

The European Commission launched a drive in 2012 to modernise the European Union's (EU) data protection framework, the most far-reaching reform of EU data protection legislation in 20 years. The importance of personal data protection, an area of EU responsibility, to key business sectors and third countries across the globe has made this reform package one of the most important EU legislative files in the civil liberties area. The Court of Justice of the European Union contributed to the reform package by elaborating case law on a key aspect of the package: the requirement of independence for data protection authorities. Work originating in previous years in two other important areas remained on the EU's agenda in 2012: balancing security and privacy, especially in the context of data retention, Passenger Name Records (PNR) and biometric passports; and ongoing debates about the fundamental rights implications of developments in information and communication technology, including with respect to the Anti-Counterfeiting Trade Agreement (ACTA), social media and internet-based services.

## 3.1. Reform of EU data protection legislation

On 25 January 2012, the European Commission proposed the most important reform of EU data protection legislation in 20 years.

In its policy communication,¹ the European Commission explains that its main aim is to put individuals in control of their personal data. The Commission seeks to ensure that consent is given explicitly and freely when it is required; internet users have an effective right to be forgotten and a right to data portability; and administrative and judicial remedies serve to reinforce the rights of data subjects.

The European Commission also explains that it wants to ensure that data protection rules support a single digital market across the EU. The Commission is therefore proposing to lay down data protection rules at EU level through a regulation which is directly applicable in all Member States and does not require further

### 1 European Commission (2012a).

### Key developments in the area of information society and data protection

- EU institutions launch the most far-reaching reform of EU data protection legislation in 20 years and stress the need for uniform rules across the EU to regulate this policy area.
- Various voices raise concerns in a number of EU Member States about certain aspects of the European Commission's reform proposals, such as over-regulation or whether such proposals need to be made at EU level. They take issue, for example, with the Commission's decision to use a regulation, which sets immediately applicable rules, rather than a directive, which defines common minimum EU standards, but permits national implementation that takes into account different legal traditions.
- The Court of Justice of the European Union (CJEU) develops its line of jurisprudence on the complete independence of data protection authorities.
- The revision of the EU Data Retention Directive is postponed, while national implementing legislation continues to face constitutional challenges in a number of Member States. The CJEU is asked to deliver an opinion on the fundamental rights compliance of the Directive.

- The Council of the European Union reaches political agreement on the proposed PNR Directive, but the European Parliament suspends cooperation on a number of legislative files including this one during the second half of 2012, delaying the legislative procedure.
- The European Parliament rejects the ACTA, which means that neither the EU nor its individual Member States can join the agreement.
- The responsible national data protection authority audits
   Facebook at its European headquarters and expresses
   satisfaction at the progress achieved, but fundamental rights
   concerns persist in other EU Member States.
- A national data protection authority investigates Google's new privacy policy, pursuing a mandate from the Article 29 Working Party on behalf of the 27 EU Member States.

transposition into national law. Thus, the Commission wishes to achieve uniformity of the data protection legal framework across the EU and estimates that this would lead to net savings for companies of about €2.3 billion a year alone in administrative burdens. The Commission also wishes to simplify the regulatory environment by doing away with formalities such as general notification requirements; the Commission estimates that would lead to net savings of €130 million a year in administrative burdens. The Commission is also proposing to set up a 'one-stop-shop' system for data protection in the EU: data controllers (including natural or legal persons

and public authorities which determine the purposes, conditions and means of the processing of personal data) in the EU will deal with a single data protection authority (DPA) alone, namely the DPA of the Member State in which the company is based.

"In this new digital environment, individuals have the right to enjoy effective control over their personal information. Data protection is a fundamental right [...] and needs to be protected accordingly. Lack of confidence makes consumers hesitant to buy online and accept new services. Therefore, a high level of data protection is also crucial to enhance trust in online services and to fulfil the potential of the digital economy, thereby encouraging economic growth and the competitiveness of EU industries."

European Commission (2012), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding privacy in a connected world — A European Data Protection Framework for the 21st Century, COM(2012) 9 final, Brussels, 25 January 2012

All the main European bodies and institutions working in the field of privacy and data protection – the European Data Protection Supervisor (EDPS),<sup>2</sup> Article 29 Working Party,<sup>3</sup> the European Economic and Social Committee (EESC),<sup>4</sup> the Committee of the Regions,<sup>5</sup> the FRA,<sup>6</sup> the European Data Protection Commissioners,<sup>7</sup> the EU Member States and different associations and non-governmental organisations active in the field of data protection<sup>8</sup> – have commented on the proposed reform. FRA submitted an opinion on the fundamental rights aspects of the reform package at the request of the European Parliament (see box p. 74).

