Stibbe

ICT Law Newsletter

Number 50 – December 2014

Judica Krikke

Partner
T • +31 20 546 02 12
judica.krikke@stibbe.com

Gérald Origer

Partner
T • +352 26 61 81 11
gerald.origer@stibbe.com

Erik Valgaeren

Partner
T • +32 2 533 53 43
erik.valgaeren@stibbe.com

FOCUS: EUROPE

No right to copies of documents for request to access one's personal data under Dutch Data Protection Act

According to clause 35 of the Dutch Data Protection Act (*Wet bescherming persoonsgegevens;* "DDPA") a person ("data subject") has the right to access the personal data that a party processes about him. This right is an elaboration of the principle of transparency and enables a person to check whether the processing complies with the DDPA. It is not necessary for a data subject to explain why he wants access to his personal data nor does he need to prove any particular interest therein.

In practice, an appeal based on the right to access often has little to do with privacy protection. Usually it is used in a dispute to obtain certain documents from the other party. Since the DDPA came into effect in 2001 several legal cases have been conducted on the right to access. The following categories highlight some of the common issues likely to arise such as: (i) which documents fall within the scope of the right to access, and in particular whether the data therein qualify as personal data (data that is directly or indirectly traceable to an individual); and (ii) questions with regard to the actual exercise of the right to access, particularly whether or not copies of documents containing personal data should be provided.

With regard to this last question, the Dutch courts differed sharply. The highest civil court, the Supreme Court, held that the right to access should be interpreted broadly: in principle, copies of documentation should be provided to anyone who requests access. On the other hand, the highest administrative court, the Administrative Jurisdiction Division of the Council of State, as a starting point, stated that the right to access must be interpreted narrowly and that copies do not always have to be provided. It suffices to provide an overview of the personal data processed.

To clarify which line should be followed in the Netherlands, both the Middelburg District Court and the Administrative Jurisdiction Division have independently asked preliminary questions to the Court of Justice of the EU in Luxembourg. This has been possible since the right to access in the DDPA is an implementation of the European Privacy Directive 95/46/EC.

Both cases dealt with refused residency permits. The applicants requested access to the minutes containing the grounds for refusal. The Minister for Immigration, Integration and Asylum refused to provide a copy of the minutes because a legal analysis would not qualify as personal data. A data subject requesting access receives an overview of his personal data, its origins and the bodies with which the information is shared.

In short, the main questions submitted to the Court were as follows:

1. Is the legal analysis recorded in the minutes to be regarded as personal data?

2. Must a copy of the minutes be provided to fulfil the obligations under the right to access?

The Court consolidated both cases and ruled on 17 July.

According to the Court it is possible that a legal analysis recorded in the minutes may contain personal data, but the minutes as such do not qualify as personal data. The legal analysis is not to be regarded as information on the applicant because it relates to the interpretation and application of the law on the merits of the case. According to the Court, this is in line with the origin of the right to access, which stems from the notion that a person whose personal data are processed, must be able to verify that this is done in a correct and lawful manner. In a legal analysis, the data subject cannot verify this nor can the analysis be corrected by relying on the right of correction since this right exists to verify whether your personal data are processed correctly and not to review a legal analysis. The purpose of the Privacy Directive is to ensure the privacy of the data subject and is not a means of providing a right of access to administrative documents. It is remarkable that so far, both the Supreme Court and the Administrative Jurisdiction Division were of the opinion that if a person appealed using the right to access, the purpose behind the application was irrelevant. The Court qualifies this position slightly: the intention of the European legislator when drafting the Privacy Directive must be taken into account: the purpose of the data subject must match this intention.

With regard to dealing with a request to access, the Member States are free to determine in what manner access must be provided, as long as the information is provided in an understandable form. This means that the data subject must be able to inspect the information and must be able to check whether the information is processed in accordance with the Privacy Directive. Applying this approach means he can exercise his right to correct inaccurate information. The restrictive interpretation of the right to access, as advocated by the Administrative Jurisdiction Division, thus appears to be the accepted route. If a copy is provided, then all information which does not qualify as personal data can be removed.

