Stibbe

ICT Law Newsletter

Number 52 – December 2015

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

European Court of Justice considers the exchange of traditional currencies for bitcoins exempt from VAT

On 22 October 2015, the European Court of Justice ("ECJ") issued a judgment in response to a request from the Swedish Supreme Administrative Court (Högsta förvaltningsdomstolen) for clarification on the question whether transactions to exchange a traditional currency for the 'Bitcoin' virtual currency or vice versa were subject to value added tax ('VAT').

This decision follows a dispute between the Swedish tax authority (Skatteverket) and Mr. Hedqvist, a Swedish national who requested permission from the Swedish Revenue Law Commission (Skatterättsnämnden) to operate his online bitcoin exchange. In a preliminary decision, the Swedish Revenue Law Commission informed Mr. Hedqvist that bitcoin was exempt from VAT under Swedish law. However, the Swedish Tax Authority did not agree and appealed against the decision, arguing that the service in question was not covered by the VAT exemption under Swedish law.

The Swedish court saw itself forced to refer the following two questions to the ECJ:

1. *Is Article 2(1) of the VAT Directive to be interpreted as meaning that transactions in the form of what has been described as the exchange of virtual currency for traditional currency and vice versa, which is effected for consideration added by the supplier when the exchange rates are determined, constitute the supply of a service effected for consideration?*

2. *If so, must Article 135(1) [of that directive] be interpreted as meaning that the abovementioned exchange transactions are tax exempt?'*

According to the ECJ, the exchange transaction at issue falls under article 2 (1)(c) of the Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (the VAT Directive). The ECJ first clarified that the exchange of different means of payments constitutes a supply of services within the meaning of article 24 of the VAT Directive, since bitcoins cannot be characterized as "tangible property" referred to in article 14 of the VAT Directive. The Court goes on to recall that the supply of services is effected "for consideration" only if there is a direct link between the services supplied and the consideration received. According to the ECJ, it is clear that the exchange of traditional currency for units of bitcoin, in return for payment of a sum equal to the difference between the price paid by the operator to purchase the currency and the price at which he sells the currency to his clients, constituted a supply of services for consideration within the meaning of Article 2(1)(c) of the VAT Directive.

Subsequently, the ECJ focussed on the question whether this supply of services could fall under one of the VAT-exemptions laid out in article 135 (1) VAT Directive, more specifically the transactions included in paragraphs (d) to (f).

The ECJ explains that bitcoins, as a direct (contractual) means of payment, cannot be regarded as a "current account or deposit account, a payment or a transfer", nor as "debt, cheques and other negotiable instruments" referred to in article 135 (1)(d) VAT Directive. The transactions targeted by this paragraph concern services or instruments that operate as a way of transferring money without actually involving money itself. The exchange transaction at issue, where bitcoins are exchanged for actual money, can therefore not fall under the scope of article 135 (1)(d) VAT Directive.

However, according to the ECJ, the exchange transaction at issue does fall under the exemption for transactions involving "currency, bank notes and coins used as legal tender" as laid out in article 135(1)(e) VAT Directive. According to the ECJ (in line with the AG's conclusions in points 31 to 34) this article applies to financial transactions involving both traditional and non-traditional currencies. The ECJ stresses that to interpret this provision as including only transactions involving traditional currencies would go against the context and aims of article 135(1)(e) VAT Directive as transactions involving non-traditional currencies that have been accepted by the parties to a transaction are also financial transactions. Applied to this case, the bitcoins exchange has no other purpose than to be a means of payment.

Finally, the ECJ concluded that the bitcoin exchange transactions do not fall within the scope of the exemptions laid down in article 135 (1)(f) VAT Directive, namely for transactions in "shares, interests in companies or associations, debentures and other securities", as it is commonly accepted that the bitcoin virtual currency is neither a security conferring a property right nor a security of a comparable nature.

With this decision, the ECJ laid out a positive future for bitcoin-purchases at bitcoin-exchanges in Europe. Following this decision, Europeans can continue to buy bitcoin with traditional currency without paying tax. We can only now hope that this approach gets adopted by countries outside of the European Union, thereby further harmonizing Bitcoin's taxation-approach.

