crowell moring

# CLIENT ALERT

## European TMT & Privacy Bulletin - February 2012

**Feb.28.2012**

*Sections of this issue:*

**ISP-Liability & Media Law**

- Court of Justice clarifies scope of copyright protection for portrait photographs
- Blocking measures imposed on Dutch ISPs with respect to The Pirate Bay
- The Court of Justice of the European Union (CJEU) issues its decision in the Sabam v. Netlog case (C-360/10) and further defines the scope of injunctions against ISPs

**Privacy & Data Protection**

- EU Commission proposes new Data Protection Regulation including various new obligations for companies and stringent enforcement rules

**Contracts & E-Commerce**

- The European Commission still undecided over Statement of Objections against Google

---

### ISP-LIABILITY & MEDIA LAW

#### Court of Justice clarifies scope of copyright protection for portrait photographs

*On 1 December 2011, the Court of Justice of the European Union (CJEU) ruled on a preliminary reference from an Austrian Court with regard to the existence and scope of copyright protection for portrait photographs and certain exceptions thereto. While some of the answers given by the Court may be considered to be all too narrowly focused on the specific facts of the case or deferred to the judgment of the national court, the Court also clearly establishes and confirms a few fundamental principles with regard to the subject.*

**The dispute in the main proceedings and the questions referred to the Court**

The reference for a preliminary ruling in this case was made by the Vienna Commercial Court (*Handelsgericht Wien*), before which proceedings were initiated by Ms Painer, a freelance photographer, against five newspaper and magazine publishers (hereinafter the "defendants"). The litigation concerned a claim by Ms Painer to have the defendants cease the reproduction

and/or distribution of a photograph and "photo-fit" (*cfr. infra*) without her consent and without indicating Ms. Painer as author, as well as a claim for damages.

The litigious photograph and "photo-fit" were those of Natascha K., an Austrian girl that was abducted at the age of 10 in 1998 and managed to escape from her abductor eight years later, in 2006. Following Natascha K.'s escape and prior to her first public appearance in the media, the defendants had published an old photograph of her, taken by Ms Painer prior to her abduction, as well as a "photo-fit," an computer-generated image on the basis of that photograph and intended to represent the supposed current image of Natascha K. at the age of 18. The defendants had, however, not indicated the name of the photographer in their publications or had indicated a name other than that of Ms Painer. In their defense before the Vienna Court, the newspapers claimed to have received the litigious photograph from a news agency without the (correct) name being mentioned.

Part of the case, namely the preliminary injunction proceedings, went all the way up to the *Obertser Gerichtshof* (Supreme Court), which ruled that the defendants did not need Ms Painer's consent to publish the photo-fit. Indeed, it ruled that the portrait photograph, which served as basis for the Photo-fit, only allowed for a small degree of individual formative freedom and hence could only benefit from a very narrow copyright protection. Moreover, the Supreme Court was of the opinion that the photo-fit was a new and autonomous work protected by copyright.

The Vienna commercial court, who had to hear this case on the merits, decided to stay the proceedings and refer a certain number of questions to the Court of Justice. For the purposes of the present newsletter, the following of those questions are relevant:

1. are photographic works, particularly portrait photographs, afforded weaker copyright protection or no copyright protection at all against adaptations because, in view of their realistic image, the degree of formative freedom is too small?;
2. does the public security exception to copyright protection (*e.g.* when using the work in the interest of criminal justice) require a specific, current and express appeal for publication of the image on the part of the security authorities, i.e. that publication of the image must be officially ordered for search purposes, or can the media rely on this exception and decide, of their volition, whether images should be published in the interest of public security, *e.g.* in order to trace a missing person?
3. can the quotation exception to copyright protection apply where the name of the author is not attached to the work or other protected matter quoted?; and

**The Court's answers**

**1)** According to the Court, a portrait photograph can be protected by copyright if - which is for the national court to determine in each case - it is an intellectual creation of the author reflecting his personality and expressing his free and creative choices in the production of that photograph.