In practice, it will still be a challenge to determine which information in a document should be regarded as personal data. It will therefore be interesting to see how future case law will deal with this issue.

The joint cases C-141/12 and C-372/12 can be found on http://www.curia.europa.eu

Friederike van der Jagt

Senior associate
T • +31 20 546 01 44
friederike.vanderjagt@stibbe.com

FOCUS: EUROPE

The new Regulation on electronic identification and trust services – eIDAS

The European Parliament and the Council adopted Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the "eIDAS Regulation") on 23 July 2014. This eIDAS Regulation repeals the E-Signatures Directive 1999/93/EC and creates a comprehensive legal framework for both electronic identification and authentication services.

This Regulation seeks to create a system of mutual recognition among Member States with regard to their national identification systems and thereby aims to enhance trust and effectiveness within the European internal market for public and private cross-border online services and e-commerce.

The first part of the Regulation sets up a legal framework to ensure, for the purpose of cross-border identification, a harmonized recognition of the numerous electronic identification means ("eIDs") used by Member States for natural and legal persons. However, the primary target is the public sector, and Member States have only the obligation to recognize those eIDs that are contained in a list published by the Commission based on the Member States' notifications. Member States remain free to decide which of their national existing eIDs they want to submit to notification, and the Regulation lays down the conditions under which the other Members States must recognize those eIDs. Moreover, Member States must cooperate with each other to ensure the interoperability of the multiple national electronic identification schemes.

The second part of the Regulation focuses on trust services (electronic identification and signatures, i.e., eIDAS).

Whereas the E-Signatures Directive only dealt with electronic signatures and had gaps in its framework, especially regarding cross-border interoperability issues and technological updating, the new eIDAS Regulation is much broader in scope. Indeed it now regulates a wide range of trust services such as electronic signatures, among others, but it also regulates electronic seals, electronic time stamping, electronic delivery service, electronic documents admissibility, and website authentication. The framework is based on the Member States' reciprocal obligation to recognize such trust services if those services are based on a qualified certificate issued in one Member State.

This new Regulation is an important step towards the enhancement of a trustworthy and secure online environment within the EU internal market. Most of it will enter into force by 1 July 2016 and thereby repeal with effect the E-Signatures Directive. Like all EU Regulations, it will not only apply directly to the services it regulates but also have an impact on some related existing national legislation. For instance, the inconsistent provisions of various national laws to implement the former E-Signatures Directive will automatically be replaced by the new Regulation's provisions.

Carol Evrard

Junior associate
T • +32 2 533 57 42
carol.evrard@stibbe.com

FOCUS: EUROPE

Public libraries may digitize books and make them available at electronic reading points without right holders' consent

Article 5 of the EU Copyright Directive 2001/29 (the "Directive") contains an exhaustive list of exceptions and limitations to the right holders' rights of reproduction and communication to the public. However, these exceptions and limitations may only be applied to certain special cases that do not conflict with a normal exploitation of the work and that do not unreasonably prejudice the legitimate interests of the right holder.

Pursuant to Article 5(3) of the Directive, Member States may provide for an exception if the acts of reproduction and/or communication are uses made by publicly accessible libraries, educational establishments, museums, or archives, and those uses concern works that are contained in these institutions' collection. Also, these acts of reproduction and/or communication should have been communicated or made available, for the purpose of research or private study, to individual members of the public through dedicated terminals on these institutions' premises—on condition that such works are not subject to purchase or licensing terms.

In the case that was referred to the European Court of Justice (the "ECJ") for a preliminary ruling, an academic library in Germany installed electronic reading points that allow the public to consult works from the library's collection. This library did not accept a publishing house's offer to the library to purchase and use electronic versions of its textbooks. Instead, the library digitized one of the textbooks it had in its collection to make it available to users on its electronic reading points on its premises. Users of those reading points could print out the work on paper or store it on a USB stick, in part or in full, and take it out of the library in that form.