Table 3.1: Elements of the data protection reform package

EU instrument	Title	Reference
Communication	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, Safeguarding privacy in a connected world, A European Data Protection Framework for the 21st century	COM(2012) 9 final, Brussels, 25 January 2012
Draft regulation	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)	COM(2012) 11 final, Brussels, 25 January 2012
Draft directive	Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data	COM(2012) 10 final, Brussels, 25 January 2012

EDPS (2012a).

<sup>3</sup> Article 29 Data Protection Working Party (2012a) and Article 29 Data Protection Working Party (2012b).

<sup>4</sup> European Economic and Social Committee (2012).

<sup>5</sup> Committee of the Regions (2012).

<sup>6</sup> FRA (2012a).

<sup>7</sup> European Data Protection Commissioners (2012).

<sup>8</sup> European Digital Rights (EDRI) (2012a) and EDRI (2012b).

The EDPS welcomed the regulation, which sets immediately binding standardised rules for all EU Member States, because it will eliminate differences in the current national implementing laws. The rules will strengthen the rights of individuals and make those who control personal data more accountable for how they handle such data. The regulation also reinforces the role and powers of national data protection authorities by empowering them to issue significant fines. The EDPS is particularly pleased to see that the instrument of a regulation is proposed for the general rules on data protection.

The EDPS expressed concerns that the European Commission has chosen to regulate data protection in the law enforcement area through a separate, self-standing legal instrument that provides less protection than the proposed regulation. The EDPS also remarked that the main overall weakness of the data protection package is that it fails to remedy the patchiness of EU data protection rules. According to the EDPS, the reform package leaves many EU data protection instruments unaffected, such as the data protection rules for EU institutions and bodies. It also leaves aside all specific instruments adopted in the area of police and judicial cooperation in criminal matters, such as the rules on Europol and Eurojust and the Prüm Decision.9

The data protection reform was on the agenda of the Informal Meeting of the Justice and Home Affairs Ministers which took place in Nicosia on 23–24 July 2012.¹º The main discussion points were the potential to further develop the digital single market without imposing disproportionate administrative burdens on those processing personal data; and a review on a case-by-case basis of the empowerment of the Commission to adopt the delegated and implementing acts contained in the proposals.¹¹

In some EU Member States, especially in the national parliaments, the European Commission proposals raised concerns. One such concern related to the principle of subsidiarity, or whether such proposals needed to be made at EU level and might not better be addressed nationally, and another to the impression that the European Commission proposals were too far reaching and too detailed, thus posing the risk of overregulation.

These concerns were, for instance, voiced in **Belgium**, 12 the **Czech Republic** (especially in relation to the draft

directive),<sup>13</sup> **Estonia**,<sup>14</sup> **Germany**,<sup>15</sup> **Slovenia**<sup>16</sup> and **Sweden**.<sup>17</sup> In **Lithuania**, in contrast, the prevailing view was that the proposals did not contradict the principle of subsidiarity.<sup>18</sup>

### **FRA ACTIVITY**

### Exploring fundamental right aspects of data protection

At its third annual Symposium in May 2012, FRA brought together 50 experts to focus on the fundamental rights dimension of the data protection reform package. The experts, who represented national government agencies and specialised bodies, international and non-governmental organisations, data protection authorities, universities and companies, split into three working groups at the symposium to examine:

- the 'right to be forgotten', which would allow people to require organisations that hold their data to delete them unless there are legitimate grounds to keep them;
- the right to portability, which would allow people to transfer their electronic information, such as a Facebook friend lists or iTunes music, to a competitor's account without hindrance;
- the independence and powers of data protection authorities; and
- profiling, which, according to the proposed regulation's definition, is a method that uses automated processing to evaluate personal aspects or analyse or predict a natural person's performance or behaviour.