When taking a portrait photograph, the photographer can stamp the work with his 'personal touch' by making free and creative choices in several ways at various points in its production:

- in the preparation phase : he can choose the background, the subject's pose and the lighting;
- when taking the photo : he can choose the framing, the angle of view and the atmosphere created; and

- when selecting the snapshot : he may choose from a variety of developing techniques or, where appropriate, use computer software.

With regard to the scope of the protection to be afforded to a portrait photograph, the Court reminds of its Infopaq-ruling (CJEU, 16 July 2009, *Infopaq /Danske Dagblades Forening*, C-5/08), in which it held that copyright protection must be given a broad interpretation in order for authors to receive an appropriate reward for the use of their works. Moreover, states the Court, nothing in the Copyright Directive supports the view that the extent of such protection should depend on possible differences in the degree of creative freedom in the production of various categories of works. Hence, once it has been determined that the portrait photograph in question is a work that can be copyright-protected, its protection cannot be inferior to that enjoyed by any other work, including other photographic works.

**2)** While it is conceivable that a newspaper publisher might, in specific cases, contribute to the fulfillment of an objective of public security by publishing a photograph of a person for whom a search has been launched, it should be required that such initiative is taken, within the framework of a decision or action taken by the competent national authorities and in coordination with those authorities, such in order to avoid the risk of interfering with the measures taken by them. However, it is not necessary to have an actual specific, current and express appeal, on the part of the security authorities, for publication of a photograph for the purposes of an investigation.

**3)** In principle, for quotations, the source, including the author's name, must be indicated, unless that turns out to be impossible. Here the Court rules that, since the defendants received the contested photographs from a news agency, it was legitimate for them to assume that this had been as a result of a lawful disposal. Second, the Court rules that the publication occurred within the context of a criminal investigation, as part of which, following the kidnapping of Natascha K. in 1998, a search notice was launched by the competent national security authorities, making it conceivable that it was the authorities who were the cause of the making available to the public of the contested photographs without the author's name. Hence, the subsequent use of those photographs by the press required the indication of their source but not necessarily the name of their author, since it had become impossible for them, in such a situation, to identify and/or indicate the author's name. In other words, here, the Court indirectly allows the defendants to benefit from the authorities' public security exception.

**Analysis and conclusion**

By explicitly ruling that the copyright protection of a work cannot vary depending on the degree of creative margin or originality, the Court rightly affords an identical protection to all protectable works. Indeed, for by doing so, it precludes both direct or indirect artistic valuation of the work within the context of a legal review of the facts, which has sometimes been the case in national legal proceedings in the past (*e.g.* as regards furniture or other functional works).

However, it seems that the Court also indirectly allows this protection to become somewhat diluted by affording a very broad exception margin to the newspaper publishers. First of all, it accepts all too easily that it 'must have been impossible' for the defendants to indicate the (correct) author's name when publishing the photograph under the quotation exception, since they received the contested photographs from a news agency and/or originally from the 'authorities'. However, it was not demonstrated that the photograph originated from the authorities. Moreover, the Court does not seem to take any account of the journalists' duty to verify the authenticity of their sources. In any case, nothing in the ruling indicates that the defendants would have even attempted to find out who the author of the work was, as one would expect them to do where no name was

mentioned. Second, it seems that the Court all too readily accepts the public security exception on the basis that the publication would have 'occurred within the context of a criminal investigation'. While it is conceivable that the criminal investigation and the victim search could have benefited from the defendants' publication of Natascha K's picture and/or photo-fit between 1998 and 2006, i.e. during her abduction, it is unclear how this could have been the case *after* her escape. Indeed, according to the ruling, the contested publication of the old photograph and the photo-fit occurred '*following Natascha K.'s escape and prior to her first public appearance in the media'*. This means that it occurred when the victim had already been recovered by the authorities and hence merely for the purposes of illustrating the news article, not with a view to helping the search party.