In its ruling of that case on 11 September 2014, the ECJ held that the requirement for benefiting from such exception whereby the works in question may not be subject to purchase or licensing terms does not encompass the mere act of offering to conclude a licensing agreement. In other words, there must be an existing licensing agreement for the work in question that sets out the conditions under which the library may use that work. Also, the ECJ ruled that the Directive does not prevent Member States from granting libraries the right to digitize the books from their collections if it becomes necessary, for the purpose of research or private study, to make those works available to individuals through dedicated terminals. The right of libraries to communicate, through dedicated terminals, the works they hold in their collections would risk being rendered largely meaningless, or indeed ineffective, if they did not have an ancillary right to digitize the works in question.

However, the Court held that the above exception does not extend to acts such as the printing out of works on paper or their storage on a USB stick carried out by users from those dedicated terminals since such acts of reproduction, unlike some operations involving the digitization of a work, are not necessary for the purpose of making the work available to the users of that work. That being said, such acts of reproduction may, if appropriate, be authorized under national legislation transposing exceptions or limitations to the exclusive right of reproduction set forth in Article 5(2) of the Directive, such as the reproduction on any medium by a natural person for private use if, in any event, the right holders receive fair compensation for those acts of reproduction.

The case (C-117/13) can be found on http://www.curia.eu

Nicolas Roland

Senior associate
T • +32 2 533 51 51
nicolas.roland@stibbe.com

FOCUS: EUROPE

The European Court of Justice applies the temporary copyright exception to on-screen and cached copies of website pages -Meltwater case

On 5 June 2014 the European Court of Justice ("ECJ") rendered a judgment in response to a question asked by the Supreme Court of the United Kingdom. It held that on-screen and cached copies of website pages stored as a result of the end-user's browsing on the Internet do not require any authorization from the copyright owner of the content of those pages. In its judgment, the ECJ confirmed that the copies generated during one's viewing of a website fall under the temporary copyright exception provided in Article 5 of the Directive 2001/29/EC (the "Copyright Directive").

The defendant in this case was the PRCA (Public Relations Consultants Association), an association which uses the media monitoring services offered by the Meltwater group of companies ("Meltwater"). Meltwater provides them with online reports on news articles published on the internet. NLA and, more generally, internet users who visit websites generate two different sorts of copies of these articles on their computer. The first one is a copy made on the user's computer screen ("the on-screen copy"), and the second one is a copy in the cache memory of the user's computer hard disk ("the cached copies"). Although only the copyright owner of those articles has a right to authorize the copying of his or her work, Article 5 of the Copyright Directive lays down an exception to this reproduction right.

In the first part of its decision, the ECJ held that the conditions laid down in Article 5(1) were fulfilled. Moreover, the Court clarified that the condition of there being a transient nature of the act of reproduction means that the reproduction must be limited to what is necessary for that process. That nature is not lost just because of the end-user's intervention. Finally, the act of reproduction must be an integral part of a technological process and must be necessary for this process to operate efficiently. The Court stated in this regard that "without the creation of the cached copies, the internet would be unable to cope with current volumes of data transmitted online" and "the process used for viewing websites would be considerably less efficient".

In the second part of its decision, the Court confirmed that the exception applied to special cases that do not conflict with a normal exploitation of the work and that does not unreasonably prejudice the legitimate interests of the right holders, as required by Article 5(5) of the Directive. Indeed, since authorization to reproduce had to be sought in the first place for the online reports and articles to be placed on the publishers' websites, the legitimate interests of the copyright holders were, according to the Court, properly safeguarded.

In summary, the ECJ held that the copies that were generated while one views a website satisfy the conditions of the temporary reproduction exception and may therefore be generated without the need for the copyright holders to grant any license or authorization for such reproduction. This decision appears to be in line with Recital 33 of the Copyright Directive, which seems to have been adopted precisely to cover situations such as the one at stake, and which states that "this exception should include acts which enable browsing as well as acts of caching to take place".