The case (C-264/14) can be found on http://www.curia.europa.eu

Michiel Van Roey

Junior associate
T • +32 2 533 52 07
michiel.vanroey@stibbe.com

Charlotte Bihain

Junior associate –
Tax department
T • +32 2 533 54 80
charlotte.bihain@stibbe.com

FOCUS: EUROPE

ECJ on territorial application of domestic data protection law: a single representative can fulfill "stable establishment" concept under Directive 95/46/CE

On 1 October 2015 the European Court of Justice ("ECJ") rendered a judgment in response to the questions raised by the Kúria (Hungarian Supreme Court) on the applicability of Hungarian data protection law and on the powers of the Hungarian Data Protection Authority ("DPA") in relation to a company that is registered in Slovakia but offers online services in Hungary.

This was an important decision as the ECJ ruled that the concept of "establishment" in the meaning of article 4 of the Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 (the "Directive") should be flexibly interpreted, and thus it cannot depend on the place where the company is registered.

The claimant, Weltimmo, is a company registered in Slovakia and runs a real estate services website for Hungarian properties. After a one-month grace period during which advertising on the website was free of charge, Weltimmo kept the advertisers' data, charged them for the services it provided, and if necessary, sent their data to debt collection agencies. The Hungarian DPA fined Weltimmo for violation of the Law of 2011 on the right to self-determination as regards information and freedom of information. Weltimmo then brought an action before the Budapest Administrative and Labour Court and then to the Supreme Court.

In the first part of its decision, the ECJ clarifies that the applicable law to a data controller must be determined in light of Article 4 of the Directive rather than Article 28, which only relates to the role and powers of the supervisory authority. The ECJ further restates the ruling on the Google Spain case (C-131/12) and confirms that the words *"in the context of the activities of an establishment"* in Article 4 of the Directive cannot be interpreted restrictively. After having clarified that, the ECJ analyzes the several aspects of this requirement.

Firstly, the ECJ refuses to adopt a formalistic approach of the concept of "establishment" whereby companies would be deemed established solely where they are registered. This establishment concept must, however, imply that there is (1) a certain degree of stability of the arrangements; and (2) an effective exercise of activities. These two conditions must be interpreted in the light of the specific nature of the company's economic activities and the provision of the services concerned. The ECJ further insists that this is even more true for companies such as the one at stake, which offers services only over the Internet.

Even more importantly, the ECJ affirms that the effectiveness of the activity can be very limited, as it was the case here, in which only one representative of Weltimmo was present in Hungary as the point of contact between the company and the data subjects. Indeed, the Court states that *"the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question."*

Secondly, the ECJ assesses whether the processing of the personal data is carried out in the context of the activities of the establishment. The ECJ refers again to the Google Spain case and clarifies that this does not mean that the activity must be carried out by the establishment itself, but rather in the context of its activities.

The ECJ, while leaving the factual assessment of Weltimmo being established in Hungarian in the case at stake, has nevertheless broadened the territorial scope of domestic data protection law significantly by affirming that the mere presence of an individual in one Member State, who acts for a company registered in another Member State, can be sufficient for the DPA of the former Member State to have power over this company.

The case (C-264/14) can be found on http://www.curia.europa.eu

Carol Evrard

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

FOCUS: EUROPE

Data transfers to the US : the European Court of Justice declares that the EU Commission's Safe Harbour Decision is invalid

The Data Protection Directive (95/46/EC) provides that the transfer of personal data to a third country outside the European Economic Area may, in principle, take place only if that third country ensures an adequate level of personal data protection. This "adequate level of personal data protection" can be established in a number of ways, one of which is a declaration of the EU Commission approving a country's personal data protection regime. Other options are consent of the data subject, implementing binding corporate rules or executing EU model clauses between the data exporter and data importer.

In its decision of 26 July 2000 (hereinafter the "Safe Harbour Decision"), the EU Commission declared that the US ensures an adequate level of personal data protection through the Safe Harbour Principles, which have been widely adopted to justify transfers of personal data to US undertakings certified within safe harbor.

This Safe Harbour Decision has now been declared invalid by the European Court of Justice (hereinafter "ECJ"), in its judgment of 6 October 2015.