**References**: Full text of the CJEU's ruling in this case
Infopaq-ruling of the CJEU

---

**ISP-LIABILITY & MEDIA LAW**

**Blocking measures imposed on Dutch ISPs with respect to The Pirate Bay**

*After the ruling of the Antwerp Court of Appeal in September 2011, ordering two Belgian internet access providers to block access to several websites of "The Pirate Bay", the Court of First Instance of 's-Gravenhage recently issued a similar order vis-à-vis two Dutch internet access providers. The ruling of the Dutch court, however, goes beyond the scope of the Antwerp court order.*

**I. *Introduction***

1. By initiating legal proceedings in several European member states, IP right owners are leaving no stone unturned in their attempt to stop "The Pirate Bay," a filesharing website that offers around 3.5 million torrents linked to audio, video, games, software and e-books. The Court ordered Telenet and Belgacom, the two largest internet access providers in Belgium, to block access to 11 specified domains of The Pirate Bay. The Court expressly stated that Telenet and Belgacom complied with the injunction as soon as the blocking measure was implemented and that Telenet and Belgacom did not have an obligation to search for other websites under which The Pirate Bay is available to its users.

2. In the Netherlands, injunction proceedings were initiated by BREIN, a Dutch foundation protecting the interests of IP right holders, against the Dutch internet access providers Ziggo and XS4ALL to block the access to The Pirate Bay. The Court of First Instance of 's-Gravenhage issued its ruling on January 11, 2012.

**II. *The ruling of January 11, 2012***

3. The Dutch Court first considered that subscribers of Ziggo and XS4ALL commit copyright infringements by downloading and uploading unlawful information from the The Pirate Bay websites. The Court referred to studies from a Dutch consultancy bureau claiming that 90% to 95% of the torrents offered through The Pirate Bay contained unlawful information. Tests by BREIN also indicated that around 30% of Ziggo's subscribers and around 4.5% of XS4ALL's subscribers had recently downloaded illegal files from The Pirate Bay.

4. The Court then went on to consider that Ziggo and XS4ALL are intermediaries whose services are used to commit the infringements on the The Pirate Bay websites. With reference to the Dutch copyright Act, the Court therefore requires Ziggo and XS4ALL to cease these infringements by blocking their subscribers' access to the websites and IP addresses of The Pirate Bay. The Court not only specifies 3 IP addresses and 24 domain names of The Pirate Bay, but also orders Ziggo and XS4ALL to block access to any other IP address and domain name used by The Pirate Bay that would be communicated to them by BREIN.

**III. *Discussion***

5. The scope of the Dutch ruling goes beyond the injunction imposed on the Belgian ISPs.
First of all, the injunction is not limited to a blocking measure at DNS level (i.e. based on the domain names) but also imposes IP blocking (i.e. based on the IP address). This implies a higher risk of blocking lawful information. IP addresses are linked to hardware rather than websites. They can correspond to a server hosting several users or websites including perfectly legitimate ones.

6. Secondly, whereas the Antwerp Court expressly stated that Telenet and Belgacom complied with the injunction as soon as the blocking measure was implemented with regard to the websites mentioned in the injunction, the Dutch Court ruled that Ziggo and XS4ALL have to block access to any other IP address and domain name of The Pirate Bay that would be communicated to them by BREIN, and to keep the access blocked. This raises several issues.

7. The Court hereby authorizes BREIN to determine which IP addresses or domain names should be blocked by Ziggo and XS4ALL, without prior judicial review. Although the Court considers that, in case of erroneous information provided by BREIN, Ziggo and XS4ALL will not be liable and can initiate proceedings with respect to the execution of the ruling, it implies both granting important censorship-like powers to a private organization and the risk of blocking legal information.

8. Furthermore, Ziggo and XS4ALL are not only ordered to "block the access" to The Pirate Bay but also to "keep this access blocked". As the Court imposed penalties in case of non-compliance with the injunction, this raises questions as to the liability of Ziggo and XS4ALL. Indeed, as subscribers can easily circumvent a DNS or IP blocking measure (e.g. by changing the proxy server), the question is whether Ziggo and XS4ALL could in that case be forced to pay penalties even though they implemented the blocking measure. Such liability would be contrary to the exemption of liability granted to mere conduit providers by Article 12 of Directive 2000/31/EC. Moreover, the injunction would then amount to a general monitoring obligation which is contrary to Article 15 of Directive 2000/31/EC. The Antwerp Court removed any doubts in this regard by expressly stating that Telenet and Belgacom would be deemed to comply with the injunction as soon as the blocking measure was implemented. The Dutch Court failed to be so specific, despite the importance of this issue.