This decision, read in conjunction with a previous decision rendered by the ECJ on the legality of hyper-links (Svensson case) makes it clear that the copyright legal framework cannot undermine progress towards the expending efficiency of the internet. The Court was, however, clear that this reasoning does not apply if the end-user downloads or prints out the content of the webpage. Finally the ECJ left open the question of legality of such copies in situations where the websites' contents were put online without the right holder's consent.

The case (C-360/13) can be found on http://www.curia.eu

Carol Evrard

Junior associate
T • +32 2 533 57 42
carol.evrard@stibbe.com

FOCUS: BELGIUM

Belgian Privacy Commission clarifies data breach notification requirement

As a consequence of several data breaches, the Belgian Privacy Commission ("BPC") published in January 2013 a recommendation to prevent data breaches. In this recommendation the BPC has for the first time mentioned the existence of a requirement to notify a data breach within 48 hours to the competent authorities. In a recently published Q&A on its website, the BPC now tries to clarify this requirement.

Although the BPC recognizes that there is no legal requirement to notify a data breach, the BPC advises strongly to do so nevertheless. It therefore reiterates the previously mentioned notification period of 48 hours.

The BPC stipulates further that the persons concerned by a data breach will also need to be informed by means that allow the affected persons to receive the relevant information quickly. The notification to the persons affected by the breach should contain the following information, among other things:

- Contact details from which the data subjects can obtain additional information on a breach incident;
- A summary of the incident that has affected the personal data of the data subject;
- The nature and the purpose of the personal data concerned;
- Conceivable consequences of the data breach for the data subject;
- Circumstances under which the data breach took place;
- Measures taken by the data controller to prevent the data breach;
- The measures on which the data controller advises the data subjects to take to mitigate the damage.

A notification to the data subjects is not required if the data have been sufficiently encrypted. Also, the notification may be postponed if there is a risk that the notification to the data subjects might jeopardize the effectiveness of the investigation. If this occurs, the data controller must indicate on the notification form that it wishes for such permission and explains the reasons for this.

The BPC also sets out further the circumstances in which no notification to the BPC is required: (i) if the data are encrypted, and (ii) if the following three conditions have been fulfilled:

1. The data subject has immediately been informed of the complete scope of the breach as well as its consequences;
2. The data breach concerns only a limited group of people (about 100 persons); and
3. No sensitive or financial data have been compromised.

Finally, the BPC also makes a form available on its website to facilitate the notification procedure. This form must be completed and sent to the BPC via a secured e-forms application on its website.

The complete Q&A of the BPC can be found on: http//www.privacycommission.be

Press offence before the Assise Court

For only the second time since World War II, the Brussels' Chamber of Indictment has referred a press offence to be trialed by a jury, before the Assise Court. A press offence is any abuse of the freedom of expression such as libel and slander (Article 383 of the Belgian Criminal Code); written insult (Art. 448 BCC); or obscene or indecent writings (Art. 383 BCC) that is committed by using the (printing) press and which is made public. A press offence is therefore only distinct from other offences, in the way that it is committed through the press. According to the Supreme Court, the criminal expression of an idea or opinion through printed and published writings constitutes a press offence.

Article 150 of the Belgian Constitution provides that all press offences, except for those which are inspired by racism or xenophobia should be trialed by jury.

However, since 1941 only one case of a press offence has been trialed by the Assise Court. Usually, the Court's Chamber of Indictment finds that the conditions for a press offence have not been fulfilled, in which case the matter is dealt with by the correctional courts, or that the case has been statute-barred. Not so in this case.

The facts concern a university professor who has sent allegedly libelous e-mails to other members of the faculty about one of his colleagues. This colleague subsequently filed charges for libel and slander. Where usually such cases are dealt with by the correctional courts or even the civil courts, in this case the defendant argued that it concerned a press offence and that it should therefore be dealt with by a jury trial. The Court's Chamber of Indictment confirmed this and referred the case to the Court of Assise. Following the judgment of the Chamber of Indictment, the prosecutor will now have to schedule the case on the Assise Court's agenda.