For more information, see: FRA (2012), FRA Symposium report – European Union data protection reform: new fundamental rights guarantees, 10 May 2012, available at: http://fra.europa.eu/sites/default/files/fra\_uploads/2280-FRA-Symposium-data-protection-2012.pdf

In other Member States, the issue of subsidiarity was coupled with the perceived lack of consistency between the proposed regulation and the proposed directive. This and other arguments were often combined with the suggestion to adopt a single legal instrument instead; preferably a directive that would define common minimum standards, but permit better standards at national level. This line of argument surfaced in the

<sup>9</sup> EDPS (2012b).

<sup>10</sup> The agenda is available at: www.statewatch.org/news/2012/ jun/eu-jha-informal-jul-agenda.pdf.

<sup>11</sup> Cyprus, Cyprus Presidency of the Council of the European Union (2012).

<sup>12</sup> Belgium, Chamber of Representatives (2012).

<sup>3</sup> Czech Republic, Committee for EU Affairs of the Senate of the Parliament of the Czech Republic (2012).

<sup>14</sup> Estonia, State Chancellery (2012).

<sup>15</sup> Germany, Federal Council (2012).

<sup>16</sup> Slovenia, Ministry of Justice and Public Administration (2012).

<sup>17</sup> Sweden, Swedish Parliament (2012).

<sup>18</sup> Lithuania, Committee on Legal Affairs of the *Seimas* of the Republic of Lithuania (2012).

Czech Republic, 19 Estonia, 20 Germany, 21 Lithuania, 22 Slovenia 23 and Sweden. 24

#### **FRA ACTIVITY**

## Highlighting the fundamental rights implications of the proposed data protection reform package

The data protection reform package is the first legislation proposed since the entry into force of the Charter of Fundamental Rights of the European Union in 2009 that explicitly aims at comprehensively guaranteeing a fundamental right, namely the fundamental right to data protection. At the request of the European Parliament, FRA issued an opinion on the proposed EU data protection reform package, suggesting ways to strengthen its fundamental rights safeguards.

In its opinion, FRA suggests inserting a general fundamental rights clause and an explicit guarantee that delegated and implementing acts, which are specific legislative powers given to the European Commission, cannot limit fundamental rights in any manner contrary to Article 52 of the Charter, which sets out the scope and principles of Charter rights.

The opinion also suggests concrete amendments to the draft text to ensure a better balancing of key fundamental rights, such as freedom of expression, freedom of the arts and sciences, freedom to conduct a business, the rights of the child or access to documents with the fundamental right of data protection.

Moreover, the opinion highlights the need to incorporate 'sexual orientation' into the list of sensitive data, thus qualifying it for a higher level of protection, with a specific reference to Article 21 of the Charter on non-discrimination to enable the collection of sensitive data for statistical research purposes, thereby clarifying the legality of such data collection to support the fight against discrimination.

For more information, see: FRA (2012), Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, FRA Opinion 2/2012, Vienna, 1 October 2012; available at: http://fra.europa.eu/sites/default/files/fra-opinion-data-protection-oct-2012.pdf

Another strand of argument focused on the economic impact of the proposals, drawing attention to

19 Czech Republic, Senate of the Parliament of the Czech Republic (2012). the administrative burdens for the private sector and alleged excessive sanctions. These concerns were raised in the Czech Republic,<sup>25</sup> Estonia,<sup>26</sup> the Netherlands,<sup>27</sup> Slovenia,<sup>28</sup> Sweden<sup>29</sup> and the United Kingdom.<sup>30</sup>

Individual EU Member States gave specific topics special attention. For instance, in **Germany**, the Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) raised concerns that the proposed regulation would only oblige companies with more than 250 staff to appoint data protection officers, thereby only covering 0.3 % of companies in Germany.<sup>31</sup>

At the European Parliament, the responsible rapporteur presented a draft report on the draft directive forming part of the data protection reform package to the Civil Liberties, Justice and Home Affairs (LIBE) Committee.<sup>32</sup> The rapporteur for the draft regulation published his report on the draft regulation in January 2013.

While these discussions maintained momentum for the important process of modernising the EU data protection legislation, a similar process was also taking place in the Council of Europe, mainly in the Consultative Committee (T-PD) of the Convention for the Protection of Individuals, with regard to the Automatic Processing of Personal Data (hereafter referred to as 'Convention 108') which prepared the modernisation of Convention 108.<sup>33</sup>

The objectives of this modernisation exercise are to better address challenges for privacy resulting from the use of new information and communication technologies and to strengthen the potential of the Convention to serve not just as a European standard, but as a global standard as well, in the area of data protection.<sup>34</sup>

<sup>20</sup> Estonia, Estonian Data Protection Inspectorate (2012).