**IV. *Conclusion***

9. Both Ziggo and XS4ALL announced that they will lodge an appeal against the decision of the Court of 's-Gravenhage. It is therefore likely that the discussion with respect to the scope of the injunction will be continued before the Court of Appeal.

*For more information, contact: Karel Janssens*

---

**ISP-LIABILITY & MEDIA LAW**

**The Court of Justice of the European Union (CJEU) issues its decision in the Sabam v. Netlog case (C-360/10) and further defines the scope of injunctions against ISPs**

*On February 16, 2012, the CJEU issued its decision in the Sabam v. Netlog case. According to the Court, it is contrary to EU law to require a hosting provider to install a general filtering system in order to prevent that copyright infringing files are made available on its platform. The CJEU applied a similar reasoning as in the Sabam v. Scarlet case of November 24, 2011 (C-70/10), in which it ruled on an injunction requiring a mere conduit provider to implement a general filtering system.*

**I. *Background***

1. The reference for the preliminary ruling was made by the President of the Brussels Court of First Instance in proceedings between Sabam, a Belgian copyright collecting society, and Netlog, an online social networking platform.

2. According to Sabam, Netlog users were infringing copyrights in Sabam's repertoire by making protected works available to the public on their profile without Sabam's consent.

   Sabam asked the President of the Brussels Court of First Instance to order Netlog (i) to immediately cease unlawfully making available works from Sabam's repertoire and (ii) to introduce a system for filtering information stored on its platform in order to prevent that copyright infringing files would be made available.

**II. *The ruling of the CJEU***

3. The Court first considered that, in accordance with Article 8(3) of Directive 2001/29 and the third sentence of Article 11 of Directive 2004/48, holders of IP rights may apply for an injunction against operators of online social networking platforms, such as Netlog, who act as intermediaries within the meaning of those provisions, given that their services may be exploited by users of those platforms to infringe IP rights. The Court also referred to its case law stating that national courts must be able to order intermediaries to take measures aimed not only at bringing to an end infringements already committed, but also at preventing further infringements.

4. Nevertheless, the Court repeated that the provisions of Directive 2000/31 must be observed and more in particular Article 15(1) which prohibits national authorities from adopting measures which would require a hosting provider to monitor all the information it stores.

   The CJEU referred to the *Sabam v. Scarlet case*, in which it ruled that the prohibition of Article 15 applies in particular to national measures which require an online intermediary, such as a hosting provider, to actively monitor all the data of

each of its customers in order to prevent any future infringement of IP rights. Furthermore, such a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly.

Referring to *Promusicae* (Case C-275/06), the Court furthermore considered that national authorities and courts must strike a fair balance between the protection of the IP right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by ISPs.

5. As the injunction requested by Sabam, requiring the hosting provider to install a filtering system that would involve actively monitoring all or most of the information stored by the hosting provider, has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also works that have not yet been created, the Court concludes that it would result in a general monitoring obligation and in a serious infringement of the hosting provider's freedom to conduct its business. It would also require that hosting provider to install a complicated, costly, permanent computer system at its own expense, which would be contrary to the conditions laid down in Article 3(1) of Directive 2004/48.

   Moreover, as the injunction would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users, the injunction may also infringe these users' right to protection of their personal data. The injunction could also potentially undermine freedom of information, since the filtering system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.

6. Based on the foregoing, the CJEU concludes that, in adopting the injunction requiring the hosting provider to install the contested filtering system, the national court would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other. Directives 2000/31, 2001/29 and 2004/48 therefore preclude such an injunction.

**III. *Conclusion***

7. *Sabam v. Scarlet* and *Sabam v. Netlog* illustrate that the protection of IP rights must be balanced against the protection of other fundamental rights such as the ISPs' freedom to conduct a business and their users' right to protection of personal data and freedom to receive or impart information. National courts and authorities must not impose injunctions that imply a general monitoring obligation and that cannot be considered to be fair, proportionate and not excessively costly.