Cédric Lindenmann

Junior associate
T • +32 2 533 54 56
cedric.lindenmann@stibbe.com

FOCUS: BELGIUM

The Antwerp Commercial Court finds that Bhaalu cannot lawfully rely upon the "private copy" exception enshrined in the Belgian Copyright Act

Right Brain Interface NV is a young technology company that has created a remote DVR (digital video recording) storage service called "Bhaalu". In essence this service allows its subscribers to record the television programs they can watch according to their TV channels' subscription and to store these programs on servers owned by the unincorporated association of Bhaalu users ("in the cloud"). This way, Bhaalu users can watch TV programs on demand up to 3 months after they have been aired.

This system is also called "Collaborative Video Recorder" (or CVR) given that the users are basically sharing the cost of certain common components of the CVR hardware, without it being technically possible for them to share or transfer content with other users.

Naturally, Bhaalu's entry on the Belgian market has led to a great deal of opposition by Belgian broadcasters. This has led Medialaan, VRT, and SBS Belgium to sue Right Brain Interface NV before the Commercial Court of Antwerp on grounds of their right to exclusive reproduction and communication enshrined in the Belgian Copyright Act.

The broadcasters asserted that Right Brain Interface NV should have obtained the broadcasters' prior consent because they had an exclusive reproduction right. But Right Brain Interface NV invoked the "private copy"-exception provided by the Belgian Copyright Act on grounds that the user may only (i) use Bhaalu if he or she has subscribed to the particular channel, (ii) watch his or her own recorded programs, and (iii) watch his or her recorded programs within the "family circle".

The Antwerp Court first concluded that it was indeed the Bhaalu user—and not Bhaalu itself—who makes a "private copy" in the sense of the "private copy"-exception under the Belgian Copyright Act.

Then the Court ascertained that the television signals originating from TV Vlaanderen and Telenet constituted the source of Bhaalu's recording capacity. These television signals needed to be decrypted and thus also copied in the Bhaalu datacenter in order for Bhaalu to be able to provide its CVR service to its users. However, Right Brain Interface NV did not obtain the prior consent from TV Vlaanderen and Telenet to decrypt these television signals.

Therefore, the Court ruled in favor of the broadcasters and declared that Right Brain Interface NV has infringed the broadcasters' copyrights because it copies television signals from an illicit source and communicates the copied signals to the public, even if the users/subscribers would have lawfully received the broadcast through a television receiver.

Finally, Right Brain Interface NV asserted that it merely provides the equipment for making the "private copy", so it should not be categorized as a service provider. But the Court rejected Right Brain Interface NV's argument. The Court found that Right Brain Interface NV's activities in the Bhaalu system were inextricably linked to the infringing acts and that the Bhaalu devices could not function without the interventions of Right Brain Interface NV. Therefore, the Court ordered Right Brain Interface NV, as the intermediary whose services were used for such infringements, to cease its activities under penalty of a fine of EUR 1,000 per week and per user.

Valerie Vanryckeghem

Junior associate
T • +32 2 533 51 72
valerie.vanryckeghem@stibbe.com

FOCUS: THE NETHERLANDS

Dutch broadcaster Tros is not obliged to remove footage/files from its website—the right to inform prevails over the right of reputation

On 10 September 2014 the Amsterdam District Court held that only in exceptional cases will broadcasters be obliged to remove news or information from their show's websites because according to the Court, the right to inform prevails over the right of reputation.

The facts of the case before this Court were as follows: Tros, a Dutch broadcaster, aired a television show called "Opgelicht?!". Certain episodes of this show featured the alleged wrongdoings of an individual. These episodes remained available on the website of the show.

