Contents

EUROPE

• EU – ECJ finds that an author of software cannot oppose the resale of his ‘used’ licenses 2
• EU – ECJ finds that the functionalities of a computer program and the programming language are not copyright-protected 2
• EU – ECJ provides clarification on jurisdictional issues relating to infringements of personality rights on the Internet 3
• EU – Article 29 Working Party adopts opinion on cookie consent exemption 3
• EU – Article 29 Working Party adopts opinion on cloud computing 4
• EU – European Commission launches new cloud computing strategy 4

BELGIUM

• BE – New Cookie Act 5
• BE – The Court of Cassation finds that the principles governing employees’ rights in case of transfer of undertakings also apply in case of insourcing 5
• BE – Labour Court of Leuven finds that there is no violation of an employee’s right to privacy if the employer obtains certain information from the employee’s Facebook profile 5
• BE – Privacy Commission adopts recommendation on surveillance at the workplace 6

THE NETHERLANDS

• NL – Amendments to Exemption Decree DDPA, Costs Decree and Notification Decree enter into force 6
• NL – Revised Telecommunications Act enters into force 6
• NL – Liquidator should get access to data in the cloud 7
• NL – Rectification on Twitter and blogs 7
• NL – Dutch National Railway has to pay penalty for exceeding the travel data retention period 7
EU – ECJ finds that an author of software cannot oppose the resale of his ‘used’ licenses

On 3 July 2012, the European Court of Justice (ECJ) published a judgment in which it affirmed the right of licence holders to ‘resell’ their rights of use of computer programs, supporting intermediaries and end customers in the way.

In this case between Oracle International Corp. (Oracle) and UsedSoft GmbH (Usedsoft), the ECJ had to decide whether the right to distribute a copy of a software falls within the scope of the exhaustion rule laid down in the directive 2009/24 on the legal protection of computer programs (the Directive) which states that the first sale in the Community of a copy of a program by the right holder (or with his consent) exhaust the exclusive right to distribute that copy within the Community. Thus the central question was whether Oracle had proceeded with a ‘sale’ within that meaning. Oracle develops and distributes softwares mainly via its website. Oracle initiated proceedings against UsedSoft seeking an order that UsedSoft ceases sales of ‘second hand’ softwares licences acquired from existing Oracle’s clients. UsedSoft lost in first instance and then appealed the judgment. The Court of Appeal then asked the ECJ to clarify the content of the directive relating to the protection of softwares.

In this respect the ECJ found that the copy of a software and the licence to use it were to be considered ‘as a whole’ and that ‘the transfer by the copyright holder (Oracle) to a customer of a copy of a computer program, accompanied by the conclusion between the same parties of a user licence agreement, constitutes a ‘first sale’ of a copy of a program’ within the meaning of the Directive. As a result, the ECJ considered that Oracle had exhausted its distribution right, regardless of the medium used to copy the software on the computer (i.e. CD-ROM, DVD or directly downloaded from Oracle’s website). The ECJ also clearly stated that the exhaustion of the distribution right covers the software as initially downloaded but also the subsequent patches and updates issued by Oracle and relating to that software.

Moreover, the ECJ ruled that, in order to comply with the copyright holder’s exclusive right of reproduction, the original user – when selling its licence to UsedSoft – must render its copy unusable. The ECJ also stressed that in case the initial user has a licence for a larger amount of computers than he needs, the reseller (UsedSoft) is not authorised by the effect of the exhaustion of the distribution right to divide the licence and resell the licences in different parts.

Although software producers still have means to stop or control the resale of their products (e.g. serial number keys), the ECJ has issued a landmark decision which clearly opens the second-hand market for softwares. One could expect that this decision will pave the way to other industries such as ebooks and music tunes. Producers of non-tangible assets will surely wish to conduct an in-depth review of the terms and conditions of their contracts and licences granted to customers. (NVH)

The case can be found on http://curia.europa.eu, case No. C-128/11

EU – ECJ finds that the functionalities of a computer program and the programming language are not copyright-protected

On 2 May 2012, the European Court of Justice (ECJ) found that neither the functionality of a computer program, nor the programming language and the format of data files used in a computer program in order to exploit certain of its functions, constitute a form of expression in the meaning of Article 1.2 of EU Directive 91/250 of 14 May 1991. As a result, these elements are not protected by the special copyright regime for computer programs.