*For more information, contact: Karel Janssens*

## PRIVACY & DATA PROTECTION

**EU Commission proposes new Data Protection Regulation including various new obligations for companies and stringent enforcement rules**

On January 25, 2012, the EU Commission proposed a comprehensive reform of existing EU data protection rules.

Whereas the aim of the draft is to simplify existing legislation, which the draft does i.a. via the abolition of the obligation to notify all data processing to the various national data protection authorities, the draft does create several new rights for data subjects as well as new obligations for companies doing business in Europe. These may become very onerous for companies and may create new compliance concerns for multi-national operations.

The new obligations include an obligation to notify the national supervisory authority of serious data breaches without undue delay (if feasible, within 24 hours …) and the obligation to appoint a Data Protection Officer for companies employing 250 employees or more and for companies involved in "risky processing."

Also, whenever consent is required for data to be processed, it will have to be given explicitly, which may have a significant impact on current practices (where consent is often assumed or obtained implicitly, via general terms and conditions of sale).

The draft also provides for a general obligation on companies to adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the Regulation.

In case of violation, the draft Regulation introduces important (administrative) sanctions. For non-intentional first offences by certain controllers, the national supervisory authorities may still send a warning letter. For other violations and/or violations by certain other controllers, the supervisory authorities shall immediately impose penalties of up to €1 million or up to 2% of the global annual turnover of a company.

The EU Commission's proposals will now be passed on to the European Parliament and EU Member States (meeting in the Council of Ministers) for discussion. It is the EU Commission's intention to work closely with the European Parliament and the Council to ensure an agreement on the new data protection framework by the end of this year, but it is likely that this will take more time. The Regulation will enter into force the twentieth day after its publication in the EU Official Journal and take effect two years after that date.

It is likely that there will still be various changes to the present text. However, it is clear that the final text will in any event have a serious impact on the way companies doing business in Europe – including companies not established in the EU, but offering goods or services in the EU or monitoring the online behavior of citizens - will be able to process personal data.

**EU Commission proposes new General Data Protection Regulation including new obligations for companies and strong enforcement rules**

**1.** On January 25, 2012, the EU Commission proposed a comprehensive reform of existing data protection rules.

The core of the currently existing EU data protection legislation, EU Directive 95/46/EC, was adopted more than 15 years ago. At that time, the internet was still in its infancy. Technological progress and globalization have now profoundly changed the way personal data is processed and the amount of personal data that circulates around the globe. Moreover, the 1995 Directive has been implemented in the various Member States in different ways, leading to fragmentation and costly administrative burdens for companies, which currently still have to examine and comply with different obligations in the various Member States. Moreover, the powers of national data protection authorities are not harmonized enough to ensure consistent and efficient application of the rules.

This is why the EU Commission wants to update and modernize the principles enshrined in the 1995 Data Protection Directive.

With this proposal, the EU Commission wants to develop a stronger and more coherent data protection framework in the EU, backed by strong enforcement rules. The direct applicability of a Regulation should reduce legal fragmentation and provide greater legal certainty by introducing a harmonized set of rules.

The Regulation will apply to companies doing business in Europe, including companies not established in the EU, but offering goods or services in the EU or monitoring the online behavior of citizens.

**2.** Key changes in the proposed reform include:

***2.1. Scope***

- A **single set of rules** on data protection will be imposed via a Regulation valid across the EU and no longer via a Directive, which had to be implemented by the various Member States. This will put an end to the cumulative application of different national data protection laws.
- The new EU rules will apply to companies not established in the EU, when they offer goods or services in the EU or monitor the online behavior of citizens.