The person concerned (the claimant) sued Tros, seeking primarily to have those episodes featuring him removed from the website within 48 hours. In the alternative, he sought to have the website file and episodes only accessible using a login name and password and further requested that Tros remove information from the website because they were inaccurate. The claimant's underlying reasoning was that he felt publicly denounced as a result of the television show, even though he was punished by imprisonment (by being convicted of embezzlement (but acquitted for fraud)). According to him, the TV show aired by Tros had major consequences for both him and his family and amounted to a violation of his privacy. Indeed, he was forced to relocate his residence, and he subsequently lost his job. Moreover, the problematic content is still available on the show's website which makes it particularly difficult for him to reintegrate into society and to find a new job.

Tros relied on Article 10 of the European Convention of Human Rights ("the ECHR") in its defence, saying that it can warn society about social wrongdoing and that the public has the right to be informed. Furthermore, Tros argued that the content published on its show's website was adequately and sufficiently supported by the facts. Tros asserted it handled the case at stake correctly since they let the public prosecutor and the press officer of the court explain the facts of the case in one of the aired episodes. Finally, Tros stated that to ensure the protection of the claimant's privacy, it has anonymized all references to the claimant by using only his initials in the internet file and blurring his face in all the footage that were on the website.

In its ruling regarding the primary claim, the Court held that Tros's interest in informing the public may only be restricted if such restriction is laid down by law and if the restriction is necessary for a democratic society to, for example, protect one's good name or the rights of others (Article 10§2 ECHR). The Court said that, to decide which right prevails, it is essential to make a balance between the freedom of information, on the one hand, and the protection of a person's good name, on the other. The Court also held that although the information published are detrimental to the claimant, this was not sufficient to uphold the claims being sought. In addition to its freedom of information, Tros—as a journalistic medium—has an important archiving role. The court held that only in exceptional cases should archived news and information be removed. Furthermore, the claimant did not prove that the information published about him by Tros were incorrect. Tros is at liberty to question the ruling of the Court in which he was acquitted, even if the claimant does not agree to the questioning. According to the Court, Tros has shown that it handled the case correctly. Finally, the Court concluded that the claimant's privacy was not violated: Tros only referred to him by using his initials and blurred his face. All in all, the Court dismissed the primary claim.

Regarding the alternative claim, the Court ruled that it should be partially upheld, i.e., it found that there was indeed one inaccuracy in a statement regarding the claimant's earlier imprisonment, and Tros was ordered to correct this fact within 48 hours (and if it did not, it would be sanctioned).

[Source: District Court Amsterdam, 10 September 2014, ECLI:NL:RBAMS:2014:5809]

This article was written by summer trainee Nini Blom, and reviewed by Frédéric François.

Frédéric François

Associate
T • +31 20 546 03 06
frederic.francois@stibbe.com

FOCUS: THE NETHERLANDS

Parking information must be provided by commercial parking operators to the Tax Authorities

In December 2012, the Tax Authorities requested SMS Parking, a parking operator in several large Dutch municipalities, to provide all its clients parking data – including registration numbers and geographical data together with date and time – so they could use this data to levy various taxes. The Tax Authorities made similar requests to several other parking operators, all of which complied. SMS Parking, however, refused to cooperate as they felt that the request was disproportionate and a violation of the privacy of their customers. Furthermore, they stated that it is possible for the Tax Authorities to obtain this information via another route, for example, by the use of digital photos. In response, the Tax Authorities started summary proceedings with an application for a temporary injunction to coerce release of the data. The summary proceedings judge followed SMS Parking in their defence and ruled that parking behaviour of customers of SMS Parking was indeed privacy sensitive information since it reveals a lot about their personal (private) behaviour. The unlimited request for data from the Tax Authorities was an infringement on the privacy of SMS Parking customers which was disproportionate to the pursued objective and SMS Parking did not have to provide the parking data.

The judgment was however overturned on appeal. The court ruled that the unlimited request from the Tax Authorities is justified to ensure the economic welfare in the Netherlands. Nonetheless the Tax Authorities are bound by the requirements of proportionality and subsidiarity. According to the court, it is not relevant whether the Tax Authorities know in advance that the data is relevant for levying taxes against a particular taxpayer. The fact that it is an unlimited request for data from an extensive database does not make the request, by definition, disproportionate. In this case, the search is through databases containing more than 3 million registration numbers. According to the court, the parking operators are not asked to provide personal details of customers but only their registration numbers. In this respect the court believes that this fiscal method is proportionate.