SAS Institute Inc. (SAS) started legal proceedings against World Programming Ltd. (WPL) for an alleged copyright infringement of its popular statistical analysis software, Base SAS. WPL had studied a version of the Base SAS software in order to mimic its functionality, without having access to the source code. To ensure compatibility for end users, WPL used the same programming language and the same format of data files that are used for Base SAS. WPL did not reproduce the protected source code but merely imitated its functions as closely as possible, SAS claimed that WPL indirectly copied its computer programs, thereby infringing its copyright. Moreover, SAS argued that its copyright was infringed by WPL as WPL studied the functionality of the ‘Learning Edition’ in breach of the terms of the license relating to that version.

The ECJ held that the functionality of a computer program does not constitute a form of expression that may be subject of copyright protection in terms of article 1(2) of Council Directive 91/250/EEC of 14 May 1991 (the Software Directive). The same applies to the programming language itself and the format of data files used in a computer program to interpret and execute application programs written by users, which are considered to be elements of that program by means of which users exploit certain functions of that program.

The ECJ ruled that copyright protection in the Software Directive only covers the individual expression of the work and leaves other authors the freedom to create similar or even identical computer programs, provided that they refrain from copying (part of) the source code and the object code. If not, it would be possible to monopolise ideas, to the detriment of technological progress and industrial development.

Finally, the ECJ stated that Article 5(3) of the Software Directive must be interpreted as meaning that a person who has obtained a copy of a computer program under a license...
is entitled to observe, study or test the functioning of that program so as to determine the ideas and principles of that program, provided that this person respects the terms and conditions of that license. In fact, the licensee may not even be prevented from doing so by means of contractual provisions. (PV)

The case can be found on http://curia.europa.eu, case No. C-406/10

EU – ECJ provides clarification on jurisdictional issues relating to infringements of personality rights on the Internet

On 22 October 2011, the European Court of Justice (ECJ) issued a judgment in which it clarifies which courts have jurisdiction in case of an infringement of personality rights on the Internet. The judgment is based on two individual cases (eDate Advertising GmbH vs. X and Olivier and Robert Martinez vs. MGN Limited).

In the case of eDate Advertising, an Austrian website owner, published an article on its website in which it reported on an alleged crime committed by Mr. X. Further thereto, Mr. X, who is a German citizen, requested eDate Advertising to remove the article concerned from its website. Since eDate Advertising refused to remove the article from its website, Mr. X initiated a claim before the German courts to have the article removed. In its defense, eDate Advertising stated that German courts do not have jurisdiction on this matter since the website is hosted in Austria. In light thereof, the German Constitutional Court referred the case for a preliminary ruling to the ECJ and asked the ECJ to determine as to whether article 5 (3) of the Brussels I Regulation allows individuals whose personality rights have been infringed, to bring an action at law in a Member State other than the Member State in which the website provider is established.

In the case of Olivier Martinez, Mr. Martinez, who is a French citizen, initiated a claim against MGN, the editor of the website of an English newspaper, for an alleged infringement of his private life. In the present case, MGN had published an article with the following title "Kylie Minogue is back with Olivier Martinez". Since Mr. Martinez believed that the article constituted an infringement of his private life, he initiated proceedings before the courts of Paris. In its defense, MGN stated that the courts of Paris do not have jurisdiction since MGN is established in United Kingdom. Further thereto, the courts of Paris referred the matter to the ECJ for a preliminary ruling and asked the ECJ to clarify whether a citizen of a Member State can initiate proceedings in his own country against a website owner established in another Member State who infringes the personality rights of that citizen.

In its judgment the ECJ concluded that Article 5 (3) of the Brussels I Regulation allows a person to initiate proceedings for an alleged violation of his personality rights against a party established in another Member State, either i) before the courts in which the website provider is established or ii) in his own country. In order for an individual who is subject to an infringement of his personal rights to bring an action at law in his own country, the ECJ also stated that such action can only be initiated if damages have occurred in such country. (LDA)

The case can be found on http://www.curia.eu

EU – Article 29 Working Party adopts opinion on cookie consent exemption

On 7 June 2012, the Article 29 Working Party issued an opinion on the protection of users of electronic communication networks and services by requiring informed consent before information is stored or accessed in the user’s terminal device via cookies and similar technologies.