<sup>21</sup> Germany, Federal Commissioner for Data Protection and Freedom of Information (2012a).

<sup>22</sup> Lithuania, Committee on Human Rights of the Seimas of the Republic of Lithuania (2012).

<sup>23</sup> Slovenia, Ministry of Justice and Public Administration (2012).

<sup>24</sup> Sweden, Parliament (2012).

<sup>25</sup> Czech Republic, Senate of the Parliament of the Czech Republic (2012).

<sup>26</sup> Estonia, State Chancellery (2012).

<sup>27</sup> Netherlands, Minister for European Affairs and International Cooperation (2012), pp. 3–7.

<sup>28</sup> Slovenia, Ministry of Justice and Public Administration (2012).

<sup>29</sup> Sweden, Parliament (2012).

<sup>30</sup> United Kingdom, Ministry of Justice (2012).

<sup>31</sup> Germany, Federal Commissioner for Data Protection and Freedom of Information (2012a).

<sup>32</sup> European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2012a).

<sup>33</sup> Council of Europe, Bureau of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (2010).

<sup>34</sup> Council of Europe, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (2012).

#### **FRA ACTIVITY**

### Ensuring the independence of data protection authorities

The FRA opinion on the data protection reform package specifically addresses the independence of national data protection authorities. The opinion recalls that it would be advisable for the independence criteria to be detailed to guarantee their practical effectiveness, and to include a reference to the 'Paris Principles', which set forth the independence criteria for National Human Rights Institutions (NHRIs), and other available standards to offer a more comprehensive definition of independence.

The FRA opinion argues that while data protection authorities have a more focused and narrow mandate than NHRIs, both types of institutions are meant to function as independent monitoring bodies in the fundamental rights field.

The opinion lists the factors that ensure independence under the Paris Principles:

- pluralism in the composition of an institution, reflecting society's composition;
- a suitable infrastructure, in particular adequate funding and budget autonomy;
- a stable mandate of the institution's members expressed through appointment and dismissal conditions and the exclusion of voting rights for government representatives within the governing bodies of institutions.

Moreover, the opinion observes that the proposed consistency mechanism contained in the draft regulation gives the Commission not only the power to adopt a reasoned opinion aimed at the suspension of the draft measures of the national data protection authorities, but also the power to adopt implementing acts.

FRA concludes that these proposed powers of the Commission may be difficult to reconcile with the guarantees of independence under Articles 8 (3) and 47 of the Charter of Fundamental Rights of the European Union and other international standards of independence.

For more information, see: FRA (2012), Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, FRA Opinion–2/2012, Vienna, 1 October 2012; available at: http://fra.europa.eu/sites/default/files/fra-opinion-data-protection-oct-2012.pdf

# 3.2. Complete independence of Data Protection Authorities

The CJEU continued to develop the concept of complete independence of data protection authorities under EU law in 2012, further delineating the precise requirements regarding independence in relation to influence and supervision, for instance, in the case of the Austrian Data Protection Authority. The CJEU, which first dealt with this issue in *Commission v. Germany*<sup>35</sup> in 2010, stressed that although the Austrian authority enjoys functional independence – meaning that no instruction can lawfully be issued to it – this alone is insufficient to protect it from all external influence. The independence required under EU law is intended to preclude not only direct influence in the form of instructions, but also any indirect influence which may affect the DPA's decisions.<sup>36</sup>

"The independence required under the second subparagraph of Article 28(1) of Directive 95/46 is intended to preclude not only direct influence, in the form of instructions, but also, [...] any indirect influence which is liable to have an effect on the supervisory authority's decisions."

C/EU, C-614/10, European Commission v. Republic of Austria, 16 October 2012, paragraph 43 The European Commission also brought an action before the CJEU against **Hungary**, asking the court to declare that Hungary had failed to fulfil its obligations under the EU Data Protection Directive<sup>37</sup> by removing the data protection supervisor from office prematurely.<sup>38</sup> The case was still pending at the end of 2012.