An appeal on the principle of subsidiarity, based on the fact that it is possible to obtain data in a way which is less invasive of the privacy of the individuals concerned, did not help SMS either. SMS Parking suggested that the Tax Authorities could photograph the registration numbers themselves. The court held that this is not less invasive of the privacy of citizens and that it would be considerably more labour intensive. SMS Parking also offered to make a pre-selection for the Tax Authorities. The court dealt with this issue summarily, on the basis that this would affect the privacy of a large number of citizens, and in view of the fact that SMS Parking is not subject to the same rules as a government body. The conclusion is that SMS Parking has no legitimate grounds to refuse the provision of data and should release it forthwith. SMS Parking stated during the proceedings that they would disclose the parking data if this was the decision of the court. The final decision of the court is a pity from a privacy perspective, especially since the supervisory authorities (the Dutch Data Protection Authority – College bescherming persoonsgegevens) have not been tempted to issue an informal opinion. Therefore, it remains to be seen whether there will be a different interpretation of the proportionality test in future cases.

[Source: Court of Appeal 's-Hertogenbosch,19 August 2014, ECLI:NL:GHSHE:2014:2803]

Friederike van der Jagt

Senior associate
T • +31 20 546 01 44
friederike.vanderjagt@stibbe.com

FOCUS: THE NETHERLANDS

Customer responsible for costs deriving from hacked voice services

NEC Nederland BV (NEC), the Dutch branch of NEC Corporation which is a worldwide provider of IT and communication solutions, uses voice services provided by KPN BV (KPN), a Dutch telecom provider. In order to use these voice services, NEC built their own PBX (Private Branch Exchange – which is a system that concentrates central office lines and enables intercommunication between a large number of telephone stations within NEC) connected through a router to the WAN (Wide Area Network). Unauthorized parties have managed to get access to the data lines via a badly secured NEC PBX device and have set up a dial up service through which telephone traffic with East Timor has taken place. KPN has invoiced NEC for the costs involved, in the sum of EUR 176,895,00. KPN claims payment of the invoice stating that it was NEC's obligation to monitor the traffic. NEC however states that KPN has a duty of care (statutory and reinforced by case law) which entails that telecom providers are obliged to monitor telephone traffic and take measures when deviating telephone traffic is noticed. Furthermore, NEC claims that KPN should have warned NEC about the risks of using voice services. Because KPN neither monitored the telephone traffic nor warned NEC of the risk (the hack was discovered during a test), NEC claims that it is not liable for the costs of the fraudulent use of the voice services.

The Court rejects NEC's claim that KPN owes it a duty of care. NEC built their own PBX system, which makes them responsible for the hardware and, being a professional in the communications sector, they are supposed to be aware of the risks of using voice services. A previous hack of their PBX system resulted in damage amounting to EUR 40,000 and confirms that NEC were aware of the risks involved. Following this incident, NEC asked KPN if it was possible to cap the use of their lines as a safeguard. KPN explained that this was not possible and instead offered a tool to enable NEC to monitor traffic on a daily basis. NEC decided not to make use of this option.

NEC also tried to rely on jurisprudence relating to telephone traffic, by claiming that such traffic should be adequately monitored on a regular basis. This plea was also rejected because – contrary to other phone traffic - different providers are used to provide voice services and KPN cannot monitor the traffic on the data lines of other providers.

Therefore, the Court concluded that NEC cannot claim a duty of care from KPN and that NEC should pay KPN's invoice.