Article 5.3 of Directive 2009/136/EC provides two criteria following which cookies are allowed to be exempted from this requirement of informed consent:

1) the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network;

2) the cookie is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Following the opinion, the above criteria are intended to ensure that the test for qualifying for such an exemption remains high.

In this light, the first criteria must be interpreted as a cookie being strictly necessary for communications taking place over a network between two parties. As such this criteria encompasses cookies that are necessary to route information over the network (e.g. identifying communication endpoints), to exchange data items in their intended order (e.g. numbering data packets) or to detect transmission errors or data loss. The second criteria can, in the Working Party’s opinion, only be invoked if the user did a positive action to request a service with a clearly defined perimeter or the cookie is strictly necessary to enable the information society service: if the cookies are disabled, the service would not work.

In application of the above criteria, the Working Party confirms that the following cookies can be exempted from informed consent under certain conditions, if they are not used for additional purposes:

1) user input cookies (session-id), for the duration of a session or persistent cookies limited to few hours in some cases;

2) authentication cookies, used for authenticated services, for the duration of a session;

3) user centric security cookies, used to detect authentication abuses, for a limited persistent duration;

4) multimedia content player session cookies, such as flash player cookies, for the duration of a session;

5) load balancing session cookies, for the duration of the session;

6) UI customization persistent cookies, for the duration of a session (or slight more);

7) third party social plug-in content sharing cookies, for logged in members of a social network. (SCO)

The opinion can be found on http://ec.europa.eu/justice/data-protection
EU – Article 29 Working Party adopts opinion on cloud computing

On 1 July 2012, the Article 29 Working Party issued an opinion on cloud computing in which it analyzes the possible privacy issues which have to be taken into account by the cloud computing service providers and their customers in the European Economic Area.

Cloud computing is a generic term for different kinds of technologies and service models which are directed at providing their services and making available their applications through the internet, and by which the end users have the benefit of the service online. These services are easy to set up and are just as easily adapted or extended, and as such lead to significant economic advantages. It also brings security benefits especially for small and medium-sized organisations, because they can acquire top-class technologies which otherwise might be too expensive.

However, the rise of cloud computing also represents a challenge to data protection. The wide scale deployment of cloud computing services can trigger a number of risks, such as the lack of control over personal data and insufficient information regarding how, where and by whom data is being processed. By submitting personal data to the systems managed by a cloud provider, cloud clients may no longer be in exclusive control of this data. This means that they may not be able to deploy the technical and organizational measures necessary to ensure for example the availability and confidentiality of data, for which the user of cloud computing services remains legally responsible under EU law.

In addition, insufficient information about a cloud service’s processing operations poses a risk to data controllers as well as to data subjects, because they might not be aware of potential threats and risks and thus cannot take measures they deem appropriate to mitigate those risks.

One of the key conclusions of the opinion is therefore that organizations wishing to use cloud computing services should, as a first step, conduct a comprehensive and thorough risk analysis. All cloud providers offering services in the European Economic Area should provide the cloud client with all the information necessary to rightly assess the pros and cons of using such a service. Security, transparency and legal certainty for the clients should be the key drivers behind offering cloud computing services. (LL)

The opinion can be found on http://ec.europa.eu/justice/data-protection

EU – European Commission launches new cloud computing strategy

The European Commission recently published a communication entitled ‘unleashing the potential of cloud computing in Europe’. With this communication the Commission tries to promote a faster adoption of cloud computing in Europe. This is because the diffusion of cloud computing is expected to have a substantial impact on the growth of the economy and the job market in the EU.

In its communication, the European Commission identifies three key areas, where intervention is required. A first key action, is to cut through the jungle of standards, so that cloud users can easily switch from one cloud-provider to another one. Interoperability, data portability and reversibility, are the main aims of this action.

A second key action, is the development of fair model contract terms and conditions. Such terms should cover issues such as data preservation after the termination of the contract, data disclosure and integrity, data location and transfer, direct and indirect liability, ownership of the data, change of service by cloud providers and subcontracting. Moreover, the Commission will review the standard contractual clauses applicable to the transfer of personal data outside of the EEA and adapt them to cloud services. The Commission will also call upon national data protection authorities to approve Binding Corporate Rules for cloud providers. These actions in combination with the proposed Regulation on a common European Sales Law and the proposed Regulation on Data Protection, will increase the trust of prospective consumers and thus accelerate the up-take of cloud computing.