The judgment was rendered in response to a question posed by the Irish High Court in which it wished to ascertain whether the Safe Harbour Decision has the effect of preventing a national supervisory authority from investigating a complaint alleging that the third country does not ensure an adequate level of protection and, where appropriate, from suspending the contested transfer of data. The question was raised during a lawsuit against Facebook, who transferred personal data from its Irish subsidiary to servers located in the United States for further data processing.

The ECJ first stated that the existence of an EU Commission decision, declaring that a third country ensures an adequate level of personal data protection, cannot reduce or eliminate the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and the Data Protection Directive.

This entails that the national supervisory authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the Data Protection Directive. Nevertheless, the ECJ pointed out that it alone has jurisdiction to declare an EU act, such as the Safe Harbour Decision, invalid.

In its validity assessment the ECJ first observed that the EU Commission did not find that the US ensured an adequate level of personal data protection by reasons of its national law or its international commitments. The EU Commission merely examined the Safe Harbour Principles, which is applicable solely to US undertakings which adhere to it. In addition, US national security, public interest and law enforcement requirements can deviate from and prevail over the Safe Harbour Principles.

With regard to the assessment whether the US essentially maintains a level of protection equivalent to the EU, the ECJ concludes that:

- US legislation violates the fundamental right to respect for private life by allowing storage of all personal data, without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use;

- US legislation violates the fundamental right to effective judicial protection by not providing legal remedies to individuals in order to access, rectify or delete personal data relating to him/her.

For all those reasons, the ECJ declares the Safe Harbour Decision invalid. As a consequence the Irish supervisory authority is required to examine the complaint against Facebook's data transfers with all due diligence and to decide whether this particular transfer to US servers should be suspended on the ground that the US does not afford an adequate level of personal data protection.

This judgment also implies that undertakings need to take action if they are currently relying on the Safe Harbour Decision to justify personal data transfers outside the European Economic Area.

Alternative solutions to ensure an adequate level of personal data protection when transferring personal data outside the EEA can be achieved by:

- obtaining consent from the data subject for the transfer; or

- implementing binding corporate rules; or

- executing model clauses between the data exporter and data importer.

Valerie Vanryckeghem

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

FOCUS: BELGIUM

Court of Cassation definitively confirms Yahoo!'s obligation to cooperate with law enforcement agencies

On 1 December 2015, the Court of Cassation dismissed an appeal lodged by Yahoo! against the ruling of the Court of Appeal of Antwerpen of 20 November 2013. The Court of Appeal partially confirmed the judgment issued in 2009 by the Criminal Court of Dendermonde that convicted Yahoo! and obliged it to disclose the identity of the persons who committed fraud via their Yahoo! e-mail addresses.

The public prosecutor of Dendermonde had requested Yahoo!, which is established in the US, to disclose the identity of certain people who used Yahoo! e-mail addresses to commit internet fraud. The public prosecutor's claim was based on Article 46*bis* of the Criminal Procedure Code (CCP), which provides that electronic communication services providers are obliged to disclose identification data to law enforcement agencies upon their request. Although Yahoo! is established in the US and has no branch or office in Belgium, the public prosecutor was of the opinion that Yahoo! is to be considered such an electronic communications service provider and is consequently obliged to comply with his request.

Yahoo!, however, refused to disclose the identification data by claiming that it is not subject to Article 46*bis* of the CCP, since it was not an electronic communications service provider. According to Yahoo!, the term "electronic communications service provider" in Article 46*bis* of the CCP had the same meaning as the term "electronic communications service provider" in Article 2 of the Belgian Electronic Communications Act of 13 June 2005 (BECA). Since this Article 2 provides that a provider of *information society* services, such as providers of free e-mail addresses, are not to be considered provider of *electronic communications* services, Yahoo! claimed that it was not obliged to disclose identification data to the public prosecutor.

Yahoo!'s argument was not followed by the Criminal Court of Dendermonde but Yahoo! successfully challenged the decision before the Court of Appeal of Ghent. However, the public prosecutor lodged an appeal before the Court of Cassation that, on 18 January 2011, found that the term "electronic communications service provider" set forth in Article 46*bis* of the CCP has an autonomous meaning. Therefore, it does not have the same meaning as is used in Article 2 of the BECA. In the Court's opinion, a provider of a service which allows its users to gather, disclose or distribute information by using an electronic communications network, is to be considered an electronic communications service provider within the meaning of Article 46*bis* of the CCP.