[Source: District Mid-Netherlands, 2 July 2014, ECLI:NL:RBMNE:2014:2617]

Joost van Eymeren

Junior associate
T • +31 20 546 03 32
joost.vaneymeren@stibbe.com

FOCUS: LUXEMBOURG

A new booklet on the supervision at the workplace published by the Luxembourg Data Protection Commission and the Luxembourg Chamber of Employees

The Luxembourg Data Protection Commission (the « CNPD ») has published in September 2014, together with the Luxembourg Chamber of Employees (*Chambre des salariés*), a booklet on the supervision at the workplace.

On the one hand, the booklet deals with the two existing systems of supervision. According to article 2 (p) of the law of August 2, 2002 on the protection of persons with regard to the processing of personal data (the « DPA »), the term "supervision" (*surveillance*) is defined as *"any activity which, carried out using technical instruments, consists of observing, collecting or recording in a non-occasional manner the personal data of one or more persons, concerning behaviour, movements, communications or the use of electronic computerised instruments".*

Articles 10 and 11 new of the DPA help to clarify the processing for supervision purposes (general system) and supervision at the workplace respectively. However, Articles 11 new refers to Article L.261-1 of the Employment Code. Therefore, processing for the purposes of supervision at the workplace is not dealt with anymore in the DPA further to Article 10 of the law of July 27, 2007 amending the DPA, but in Article L.261-1 of the Employment Code. According to this Article, processing for the purposes of supervision at the workplace is only possible if needed for:

1. the security or the health of employees, or;

2. the protection of the properties of the company, or;

3. the control of the production process handled by machines, or;

4. the temporary control of the production or the service of employees if this is the only way to ascertain the exact salary, or;

5. the organisation of flexible working hours.

On the other hand, the booklet focuses on the various forms of supervision used at the workplace, such as, *inter alia*, (i) the video surveillance, (ii) the use of computing tools (e.g. check of the emails received and sent, logs of the websites visited), (iii) the recording of telephone conversations, (iv) the biometric identification systems, (v) the geolocation systems, (vi) the supervision of the working hours and the entrances of the building.

The booklet is available in French on the website of the CNPD on the following link: http://www.cnpd.public.lu/fr/publications/brochures/brochure-surveillance-CNPD-CSL/CSL-CNPD-La-surveillance-sur-le-lieu_de_travail.pdf

Johanne Mersch

Associate
T • +352 26 61 81 20
johanne.mersch@stibbe.com

Stibbe

Meet us at...

Stibbe is proud sponsor of and contributor to the upcoming IBA Conference and CPDP conferences. The IBA Conference focuses on “Legal Risks and New Technologies: Challenges for the Modern Enterprise”, and is held in Brussels between 23 and 25 January 2014. The theme of the 2015 CPDP conference (21-23 January 2015, Brussels) is “Data protection on the Move”.

Our team will be present, and we hope to see you there!

Keep a close eye on our website for updates.

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

Brussels

Central Plaza
Loksumstraat
Rue de Loxum 25
1000 Brussels
Belgium
T • +32 2 533 52 11
F • +32 2 533 52 12

Amsterdam

Stibbetoren
Strawinskylaan 2001
PO Box 75640
1070 AP Amsterdam
The Netherlands
T • +31 20 546 06 06
F • +31 20 546 01 23

Luxembourg

Rue Jean Monnet 6
2180 Luxembourg
Luxembourg
T • +352 26 61 81
F • +352 26 61 82

The ICT Law Newsletter is also available on our website

www.stibbe.com

Dubai

Dubai International Financial Centre
Gate Village 7, Level 4
PO Box 506631
Dubai UAE
United Arab Emirates
T • +971 4 428 63 13
F • +971 4 365 31 71

Hong Kong

Suite 1008-1009
10/F, Hutchison House
10 Harcourt Road
Central, Hong Kong
T • +852 2537 0931
F • +852 2537 0939

London

Exchange House
Primrose Street
London EC2A 2ST
United Kingdom
T • +44 20 7466 6300
F • +44 20 7466 6311

New York

489 Fifth Avenue, 32nd floor
New York, NY 10017
USA
T • +1 212 972 4000
F • +1 212 972 4929