### 3.3. Data retention

The EU Data Retention Directive,<sup>39</sup> which has been the subject of fundamental rights concerns ever since its adoption in 2006, promotes the fight against terrorism and serious crime through the retention of traffic (mainly traffic data on telephone calls made and received, emails sent and received and websites visited) as well as location data (mainly the telephone number or internet protocol address used).

The directive prescribes that the national laws of EU Member States must require providers of publicly available electronic communications services and public communications networks to retain traffic and location data for a period of between six months to two years from the date of the communication.

<sup>35</sup> CJEU, C-518/07, European Commission v. Federal Republic of Germany, 9 March 2010.

<sup>36</sup> CJEU, C-614/10, European Commission v. Republic of Austria,

<sup>37</sup> Directive 95/46/EC of the European Parliament and of the Council, OJ 1995 L 281.

<sup>38</sup> CJEU, C-288/12, European Commission v. Hungary, action brought on 8 June 2012.

<sup>9</sup> Directive 2006/24/EC of the European Parliament and of the Council, OJ 2006 L 105.

The transposition of the directive continued to face difficulties that resulted in proceedings both before the CJEU, and before national constitutional courts. On 11 July 2012, the European Commission brought **Germany** before the CJEU for only partially and insufficiently transposing the directive. <sup>40</sup> This followed a March 2010 German Federal Constitutional Court ruling in which it held that the Federal Republic's transposition measures were unconstitutional and void. Since then, Germany has failed to meet its obligation to transpose the directive in full, the European Commission argued. The European Commission contends that the CJEU should impose a penalty of €315,036.54 a day against Germany.

Separately, on 31 May 2012, the European Commission formally decided to end infringement proceedings against Austria, which had notified it that it had fully transposed the Data Retention Directive. The Commission also decided to withdraw the request for a penalty payment from the CJEU against Sweden while maintaining before the court the request sentencing Sweden to pay a lump sum for the directive's late transposition.<sup>41</sup>

In **Ireland**, the High Court referred a case to the CJEU with questions concerning the compatibility of the data retention directive with key fundamental rights, specifically freedom of movement, freedom of expression and the right to privacy, data protection and good administration.<sup>42</sup>

National Constitutional Courts became involved in Austria and in Slovakia. In **Austria** 11,139 persons filed a joint complaint to the constitutional court. <sup>43</sup> In December 2012, the Austrian Constitutional Court expressed doubts about the compatibility of the EU Data Retention Directive with the EU Charter of Fundamental Rights and referred the case to the CJEU. <sup>44</sup> Moreover, a petition with 106,067 signatures against data retention was submitted to the parliament. <sup>45</sup>

In **Slovakia**, a group of Members of Parliament filed a complaint against the national implementation of data retention before the Constitutional Court on 9 October 2012. The complaint asks the Constitutional Court to refer the case to the CJEU for a preliminary ruling, if necessary, questioning it on the validity of the Data Retention Directive.<sup>46</sup>

40 CJEU, C-329/12, European Commission v. Federal Republic of Germany, action brought on 11 July 2012.

41 European Commission (2012b).

- 43 Austria, AK Vorrat (2012a).
- 44 Austria, Constitutional Court (2012).
- 45 Austria, AK Vorrat (2012b).
- 46 EDRI (2012c).

In the **Netherlands**, the need to use data retention to solve serious crimes was questioned. The Ministry of Security and Justice invited Bits of Freedom, an organisation specialising in digital civil rights like data protection and privacy, to submit its review evaluating the Data Retention Telecommunication Act, which implemented the directive.<sup>47</sup>

Bits of Freedom points out that neither the Dutch government, nor the European Commission has been able to empirically prove that data retention has led to a significant increase in the number of serious criminal cases solved. The prosecution and secret services frequently seize data when competence is lacking and procedural safeguards are not met. Additionally, Bits of Freedom warns of function creep – the use of data for other purposes than those foreseen by law.<sup>48</sup>

### 3.4. Passenger Name Record (PNR) data

In 2011, the European Commission introduced a new proposal for a PNR Directive, <sup>49</sup> concerning data that include information such as passenger names and details on their contacts, ticketing and itinerary. The PNR Directive would complement the various PNR agreements with third countries.

The Council of the European Union reached a general approach on establishing an EU-PNR system in April 2012, which permitted the Council to start negotiations with the European Parliament under the ordinary legislative procedure. 50 The discussion in the Council touched, among other things, on two main issues.