***2.2. A few important changes for companies doing business in the EU***

- The current obligation for companies **to notify all their data processing** activities to the various data protection supervisors in the different Member States is **removed**. According to the EU Commission, this simplification alone would result in net savings of €130 million per year in terms of administrative burdens alone. Whereas it may be true that the abolition of the notification duty may save money, we anticipate that cost for compliance with other obligations in the proposed Regulation may very well reverse those savings.
- Instead of the notification duty, the Regulation provides for increased **responsibility and accountability** for the entities processing personal data (as a controller or as a processor). For example, companies must **notify the national supervisory authority of serious data breaches** without undue delay (if feasible, within 24 hours …) and, if the data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the data subjects concerned. This obligation to notify serious data breaches within 24 hours (and to provide all the data required such as the details of the data lost, a description of the consequences of the breach and steps taken to mitigate those consequences), does not seem to be very realistic.

- Instead of having to deal with a national data protection authority in each Member State where a company does business, companies will only have to deal with **a single national data protection authority**, i.e. in the EU country where they have their main establishment.
- There will be a general obligation on companies to **adopt policies and implement appropriate measures** to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the Regulation. This will without a doubt lead to increased compliance costs.
- Companies employing 250 employees or more appoint a **data protection officer**. Companies which do not reach this threshold but which are involved in processing operations which, by virtue of their nature, their scope or their purpose, present specific risks to the rights and freedoms of individuals ("risky processing") should also appoint a data protection officer. A group of undertakings may appoint a single data protection officer.
- Companies involved in risky processing should also carry out an assessment of the impact of the envisaged processing operations on the protection of personal data ("**Data Protection Impact Assessments**").
- Wherever **consent** is required for data to be processed, it will have to be given ***explicitly***, rather than assumed as is sometimes the case now. This means that a data subject's consent should be based either on a statement or a clear affirmative action by the person concerned and should be given freely. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented in a form distinguishable in its appearance from this other matter. This means that current practices to obtain consent via statements in the general terms and conditions of companies, will no longer be sufficient.
- **Data flows to third countries outside the European Economic Area** will, according to the EU Commission, be made easier by reinforcing and simplifying rules on international transfers. However, the restriction of transferring personal data to countries outside the EEA that are not considered to provide an adequate level of protection (including the United States) is maintained.Next to transfers to countries covered by an adequacy decision of the EU Commission, transfers via appropriate safeguards (binding corporate rules, EU standard contractual clauses) are provided. There do not seem to be significant changes. The changes are, *inter alia*, that the EU Commission may recognize the adequacy of certain sectors within a third country.
- The "**privacy by design principle**" is introduced to make sure that data protection safeguards are taken into account at the planning stage of procedures and systems. Hence companies should, both at the time of the determination of the means of processing and at the time of the processing itself, implement appropriate technical and organization measures and procedures.
- Under the **'right to be forgotten'** data subjects will be able to ask for the deletion of their data if there are no legitimate grounds for retaining it. The controller, who has made the personal data public, will be under the obligation to take all reasonable steps to inform third parties which are processing such data, that a data subject requested them to erase any links to, or copy or replication of, that personal data. The controller who has authorized a third party publication of personal data shall be considered responsible for that publication.
- People will have easier **access to their own data** and be able to **transfer personal data** from one service provider to another more easily (**right to data portability**). They have a right to be provided with a copy of that data in a commonly used format.

### *2.3. Other important changes*

- The Members States, supervisory authorities and the EU Commission shall encourage the drawing up of **codes of conduct** intended to contribute to the proper application of the Regulation. Associations and other bodies representing categories of controllers or processors in one Member State may submit them for an opinion of the supervisory authority, and associations and other bodies representing categories of controllers or processors in several Member States may submit draft codes to the EU Commission which may adopt implementing acts which stipulate that these have general validity within the Union.
- The Members States and the EU Commission shall encourage the establishment of data protection **certification mechanisms** and of **data protection seals and marks**, allowing data subjects to quickly assess the level of data protection provided.
- The new Regulation focuses specifically on the protection of the **personal data of children**, for which specific conditions apply.
- A new **Directive** will apply general data protection principles and rulesfor **police and judicial cooperation** in criminal matters. The rules will apply to both domestic and cross-border transfers of data.