The case was then referred to the Court of Appeal of Brussels that, on 12 October 2011, held the view that the order had not been validly communicated to Yahoo!. In the Court's opinion, the mere fact that it is technically possible, amongst others, for the public prosecutor to contact Yahoo! from the Belgian territory by means of electronic or other means of communication, is not sufficient. However, the public prosecutor lodged a second appeal before the Court of Cassation that, on 4 September 2012, found that the circumstance that the public prosecutor sends his written request within the meaning of Article 46*bis* of the CCP, whereby the cooperation is required from an operator established outside the Belgian territory, from Belgium to a foreign address, does not render the request invalid. The case was then referred to the Court of Appeal of Antwerpen that confirmed the applicability of Article 46*bis* of the CCP and punished Yahoo! with a fine of 44.000 euros, whose 22.000 euros are conditional during three years. It's worth mentioning that, pursuant to the Court, if Yahoo! is not willing to comply with the requirements of Article 46*bis* of the CCP, it may decide to exclude IP-range from Belgium.

In its decision of December 2015, the Court of Cassation found that, unlike Yahoo!'s opinion, there was no issue of extraterritorial jurisdiction at stake. Indeed, according to the Court, the request for disclosure to an operator of an electronic communication network or an electronic communications service provider who is active in Belgium does not imply any intervention outside the territory of Belgium, such as sending civil servants abroad. Also, notwithstanding the place of location of such an operator or provider, its refusal to comply with such request constitutes an offence that takes place in Belgium. Finally, the Court of Cassation agreed with the Court of Appeal that Yahoo! "voluntarily" submits itself to the Belgian law because it actively participates in the economic life of Belgium, notably by using the domain name .be or by displaying ads based on the location of its users.

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

Nicolas Roland

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

FOCUS: BELGIUM

Failure to submit a notification as an electronic communication service provider does not constitute a violation of a public order provision

Pursuant to article 9 of the Act of 13 June 2005 on electronic communications (the "**Act**"), an electronic communication service provider (the "service provider") must submit a notification to the Belgian regulator (the Belgian Institute for Postal Services and Telecommunication, the "**BIPT**") before it can start to offer its services. In its decision of 6 November 2015, the Brussels Court of Appeal has ruled that this obligation does not constitute a provision of public order *("disposition d'ordre public"/"openbare order")*. Consequently, its violation does not trigger the nullity of the contracts entered into by the operator who failed to submit a notification in accordance with article 9 of the Act.

This judgment was rendered after an appeal was lodged by a company (the electronic communication service provider) which was convicted to reimburse certain fees paid by another company pursuant to their contract for the provision of telephony services. According to the first judge, failure to introduce a notification to the BIPT as an electronic communication service provider must trigger the nullity of the contract.

The Court of Appeal overruled this decision. The Court of Appeal pointed out that the Act implements in Belgian law the new European regulatory framework on electronic communication services and networks of 7 March 2002. This European regime ensures the freedom of operators to provide electronic communications networks and services. It does so by prohibiting Member States to impose an authorization obligation on those operators. Nevertheless, Member States remain entitled to set up a notification process which does not depend on any explicit decision or any other administrative act by the national regulatory authority. In Belgium, such a possibility has been implemented in article 9 § 1 of the Act. However, the Court of Appeal noted that there is no sanction for notifications that are submitted late, i.e. after the service provider has started providing its services, neither in article 9 § 1 of the Act, nor in the Belgian Royal Decree of 7 March 2007 on the notification of electronic communication services and networks.

The Court of Appeal stressed that according to the Court of Cassation ("Belgian Supreme Court"), a rule can only be of a public order nature *("disposition d'ordre public"/"openbare order")* if it relates to essential national or collectivity's interests or to rules establishing, in private law, the legal basis of the society's moral or economic order. The Court of Appeal also referred to another decision by the Court of Cassation according to which the mere fact that the violation of an obligation is subject to criminal sanctions does not mean that the agreements entered into in violation of this obligation are null and void.

