been hacked. DigiNotar confirmed that it had first discovered the security breach on July 19. However, DigiNotar had not informed the Government immediately. The Government then launched an investigation which revealed that the hacker(s) by-passed DigiNotar’s servers in mid-June and made off with more than 500 certificates.

On September 13 2011, the Independent Post and Telecommunications Authority (“OPTA”) revoked the registration of DigiNotar as a supplier of the certificates for qualified electronic signatures. In addition, OPTA decided that DigiNotar should repeal all issued certificates within two weeks. Since the Government had only been using DigiNotar-supplied certificates, the cancellation of DigiNotar’s registration effectively leaves all websites of the Government with invalid certificates until a new supplier of certificates can be found.

The Minister of the Interior has recommended citizens not to access governmental websites if a warning about an invalid certificate appears.

DigiNotar filed for bankruptcy on 19 September, and its assets will be liquidated by a court-appointed trustee. (SG/FF)

The publication can be found on http://www.opta.nl
NL – Dutch Security and Justice Minister addresses Parliamentary questions regarding American companies having access to European cloud data under the US Patriot Act

In a recent interview, Microsoft’s UK manager admitted that cloud data worldwide do not fall outside the reach of the US Patriot Act. Consequently, Microsoft will, upon request, hand cloud data it processes over to US Authorities. Although Microsoft will inform customers wherever possible, it does not provide any guarantee. In short, US authorities may intercept and inspect any data which is stored, housed or processed either by US based companies or by companies wholly owned by a US parent company. Following Microsoft’s admission, questions were raised in the Parliament.

According to the Dutch Security and Justice Minister (the “Minister”), the conflict of duties arising as a result of the extra-territorial application of US legislation is not limited to the Netherlands, but equally affects all EU member states. Therefore, it is up to the European Commission to reach an agreement with the American authorities.

In the Netherlands, no policy has been developed yet which aims at responding to the possible undesirable extra-territorial application of foreign legislation. The Minister of the Interior has announced he is investigating the possibilities. In order to avoid that governmental data (i.a. of civilians) could be retrieved by the USA under the US Patriot Act, the Minister proposes to include a requirement to the schedule of requirements in procurements stating that the supplier is under no circumstance allowed to transfer governmental data (also on civilians) to any foreign legal body. As a result, US companies could be excluded from such tenders and assignments. (FF)

The Parliamentary questions can be found on: https://zoek.officielebekendmakingen.nl

NL – National Prosecutor’s Office finds that KPN’s use of Deep Packet Investigation is not a criminal offence

In May 2011, KPN admitted to its use of Deep Packet Inspection (DPI). With this controversial technique, KPN is not only able to analyze the types of data transmitted between sender and recipient, but also the content of such data. KPN argued it needed to engage DPI in order to quantify charges for popular applications like ‘Skype’ and ‘WhatsApp’, which skim off telecom providers’ income on traditional data traffic. DPI is controversial because it may violate the Personal Data Protection Act (“DPA”). In addition, intercepting telecommunication

Third party cookies are being used to adapt advertisements to the surfing behaviour of the visitor. This is called “online behavioral advertising” or “retargeting”. According to a decision of the House of Representatives, unambiguous consent from internet users is required for this type of advertising.

Since 30 August 2011, cookie icons have appeared in many online advertisements in the Netherlands. If a user clicks on these icons, the user will enter a register where he can indicate from which parties he would or would not like to receive third party cookies. Several European countries have been working with this system.

The cookie icon is a form of self-regulation by big internet operators such as Google, Microsoft, Sanoma Media, De Persgroep, Telegraaf Media Nederland and RTL. According to IAB Nederland, these operators represent 75 percent of the total internet coverage. IAB Nederland emphasises that this self-regulation, in particular the possibility to opt-out, is not a substitute for the law, but must be seen as a supplement. (SG/ND)
messages is considered a criminal offence within the meaning of the Criminal Code. After the disclosure by KPN, several Parliamentary questions were raised. The State Secretary for Public Order and Safety explained that the legitimacy of DPI depends on the way the technique is applied, the intended purpose and the sort of data obtained. The State Secretary also announced that the National Public Prosecutors’ Office and the Independent Post and Telecommunications Authority (“OPTA”) were conducting an investigation into this activity.

The National Public Prosecutors’ Office recently stated that the DPI-usage of KPN cannot be deemed a criminal offence, since the findings did not indicate in any way that KPN was intercepting telecommunication content. KPN’s data is not stored comprehensively and therefore it cannot gain insight into the specific content of the data between sender and recipient.