The first concerned whether the proposed new rules should cover the collection of PNR data only for flights from and to third countries or whether they should also cover flights within the EU. The proposed compromise would allow, but not oblige, EU Member States to also collect PNR data concerning selected intra-EU flights. The proposed system potentially affects the right to privacy, the right to data protection and the prohibition of non-discrimination.

The second key question was the retention period of PNR data (whereas the Data Retention Directive discussed earlier traffic and location data concerns). The initial European Commission proposal provides for a total retention period of five years. After 30 days, however, the PNR data would have to be masked out, so that the recognisable person-related elements of the PNR would

<sup>42</sup> CJEU, C-293/12, Reference for a preliminary ruling from the High Court of Ireland, lodged on 11 June 2012 – Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Siochána, Ireland and the Attorney General, 25 August 2012.

<sup>47</sup> Netherlands, Bits of Freedom (2012), p. 1.

<sup>48</sup> *Ibid.*, pp. 2-9.

<sup>49</sup> European Commission (2011).

<sup>50</sup> European Commission (2012c).

no longer be visible to a 'front-desk' law enforcement officer but only to a few specially authorised individuals.

A number of EU Member States considered that this initial 30-day storage period was too short from an operational point of view. The Council agreed to prolong the first period of fully accessible data to two years and maintain the overall retention period of five years.<sup>51</sup>

In the European Parliament, the rapporteur of the committee responsible for this proposal, the Committee on Civil Liberties, Justice and Home Affairs (LIBE), presented a draft report on 14 February 2012<sup>52</sup> that agreed with the bulk of the European Commission's approach to the transmission and use of PNR data. The rapporteur also agreed that the Commission and law enforcement bodies had presented persuasive evidence of the PNR system's effectiveness and contended that such a system was necessary, proportional and of added value.

The rapporteur was convinced that the inclusion of intra-EU flights would add clear value. He proposed no changes to the controversial definitions of 'terrorist offence' and 'serious crime' or to the proposed retention period of five years in order to ensure the necessity and proportionality of the measure, but he did suggest adding a definition to clarify the term 'masking of data'.

Members of the LIBE committee tabled 489 amendments to his draft.<sup>53</sup> The Committee on Transport and Tourism<sup>54</sup> and the Committee on Foreign Affairs<sup>55</sup> also contributed opinions that differed substantially from the LIBE rapporteur's draft report and expressed caution regarding the proposal based on fundamental rights considerations.

In June 2012, the European Parliament suspended its cooperation with the Council of the European Union on the EU PNR dossier and four other legislative dossiers. <sup>56</sup> The work in the LIBE committee on the draft report only resumed towards the end of 2012.

### 3.5. Biometric passports

The EU Regulation on Biometric Passports<sup>57</sup> has raised fundamental rights concerns since its inception in 2004. In the aftermath of the tragic events of 11 September 2001, EU Member States asked the European Commission to take immediate action to improve document security. The Council of the European Union decided to integrate biometrics into European passports. Passports and travel documents now include a high-security storage medium for memorising computerised data, with sufficient capacity to guarantee the integrity, authenticity and confidentiality of the data included. The storage medium contains a facial image and two fingerprints.

On 12 June 2012, the **German** Administrative District Court of Gelsenkirchen referred a question for preliminary ruling to the CJEU, asking it to determine whether the EU Regulation on Biometric Passports was valid.<sup>58</sup> Some three months later, in September 2012, the highest **Dutch** administrative court also referred four cases to the CJEU, asking it whether the same regulation infringes citizens' right to privacy and whether the fingerprints could be collected if used only for passport or identity card issuance.

In all these cases, authorities refused to issue passports/ID cards to the applicants because they declined to provide their fingerprints.<sup>59</sup> The issue raises two key fundamental rights concerns: fingerprints are taken not just of suspects but of every citizen, raising questions of necessity and proportionality with regard to data protection and privacy protection; and concerns that these fingerprints are not used just to check the authenticity of identity documents but for other purposes as well.

In the Council of Europe, the 2005 progress report on the application of the principles of Convention 108<sup>60</sup> to the collection and processing of biometric data<sup>61</sup> is being updated in order to be in line with the modernisation proposals of Convention 108, as well as to deal with developments in biometric technology (see also

► Chapter 2 in this Annual report).