Finally, the Court of Appeal clarified the *ratio legis* of this notification obligation and explained that it only aims at identifying new operators before their national regulatory authorities, and not at demonstrating their capacity to offer electronic communication services. Following the above, the Court of Appeal concluded that the notification obligation does not constitute a rule of public order *("disposition d'ordre public"/"openbare order")*, and that its violation does not trigger the nullity of the agreements concluded by an operator which submitted such a declaration after the conclusion of agreements relating to electronic communication services. Such a civil sanction would indeed be disproportionate in light of the recent developments in the European regulatory framework of the electronic communication sector.

Carol Evrard

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

FOCUS: AMSTERDAM

Who owns the copyright in an app?

On 13 May 2015 the District Court in The Hague rendered a judgment in the case of X against Y on the alleged infringement of copyright in a web application ("app") that had been created for daycare centres.

Plaintiff X is the manager of Teddy Kids B.V. daycare centre. X wished to develop an app using graphics that give users insight into information on the children staying at daycare centres and on their parents. Also, information about the daycare centre's employees, such as their working schedules, could also be viewed via the app. Defendant Y is the manager of two Bulgarian companies that develop commercial software. X and Y entered into an agreement for the joint development of the so-called eKidz-app and the marketing thereof.

From October 2012 until April 2013, X and Y worked on the eKidz-app and field-tested it at X's daycare centre. The eKidz-app consists of two main elements: the *Grid View* (a user interface in the form of a grid with portrait photos of the accommodated children) and the *Teacher Planning* (a user interface showing the working schedules of the daycare centre's employees). In February 2013, Y registered the domain names ekidz.nl and e-kidz.nl.

In April 2013, Y terminated the cooperation it had with X and entered into negotiations with other partners for the marketing of the eKidz-app. A month later, Y denied X access to the eKidz-app and transferred the relevant files to another server.

In the dispute before the District Court, X stated that Y committed a contractual breach or had at least acted wrongfully towards him. He believed that Y had infringed his copyright in respect of the eKidz-app. X demanded that Y should therefore remove all the content relating to the eKidz-app from his servers and should inform third parties that the eKidz-app had been provided to Y without the permission of the copyright owner. Finally, X demanded that the domain name ekidz.nl be assigned to it and sought damages.

Firstly, the Court stated that an app can be eligible for copyright protection under Dutch law if it can be considered an *expression* in any form of a computer program. European case-law indicates that the overall concept of functionality of computer programs *as such* does not qualify as an expression of a computer program. However, the individual elements of a computer program may be eligible for copyright protection if they are original in the sense that they are the author's own intellectual creation. Subsequently, the Court pointed out that the eKidz-app consists of various elements (functionalities, source codes, and user interfaces) and that for each of these elements, it should be assessed whether it is copyright protected and whether X or Y is the rightful owner of the copyright.

The Court held that the functionalities, as a component of the eKidz-app, are not protected by copyright because they do not form an expression of the app. The individual functionalities *as such* could have been protected by copyright, but X did not make a claim on these grounds in the case here. In respect of the source codes, the Court held that they are protected by copyright. It also held that Y was the rightful claimant of these rights since they derive from his intellectual creation and he had made all creative choices related thereto. Furthermore, the Court found that X designed the *Grid View* and the *Teacher Planning* and, as such, X must be considered the owner of the copyright in these user interfaces.

Moreover, the Court ruled that the eKidz-app must be considered a combination of the source codes and the user interfaces. As such, the exploitation of the eKidz-app requires the consent of both copyright holders (Y in respect of the source codes and X in respect of the user interfaces).

In light of the foregoing, the Court concluded that Y had infringed X's copyright in the user interfaces by making the eKidz-app public to potential business partners without the prior consent of X. Therefore, Y has to pay compensation for the damage suffered by X as a consequence thereof. The damage will be assessed in subsequent hearings.

Y successfully disputed X's claim that X maade up the name eKidz and that X could claim any rights in respect of the domain name ekids.nl. Therefore, Y does not have to transfer this domain name to X.