OPTA on the other hand concluded that KPN as well as other operators (T-Mobile, Vodafone and Tele-2) are possibly breaching the secrecy of communications. The Dutch Data Protection Authority is investigating this. The results of this investigation will decide if measures will be taken against the operators further.

KPN and several other operators have stated that they will continue to use DPI as long as this is permitted. (SG)

**LUXEMBOURG**

**LUX – Legislator implements ePrivacy Directive**


First, the scope of the Act has been extended and the Act now also addresses communication services to the public such as RFID chips. In addition, where the former act of 2005 only required prior consent of a person in case he or she is the target of unsolicited calls via automatic call mechanisms, the Act now also requires prior consent of a subject in case SMS or MMS is used. This shows the legislator’s attempt to neutralise the concept “communication” and to extend it to currently unknown forms of communication. Violation of this provision may lead to criminal sanctions and/or an injunction to cease the prohibited processing of data with a penalty payment.

In addition, communication service providers have the legal obligation to contact the Luxembourgish National Data Protection Commission (the “Commission”) if there is a security breach relating to the confidentiality of personal data. Communication service providers are also obliged to inform their customers when they become aware of such a potential risk. The Act defines a violation of personal data as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure or unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of electronic communications services to the public”.

According to the ePrivacy Directive and the Commission, this definition aims at “breakdowns”, e.g. when an employee of a telecom service provider losing a CD-ROM or a USB key with client data or if some
people have access to personal data that are normally only accessible with a password. If such a breach of security occurs, the service provider must notify the Commission and the customer whose personal data have been affected if the violation is likely to have a negative impact on the customer's personal data. However, this notification is not legally required if the service provider can guarantee that sufficient protection technologies have been set up and that such technologies have been applied to the data affected by the breach. The Commission may also issue an injunction against the service provider if it is of the opinion that the breach is likely to have negative effects on the personal data of the consumer. Furthermore, the Act provides for an obligation for all Luxembourgish service providers to maintain a register listing all breaches of personal data, elaborating on the context, the effects and the measures that were taken.

The CNPD may also impose fines which are equal to criminal sanctions even though they are not imposed by a judicial authority. (NVH)
Contributors to this issue of the ICT Law Newsletter: Lien Ceulemans, Sofie Costermans, Laurens Dauwe, Frederic Debuissère, Niels Douma, Frédéric François, Serge Gijrath, Lore Leitner, Thomas Lewaite, Cédric Lindenmann, Nicolas Roland, Christien Saris, Erik Valgaeren and Nicolas van Heule.

For more information
If you require further copies of this newsletter, or advice on any of the matters raised in it, please contact:

Erik Valgaeren, T +32 2 533 53 51, F +32 2 533 51 15, erik.valgaeren@stibbe.com
Serge Gijrath, T +31 20 546 02 12, F +31 20 546 08 11, serge.gijrath@stibbe.com

Amsterdam
Strawinskylaan 2001
P.O. Box 75640
1070 AP Amsterdam
The Netherlands
T +31 20 546 08 06
F +31 20 546 01 23
info@stibbe.nl

Brussels
Central Plaza
Loksumstraat 25 rue de Luxum
1000 Brussels
Belgium
T +32 2 533 52 11
F +32 2 533 52 12
info@stibbe.be

London
Exchange House
Primrose Street
London EC2A 2ST
United Kingdom
T +44 20 7466 63 00
F +44 20 7466 63 11
info@stibbe.co.uk

Dubai
Gate Village 7 Level 4
P.O. Box 566531
Dubai UAE
T +971 4 428 63 13
F +971 4 965 31 71
info@stibbe.ae

Strawinskylaan 2001
P.O. Box 75640
1070 AP Amsterdam
The Netherlands
T +31 20 546 08 06
F +31 20 546 01 23
info@stibbe.nl

The ICT Law Newsletter is also available on our website www.stibbe.com

All rights reserved. Care has been taken to ensure that the content of this newsletter is as accurate as possible. However the accuracy and completeness of the information in this newsletter, largely based upon third party sources, cannot be guaranteed. The materials contained in this newsletter have been prepared and provided by Stibbe for information proposes only. They do not constitute legal or other professional advice and readers should not act upon the information contained in this newsletter without consulting legal counsel. Consultation of this newsletter will not create an attorney-client relationship between Stibbe and the reader. The newsletter may be used only for personal use and all other uses are prohibited.

Stibbe, Herbert Smith LLP and Gleiss Lutz are three independent firms which have a formal alliance.

© Stibbe 2011 Publisher: Erik Valgaeren, Stibbe, Central Plaza, Loksumstraat 25 rue de Luxum - BE-1000 Brussels