A third key action is the creation of the European Cloud Partnership (ECP) to bring together industry expertise and public sector users to work on common procurement requirements for cloud computing. The aim of this action is to adapt the commercial offer to the European needs. This should eventually also benefit the private sector. (CLI)

The full communication can be found on http://ec.europa.eu.
BELGIUM

BE – New Cookie Act

On 28 June 2012, the Belgian Senate has adopted the new cookie provision by modifying the existing Belgian Act on Electronic Communication. The new provision shall enter into force on 1 October 2012. By enacting the cookie provision, the Belgian Senate transposed Article 5.3 of Directive 2002/58 as amended by Directive 2006/24. The official deadline for the implementation of this article was 25 May 2011. However, Belgium, among other countries, showed reluctance to transpose the rules into national law because of the on-going controversy on the subject. In May 2012, this incited the European Commission to request the European Court of Justice to impose fines on five countries, including Belgium, for failure to enact the appropriate national legislation.

The new measure requires website owners to obtain internet users’ consent before using certain kinds of ‘cookies’. In their most innocent form, cookies have a mere ‘technical’ use and they are used to improve a user’s experience by saving information such as log-in details and other preferences relating to a particular website. If the files known as cookies are placed on a user’s computer for the first time, they are known as ‘first party’ cookies – in contrast to ‘third party’ cookies. The latter are mostly used by advertisers and direct marketing service providers, and this use often collides with the privacy expectations of the average user.

The new Belgian provision makes a distinction between these two kinds of cookies. Whereas the Belgian legislator does not call for explicit permission whenever a first party cookie is set, such permission is required when third party cookies are installed on a user’s computer. Unlike the Dutch cookie legislation, which imposes ‘unequivocal’ permission for the installation of both first and third party cookies, the Belgian law is more lenient. The practical impact of the new cookie provision cannot be assessed at this stage. (LMA)

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

BE – The Court of Cassation finds that the principles governing employees’ rights in case of transfer of undertakings also apply in case of insourcing

Outsourcing is usually defined as the process of contracting an existing business function which an organization previously performed internally to an independent organization, where the function is purchased as a service. At the opposite, when a company ceases to contract a business process and begins to perform it internally, it is called insourcing.

There are rules which protect employees if the business in which they are employed changes hands. The European Directive of 14 February 1977 on the harmonization of employees’ rights in case of transfers of undertakings, businesses or parts of businesses (the ‘Acquired Rights Directive’) has been transposed under Belgian law in the Collective Bargaining Agreement no. 32bis of 7 June 1985 (‘CBA 32bis’).

In the event of a transfer of undertaking within the meaning of CBA 32bis, the rights and obligations of the transferring employer arising from the employment contracts existing on the date of transfer are automatically transferred to the new employer. In other words, the new employer must take over those staff on their existing employment conditions (including remuneration, job status, acquired length of service, place of work and working conditions), without any specific formalities having to be complied with.

The applicability of the CBA 32bis is subject to the following conditions: (1) the transfer must result in a change of employer, (2) it must be the result of a contract, and (3) it must concern a transfer of an undertaking, a business or a part of an undertaking or a business. The first two conditions are very broadly interpreted by the European Court of Justice (‘ECJ’) and usually do not create any application problems. The fulfilment of the third condition, however, gives rise to a lot of case-law.

Pursuant to Article 1(1) (b) of the Acquired Rights Directive, a transfer is defined as ‘a transfer of an economic entity which retains its identity, meaning an organized grouping of resources which has the objective of pursuing an economic activity, whether or not that activity is central or ancillary.’

On 7 May 2012, the Court of Cassation found that there is a transfer within that meaning when the catering activities of a business school were first outsourced and then brought in again. The fact that most of the assets used for the catering activities remained the property of that business school has no impact thereon.