In respect of X's claim of contractual breach, the Court held that Y failed to perform his obligations under the agreement with X (e.g., by removing the software from the server). Consequently, Y was liable for the damage suffered by X as a consequence of his non-performance. These damages will also be assessed in subsequent hearings.

Source: District Court, The Hague, 13 May 2015, ECLI:NL:RBDHA:2015:5598.

Elisa Hendriksen

Junior associate
T • +31 20 546 06 57
elisa.hendriksen@stibbe.com

FOCUS: AMSTERDAM

UN Convention on Contracts for the International Sale of Goods applies to certain software license agreements

The Canadian-based software supplier Corporate Web Solutions Ltd. ("CWS") and a Dutch customer concluded an online license agreement for software that can generate diagrams and other graphic reproductions of processes. The Dutch customer transferred his downloaded copy of the licensed software to the company Vendorlink B.V. of which he was a director. CWS objected to this transfer and decided to terminate the agreement with Vendorlink conditionally, insofar as a license agreement existed between CWS and Vendorlink. The dispute came before court, and the court had to determine whether the software license agreement qualified as a purchase agreement, and whether the right of ownership of the downloaded copy of the software had in fact passed to Vendorlink.

Since the software license agreement was an international agreement, the court discussed the applicability of the United Nations Convention on Contracts for the International Sale of Goods ("the Convention"). In its interpretation of the Convention, the court explained that it must take into account the international nature of the Convention, the need to promote uniformity in its application, and the observance of good faith in international trade. Furthermore, the *intention* of the parties with respect to their agreement was a decisive factor for its interpretation, not the *title* of the agreement. The court pointed out that the term "movable goods" in the Convention also includes intangible goods, such as downloaded copies of software. Therefore, software that is not delivered in a tangible form can be the object of a sales agreement, so software falls under the scope of the Convention.

The court then considered whether the license agreement qualified as a purchase agreement. To answer this, the court applied the guidelines in the *UsedSoft* case, which were set out by the European Court of Justice ("ECJ"). In the *UsedSoft* decision, the ECJ held that an agreement consisting of a (i) user right that is not limited in time, in return (ii) for payment of (ii) a one-time fee, can be qualified as a purchase agreement.

With respect to the CWS software license agreement, the court noted that the agreement was titled "license agreement". This license agreement stated explicitly that the software was licensed, not sold, and that the rights under the agreement could not be transferred. These terms therein indicate that it was CWS's intention to provide its customers with merely a right to *use* the software, not with the *ownership* of it. However, this intention was not apparent from the actual interpretation of the license agreement. After all, the right to use the software was not limited in time, which indicates that the agreement was a purchase agreement. Furthermore, the required fee for the software had to be paid once and in full. Therefore, the characteristics of the license agreement in question did not differ from those of a purchase agreement.

The fact that the software was transferred under the contractual restrictions in the license agreement, such as those pertaining intellectual property rights, did not preclude the transfer of ownership rights. In addition, the court held that CWS' retention of ownership by unlawfully terminating the license agreement was legally void. Referring to the *UsedSoft* judgment, the court reiterated that contractual clauses prohibiting the transfer of ownership completely, such as the clause set out by CWS in the license agreement, are not legally binding, hence void.

The court applied the *UsedSoft* requirements to the CWS international license agreement. It concluded that the software license agreement fulfilled the requirements of the Convention and therefore qualified as a purchase agreement of movable goods. The Dutch customer obtained the right of ownership of the copy of the software and could legally transfer his rights to Vendorlink. CWS' termination of the agreement therefore does not affect the ownership rights of Vendorlink in relation to the purchased copy of the software.

Source: District Court Mid-Netherlands 25 March 2015, ECLI:NL:RBMNE:2015:1096

This article was co-written by Friederike van der Jagt.

Joost van Eymeren

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

FOCUS: AMSTERDAM

Higher fines for privacy breaches and data breach notification duty enter into force on 1 January 2016

Recently the Dutch Senate passed the bill on data breach notifications and sanctions. This bill introduces higher fines for non-compliance with the Dutch Data Protection Act. In addition, companies will be obliged to notify the Dutch Data Protection Authority ("**DPA**") immediately of any data breach. Depending on the exact circumstances, data subjects will also have to be notified if their data are compromised. Non-compliance with privacy laws can lead to an administrative fine for each violation, the amount of which can be up to a maximum of EUR 810,000 or 10% of the company's annual net turnover. The new legislation will enter into force on 1 January 2016.