57 Council Regulation (EC) No. 2252/2004.

on 12 June 2012 - Michael Schwarz v

<sup>58</sup> CJEU, C-291/12, Reference for a preliminary ruling from the Verwaltungsgericht Gelsenkirchen (Germany) lodged on 12 June 2012 – Michael Schwarz v. Stadt Bochum, 8 September 2012.

<sup>59</sup> CJEU, References for preliminary rulings from the Raad van State (Netherlands) in C-446/12, Willems v. Burgemeester van Nuth lodged on 3 October 2012; C-447/12, H.J. Kooistra v. Burgemeester van Skarsterlân, lodged on 5 October 2012; C-448/12, Roest v. Burgemeester van Amsterdam, lodged on 8 October 2012; and C-449/12, van Luijk v. Burgemeester van Den Haag, lodged on 8 October 2012.

<sup>60</sup> Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 1981.

<sup>61</sup> Council of Europe (2005).

<sup>51</sup> Ibid.

<sup>52</sup> European Parliament, LIBE committee (2012b).

<sup>53</sup> European Parliament, LIBE committee (2012c).

<sup>54</sup> European Parliament, Committee on Transport and Tourism (2011).

<sup>55</sup> European Parliament, Committee on Foreign Affairs (2012).

<sup>56</sup> European Parliament (2012a).

# 3.6. The protection of intellectual property rights

## 3.6.1. Anti-Counterfeiting Trade Agreement (ACTA)

The Anti-Counterfeiting Trade Agreement (ACTA) is a controversial international trade agreement whose purpose is to establish international standards for intellectual property rights enforcement. The agreement aims to establish an international legal framework for combating intellectual Property Rights (IPRs) infringements, namely counterfeiting and copyright infringements on the internet (piracy). Establish the EU and its Member States, ACTA signatories are Australia, Canada, Japan, Mexico, Morocco, New Zealand, Singapore, South Korea, Switzerland and the United States.

"The goal of the ACTA negotiations is to provide an international framework that improves the enforcement of intellectual property right (IPR) laws. It does not purport to create new intellectual property rights, but to create improved international standards as to how to act against large-scale infringements of IPR."<sup>64</sup> For its opponents, ACTA is controversial for a number of reasons.<sup>65</sup>

ACTA is a mixed agreement – it contains different sets of provisions, which partly fall under the EU's exclusive competence and partly under its shared competence with Member States. 66 The entry into force in the EU, therefore, requires all EU Member States to ratify it and the European Parliament and Council of the European Union to consent to it. 67 On 26 January 2012, the EU and 22 EU Member States (excluding Cyprus, Estonia, Germany, the Netherlands and Slovakia which were "expected to do so on the completion of their respective domestic procedures") signed ACTA. 68

Due to the growing concerns, the EDPS issued a second opinion on ACTA<sup>69</sup> on 24 April 2012, complementing its earlier February 2010 opinion. The second opinion provides guidance on the privacy and data protection issues ACTA raises and assesses some of its legal provisions.

The opinion holds that ACTA fails to spell out precisely the measures to be deployed to tackle infringements of intellectual property rights on the internet, a failure which could have side effects on individuals' fundamental rights if the measures are implemented improperly. It underlines that many of the measures to strengthen the enforcement of intellectual property rights online could involve the large-scale monitoring of users' behaviour and of their electronic communications.

Because such measures intrude significantly into persons' private spheres, they should only be implemented if they are necessary and proportionate to the aim of enforcing intellectual property rights.

The opinion also argues that ACTA does not sufficiently take into account effective judicial protection, due process, the principle of the presumption of innocence, and the right to privacy and data protection.<sup>70</sup>

The Committee on International Trade delivered a negative recommendation concerning ACTA. The recommendation says that: "the intended benefits of this international agreement are far outweighed by the potential threats to civil liberties".71 The European Parliament received numerous petitions asking Members of the European Parliament to vote against ACTA. More than 2.8 million internet users from across the globe72 signed one of the petitions against ACTA.73 Those who signed the petitions fear that the agreement will pose a threat to a free and open internet.