On 20 November 2003 (C-340-01), the ECJ already ruled that the catering activity could not be regarded as an activity based essentially on manpower since it requires a significant amount of equipment. The Court, however, continued that the transfer of actual ownership of assets is unnecessary for the transfer of an undertaking to be deemed to have occurred. The mere use of ‘substantial parts’ of the tangible assets previously used by the first contractor and subsequently made available by the contracting authority to another one, sufficed for a transfer to fall under the Acquired Rights Directive. (NRO)

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

BE – Labour Court of Leuven finds that there is no violation of an employee’s right to privacy if the employer obtains certain information from the employee’s Facebook profile

In a recently published judgment of 17 November 2011, the Labour Court of Leuven found that an employee’s right to privacy is not violated if his employer obtains information which was circulated by the employee on his public Facebook profile.

In this case, an employee of a company which is quoted on the Belgian stock exchange consistently published comments on his Facebook profile on the financial difficulties of the company, the collective redundancy measures the company was forced to undertake, its annual results and its market position. These comments had been shared on a publicly available part of the employee’s profile. In addition, on its profile, the employee claimed to be responsible for the
business development in Asia and to hold the position of director, while actually only holding the position of business development manager. As its employer, the Belgian company argued that the employee’s comments were irreconcilable with the position the employee held. Furthermore, it claimed that the untrue representation as director on the employee’s Facebook profile worsened the situation because it gave more gravity to the significance of the comments.

In his defense, the employee argued that his right to privacy as laid down in the Belgian Data Protection Acts and in Article 8 of the European Convention on Human Rights had been violated because his Facebook profile was checked by his employer without his consent.

In its judgment, the Labour Court of Leuven found that in this case there was no violation of the employee’s privacy rights. It stated that, if an employee makes use of a social network and identifies himself on this network as a member of a company’s personnel, the employee has to refrain from acting or making statements in a way which could either be disloyal or detrimental for the company. (LL)

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

---

**BE – Privacy Commission adopts recommendation on surveillance at the workplace**

Following the public consultation of the Privacy Commission from July and November 2011 about what was called ‘cybersurveillance’ and which concerned internet and e-mail use at the workplace, the Privacy Commission published its findings and then recently also issued a brochure in which it sums up the main conclusions and recommendations relating to this issue. (LL)

The recommendation can be found at http://www.privacycommission.be.

---

**THE NETHERLANDS**

**NL – Amendments to Exemption Decree DDPA, Costs Decree and Notification Decree enter into force**

On the first of July 2012, some important changes in the secondary privacy legislation have entered into force.

Article 27 of the Dutch Data Protection Act (DDPA) determines that the processing of personal data has to be notified with the Dutch Data Protection Authority (DPA). The Exemption Decree DDPA provides several exemptions to the obligation to notify the DPA. The Exemption Decree has added several new exemption possibilities and has extended some of the exemptions already in place. For example, an exemption for the notification duty is introduced for the processing of personal data on an intranet, a personal website or weblogs. Furthermore, a notification to the DPA is no longer necessary when the personal data are transferred outside of the EEA, based upon the Standard Contractual Clauses of the European Commission or when a company has Binding Corporate Rules in place.

The Costs Decree enables a data controller to pass on the costs incurred, arising from an access request follow-up based upon article 35 of the DDPA, to the data subject. The maximum compensation which a data controller may charge has been slightly raised (from EUR 4.50 to EUR 5.00) and a special compensation for the provision of x-rays is introduced.

The changes in the Notification Decree lead to a simplification of the notification duty for large companies. If the different entities of a large company can be considered as a group in accordance with article 2:24b of the Dutch Civil Code, one of the companies can notify a certain type of processing on behalf of the whole group. (FVDJ)

---

**NL – Revised Telecommunications Act enters into force**

On the 5th of June 2012, the revised Dutch Telecommunications Act (Telecommunicatiewet), based upon the revised European Telecommunications Framework, has entered into force. The most relevant changes are the new cookies regulation, the rules on net neutrality and the notification obligation for data leaks and data security breaches.