We see the media report increasingly about privacy sensitive information becoming publicly available because of a hack or security breach. With this new legislation, companies will be obliged to notify the DPA of any security breach in personal data protection "*that has or is likely to have serious negative consequences on the protection of personal data*" (new Article 34(a)(1) Dutch Data Protection Act). In addition to the duty to notify the DPA, the individuals whose personal data have been compromised must also be notified if "*there is reason to believe that the breach could have negative consequences on their privacy*" (new Article 34(a)(2) Dutch Data Protection Act). The practical implementation of these new provisions will be worked out in specific guidelines from the DPA. In any event, companies will be obliged to maintain an internal data breach register of any of the types of breaches mentioned above.

The new amendments to the Dutch Data Protection Act will allow the DPA to impose fines for the violation of a large number of general obligations (see the amended Article 66 of the Dutch Data Protection Act). These fines vary from a minimum of EUR 20,250, for relatively minor violations, to a maximum of EUR 810,000, for deliberate or repeated violations. For legal entities, the amount of the fine is not fixed: if the highest fine category is not sufficiently punitive, the violation can be sanctioned by a fine equal to 10% of the company's annual net turnover.

Fines may only be imposed on the company if a binding instruction given by the DPA is not followed. By way of such an instruction, the DPA can inform the company what steps it should take to avoid paying the fine. However, if the violation concerned was either intentional or a matter of serious culpable negligence, the DPA is not obliged to given any instruction and can impose a fine directly on the company. It is important that companies prepare themselves for these legislative changes. The following steps can help your company to do so:

Identify the different types of personal data processing and the related data retention policies within your company. Is it really necessary to process all those data, and are the retention policies adequate?

1. Check whether the level of data security is still adequate and whether your agreements with data processors need to be updated in order to ensure that they will inform you when a data breach occurs at their end.
2. Identify which (data) security breach notification duties apply to your company. Is this (merely) the general notification breach duty or might other sector-specific duties apply?
3. Set up a team that will be responsible for handling data breaches, and divide responsibilities amongst them, such as keeping an internal data breach register. The IT and legal departments should form part of this team.
4. Create privacy awareness within your company, for example, by providing data protection training. Be aware that technical measures do not necessarily prevent human errors. Employees should be made aware of the risks involved and their responsibilities when they work with personal data.

To summarize: prepare and be aware!

This article was written by Friederike van der Jagt. For questions, please contact Judica Krikke.

Judica Krikke

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

FOCUS: AMSTERDAM

Dutch Data Protection Authority imposes strict security requirements on absence management systems

The Dutch Data Protection Authority ("DPA") conducted an investigation recently into the security of the absence management systems Humannet Starter and Humannet Absence ("the absence systems"), both are staff absence management software solutions of IT company Humannet B.V. ("Humannet"). Humannet's customers (employers and those companies offering occupational health and safety services) use these software solutions for absence management of employees, including their re-integration following a sick leave period. For the purpose of absence management, medical data of employees are processed via these absence systems, and it is important for these data to be well protected. During a broadcast of the Dutch television programme ZEMBLA in 2012, it was evident that there had been a data leak in Humannet's absence systems. After the broadcast, the DPA made enquiries at Humannet promptly and then launched an investigation into the leak. The DPA concluded that Humannet's absence systems did not have an appropriate level of data security in place.

According to Article 1 of the Dutch Data Protection Act, Humannet's customers (i.e., the employers and those offering occupational health and safety services) can be qualified as data controllers for the processing of employee absence data. After all, Humannet's customers determine the *purpose* of the processing (absence management) and the *means* (the use of the absence systems) to achieve this purpose. Humannet qualifies as a data processor because the absence systems run on its self-managed servers. Further, Humannet has access (and can give third parties access) to the medical data it holds, and it can alter or delete the data. An element of managing the absence systems is the security thereof. The DPA emphasized that Humannet, as a data processor, has an active role in data security especially since specialized expertise concerning the complex automation of data is necessary. The customers' lack or absence of such expertise is the very reason why they hire specialized data processers. The DPA states: *"This active role involves responsibilities that it [the data processor] needs to fulfil actively, for instance in respect of sufficiently securing the processing of data that it manages or performs for the data controller."* Therefore, Humannet, despite being a data processor, is required to contribute to providing adequate data security actively for the absence systems in which medical data are being processed, and it should do this according to the appropriate technical and organizational measures as laid down in Article 13 of the Dutch Data Protection Act.