***2.4. Powers of the national data protection authorities - enforcement and judicial remedy***

- **The national data protection authorities** will be strengthened so they can better enforce the EU rules. The national data protection authorities will be **empowered to** i.a. (i) notify the controller or processor of an alleged breach and, where appropriate, order them to remedy that breach in a specific manner, (ii) order the controller or processor to comply with a data subject's request, (iii) warn or admonish the controller or processor, (iv) order the rectification, erasure or destruction of data when processed in breach of the Regulation, (v) impose a temporary or definitive ban on processing, (vi) suspend data flows to a recipient in a third country and (vii) **impose administrative sanctions** on companies that violate EU data protection rules.

  The latter can lead to penalties of up to €1 million or up to 2% of the global annual turnover of a company.

- Data subjects will have a **general right to judicial remedy** against controllers or processors if they consider that their rights have been infringed. Proceedings shall be brought before the courts of the Member State where the controller or processor has an establishment and, alternatively, before the courts of the Member State where the data subject has its habitual residence.
- Bodies, organizations or associations which aim to protect the data subject's rights shall have the right to initiate legal actions on behalf of one or more data subjects, which opens the door for **class actions**.

Although reducing complexity is one of the aims of the proposed Regulation, the present proposal seems to go too far in the direction of imposing yet another set of prescriptive measures towards companies.

It is the EU Commission's intention to work closely with the European Parliament and the Council to ensure an agreement on the new data protection framework by the end of this year. It is therefore likely that there will still be various changes to the present text. However, it is clear that the final text will in any event have a serious impact on the way companies doing business in Europe – including companies not established in the EU, but offering goods or services in the EU or monitoring the online behavior of citizens - will be able to process personal data. Businesses should already consider implementing systems and structures in line with what can be expected to become obligatory in the years to come.

The Regulation will enter into force the twentieth day after its publication in the EU Official Journal but will only take effect two years after that date.

For more information, see:
http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

*For more information, contact: Frederik Van Remoortel*

---

**CONTRACTS & E-COMMERCE**

**The European Commission still undecided over Statement of Objections against Google**

*The European Commission has been looking at Google's behavior since the end of 2010, after a number national competition authorities referred antitrust complaints against the search engine giant. In the meantime, several companies have decided to file complaints with the EU Regulator directly. To date, the Commission has not yet issued a formal Statement of Objections against Google. It is expected to decide whether or not to do so by the end of March.*

In November 2010, the European Commission opened an investigation into potential abuse of dominance by Google on the internet search and advertising markets. Since then, several companies have filed formal complaints against Google directly. Some complainants – such as Ciao, Euro-Cities, Foundem and Microsoft – have publicly declared their interest, while others have not. However, in a recent report, Google revealed the identity of these other complainants. They are: the French company Interactive Labs, the German listings association VfT, the Italian website NNTP.it, the German mapping firm Hot-Map, and the Dutch football website Elfvoetbal.

Many of the complaints concern allegations that Google gives preferential treatment to its own services in its search results. Michael Weber, director of the German mapping firm Hot-Map, for instance gives the following explanation for its complaint: "*Google Maps API, which is licensed free of charge to a mass of websites around the world, leaves no more income to be made for cartographers on the web or on mobile devices, and Google's universal search always prioritises Google Maps, taking almost all of the possible traffic away from other online cartographers*".

Preferential treatment of Google's own services was also the reason the French shopping-comparison site Twenga filed its recent complaint with the European Commission. Twenga alleges that Google is manipulating its search algorithm in order to give preference to its own shopping services, resulting in the discriminatory downgrading of competitors in search results. While this problem may have existed since the beginning of 2011, it is alleged to have increased since the introduction of a new program - known as Panda -, causing Twenga to file an antitrust complaint with the Commission in January 2012.

The European Commission is still investigating the various complaints against Google. In a letter of January 2012, Competition Commission Joaquín Almunia, while recognizing the need "*to intervene in a timely manner in fast-moving sectors such as the ones in which Google is active,*" indicated that the Commission is not yet in a position to say whether it will issue a Statement of

Objections. However, according to the latest reports, the European Commission expects to decide by the end of March whether or not it will do so.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

**Thomas De Meese**
Partner – Brussels
Phone: +32.2.282.1842
Email: tdemeese@crowell.com

**Frederik Van Remoortel**
Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com