Anyone who wishes to use cookies should provide website users with clear and unambiguous information about the purposes for which the cookies are used. Cookies can only be placed or accessed when the user has given its prior and explicit consent. This means that the old opt-out regime, in which the information on the use of cookies could be laid down in a privacy policy together with a possibility to opt-out, is replaced by an opt-in regime. This opt-in regime applies to all categories of cookies. Only cookies that are necessary for a service requested by the user or cookies that are strictly necessary to carry traffic data over an electronic communication network are exempted. It is not yet clear in which way the opt-in consent should be obtained. It is however clear that consent cannot be obtained via the browser settings.
The company is of the opinion that the defendant's accusations are unfounded and damaging for the company's reputation and its director. The company claimed that the defendant should remove all remarks and publications and also place rectifications.

The Court agreed with the claimant since all accusations were unfounded by the defendant and although the defendant claimed that the remarks had been removed, they were still available online. The defendant should also remove the (meta) tags on her blogs. Meta tags make it possible to provide certain information about a website. By linking the name of the company via tags to the negative remarks on her blogs, the defendant acts unlawfully.

The most interesting part of this case is the fact that the Court does not only order the defendant to place a certain rectification text on her blogs, but also orders her to do so on her Twitter-account. The Court did however not take into account that a tweet is limited to a maximum of 140 characters and that it will therefore not be possible to place the rectification in one single tweet. (FVDJ)

This case can be found on http://zoeken.rechtspraak.nl, LJN = BW3330.

NL – Liquidator should get access to data in the cloud

In a recent case before the Court of Appeal in 's-Hertogenbosch, the question was raised whether a liquidator should get access to data stored in a cloud, when the company, having a contractual relationship with the cloud provider, has gone into bankruptcy.

According to the Court, a liquidator has a concrete interest in getting access to the information in the cloud. Based upon article 93a of the Bankruptcy Act, the liquidator is empowered to enter any place to the extent that this is reasonably necessary for the performance of his duties. The Court is of the opinion that this means that the liquidator should also have access to the data stored in a cloud. The cloud provider should therefore fully cooperate in providing access to the data.

The liquidator also claims before the Court that the cloud provider should provide the data free of charge in an organized form. The cloud provider has however stated that this is unreasonable, since this would be very time-consuming and he would not get compensated for its efforts. The Court agreed: the cloud provider should make the data accessible, but it is up to the liquidator to ensure that the data are readily comprehensible. The liquidator can involve a third party or can request the cloud provider to organize the data in a suitable format for him. The liquidator will have to pay the cloud provider for its services. (FVDJ)

The case can be found on http://zoeken.rechtspraak.nl, LJN = BV9640

NL – Dutch National Railway has to pay penalty for exceeding the travel data retention period

In July 2011, the Dutch Data Protection Authority (Dutch DPA) imposed an order subject to a penalty of EUR 125,000 on the Dutch National Railway (NS) for exceeding the maximum retention period of travel data of students. The penalty forms part of a broader inquiry conducted by the Dutch DPA in December 2010 with regard to travel data processing, such as the card number and actual travel data (e.g. destination, location, time) by several Dutch transport companies. The Dutch DPA concluded that the transport companies retained the travel data of the students longer than necessary, as the data were stored for a period of seven years. All transport companies were obliged to reduce their data retention period subject an administrative penalty. The Dutch DPA is of the opinion that a maximum retention period of 24 months should apply for travel data.

The Dutch DPA granted the NS time up to and including November 2011 to introduce the compliant retention period. Furthermore, the NS was forced to delete the processed travel data after 24 months. The NS did not delete these data but informed the Dutch DPA that the data were anonymized and could therefore no longer qualify as personal data.
However, it turned out that the data could in fact be (in)directly traced back to the travelling student. Therefore, the NS has incurred the penalty. The NS has informed the Dutch DPA that it has now introduced the shortened retention period and that all travel data older than 24 months have been deleted. Furthermore, the penalty has been paid.

In the course of the 2010 inquiry, the Dutch DPA had also imposed an order subject to a penalty to the NS with regards to non-compliance with the information duty. The NS obliged students to check in and out with their travel chip card also during periods where they were entitled to travel for free, while this was actually not mandatory. The train company, however, did not inform the students that this was in fact optional and could therefore process the travel data of those students travelling during the free travel hours. Since the NS has in the meantime informed the students sufficiently, the NS will not incur this specific penalty.

The Dutch DPA is still investigating whether or not the other Dutch transport companies involved in the 2010 inquiry have complied with the requirements set in their administrative enforcement orders. (FVDJ)