In its report, the DPA set out which appropriate technical measures Humannet must adopt. Humannet was obligated to apply so-called "multiple factor authentication" to all its customers. Humannet's systems were previously accessible by merely logging in with a user name and password ("one factor authentication"). Humannet had to add an extra factor, like a token, a smartcard (a personal access card), or a biometric characteristic to enable a person to prove his or her identity using another manner before gaining access to the absence system. Humannet must also continuously identify and list security risks. According to the DPA, Humannet must perform penetration tests and/or security scans several times a year. In doing so, vulnerabilities in the absence systems can be promptly identified and resolved. In response to the DPA's report, Humannet decided to offer its

customers “multiple factor authentication”, but it did not make this an element of its standard service. Furthermore, an audit was only performed once a year, and the results thereof were not properly addressed. The DPA therefore concluded that Humannet had violated Article 6 of the Dutch Data Protection Act, which states that personal data must be processed in a proper and careful manner and in accordance with the law, because Humannet did not take appropriate security measures, it failed to comply with Article 13 of the same Act, and therefore the processing of data was improper and careless.

For the definition of security measures, the DPA refers to the following as guidelines: its own Beveiliging van persoonsgegevens (Security of personal data, only available in Dutch), as well as the Code voor Informatiebeveilging (Code on Information Security (NEN-ISO / IEC 27002 2007 nl), the ICT-beveiligingsrichtlijnen voor webapplicaties (ICT security guidelines for web applications, only available in Dutch) issued by the National Cyber Security Centre, and the Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten (Reliability levels for authentication at electronic government service departments, only available in Dutch) issued by the Forum Standardization.

Noteworthy is that the security guidelines from other industries and security guidelines whose accessibility is conditional on payment were referred to by the DPA in its interpretation of Article 13 of the Dutch Data Protection Act. Controllers and processors therefore need to be aware of security guidelines besides those that are relevant for their respective industry when considering security measures.

Meanwhile, Humannet has implemented the necessary adjustments, and the DPA has decided to not take enforcement action. The investigation gave the DPA cause to send letters to 53 administrators of absence systems, drawing attention to the appropriate interpretation of the security requirements under the Data Protection Act. The letter, in addition to the investigation, states explicitly that if an administrator wants to test or develop its system further, no medical data can be used for that, but only dummy or anonymized data. Furthermore, the risks of the open fields in the system must be addressed. In these open fields, an employer may specify information on the nature and cause of the employee’s illness. However, an employer is not allowed to process such data. To prevent such processing, the DPA has warned against building open fields into the systems. Moreover, it has to be guaranteed that the employer cannot access the data that are being processed by the company doctor. It is therefore crucial that the administrator of the absence system—and not the employer— provide the login codes. The DPA has indicated that it will not hesitate to take enforcement action if it suspects that absence administrators are not complying with the law.

Source: DPA June 2015, z2012-00288, see: https://cbpweb.nl/sites/default/files/atoms/files/rapport_definitieve_bevindingen_humannet_15122014_openbare_versie_01062015.pdf. The letter to the administrators can be viewed on https://cbpweb.nl/sites/default/files/atoms/files/brief_aan_beheerders_28052015_def_openbare_versie.pdf.

This article was co-written by Friederike van der Jagt.

Joost van Eymeren

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

Stibbe

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
P.O. 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 10 Level 3 Unit 12
P.O. Box 506912
Dubai
United Arab Emirates
T • +971 4 401 92 45
F • +971 4 401 99 91

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
53 New Broad Street
London EC2M 1JJ
United Kingdom
T • +44 207 151 09 20
F • +44 207 151 09 30

New York

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