In July 2012 the European Parliament rejected the agreement in plenary session. This rejection means that neither the EU nor its individual Member States can join the agreement.<sup>74</sup>

Although the European Commission has said it is convinced that ACTA is fully in line with EU standards and does not interfere with citizens' fundamental rights of freedom of expression and data protection, it nevertheless asked the CJEU on 10 May to rule on whether ACTA violates those rights and freedoms.<sup>75</sup> Whereas the European Parliament rejected ACTA, the European Commission still intends to seek the CJEU's legal opinion. However, on 19 December 2012, a Commission spokesperson announced that the Commission had decided to withdraw its referral to the CJEU.<sup>76</sup>

<sup>62</sup> European Parliament (2012b).

<sup>63</sup> ACTA is open for signatures until 1 May 2013 and it would enter into force in countries that ratified it after ratification by six countries.

<sup>64</sup> European Commission, Trade (2008); see also European Parliament (2012c).

<sup>65</sup> European Parliament, Directorate-General for External Policies, Policy Department (2011), p. 6.

<sup>66</sup> European Parliament (2012b).

<sup>67</sup> European Parliament (2012c).

<sup>68</sup> European Parliament (2012b).

<sup>69</sup> EDPS (2012c); see also EDPS (2012d).

<sup>70</sup> EDPS (2012e).

<sup>71</sup> European Parliament (2012c).

<sup>72</sup> European Parliament (2012d).

<sup>73</sup> Text of the petition available at: www.europarl.europa. eu/pdfs/news/public/focus/20120220FCS38611/20120220FCS38611\_en.pdf.

<sup>74</sup> European Parliament (2012b).

<sup>75</sup> European Commission (2012d); see also European Commission (2012e).

<sup>76</sup> See video at: www.youtube.com/watch?v=VCBTFh3IhQY.

# 3.6.2. CJEU analyses the limits of the protection of intellectual property rights

The CJEU also analysed the limits of the protection of intellectual property rights in 2012. In the Sabam (Société Belge des Auteurs, Compositeurs et Editeurs) case, the CJEU ruled that a social network "cannot be obliged to install a general filtering system, covering all its users, in order to prevent the unlawful use of musical and audiovisual work".77

Sabam, the Belgian society for collecting music royalties, brought the social network Netlog, which allows users to create and exchange content, to court to require it to install filtering systems aimed at preventing infringements on its website by Netlog's large Belgian membership. Sabam asked the **Belgian** Court to impose a penalty payment of €1,000 per day if the injunction was not respected. But much user-generated content re-works copyrighted material to produce new creations, making assessments of legality particularly difficult and inappropriate for automatic filtering systems.

On 10 July 2010, the Brussels Court of First Instance denied the penalty payment request and asked the CJEU to rule whether or not a national judge may require a hosting service provider to filter most of the information stored on its servers in order to identify electronic files containing musical, cinematographic or audiovisual work, and subsequently to block the exchange of such files. The injunction that Sabam requested covered all Netlog customers to avoid any potential future abuses.

On 16 February 2012, the CJEU decided that it is against EU law to order such a measure. The judgment contains important interpretations of the following fundamental rights: intellectual property; freedom to conduct a business; data protection and freedom of information. The court held that the protection of intellectual property is a fundamental right protected by Article 17 (2) of the Charter of Fundamental Rights of the European Union, but remarked that this right is not absolute. According to the court, an injunction requiring the installation of a filtering system is complicated and costly, and for this reason an infringement of the freedom to conduct a business of the hosting service provider protected by Article 16 of the EU Charter of Fundamental Rights. The court held that such a measure also infringes the fundamental rights of the users of the services of the hosting service provider, namely the protection of personal data protected by Article 8 of the Charter and freedom of information protected by Article 11 of the Charter. All these fundamental rights need to be balanced with the protection of intellectual property and can, as a consequence, serve as a justification for its limitation.

77 CJEU, C-360/10, Sabam v. Netlog NV, 16 February 2012.

"Indeed, the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified [...]."

CJEU, C-360/10, Sabam v. Netlog NV, paragraph 49

## 3.7. Social media and internet-based services

Social media and other internet-based services raise fundamental rights concerns regarding the scope of the data collected and their use, concerns which are not always clear to users of these services. The consent of users could, therefore, be called into question as they are not always fully informed and cannot always assess the consequences of their consent.

In 2012, the Council of Europe adopted two recommendations in this area: a recommendation on the protection of human rights with regard to search engines<sup>78</sup> and a recommendation on the protection of human rights with regard to social networking services.<sup>79</sup>

The latter recommendation specifically suggests that social networking services seek the informed consent of users if they wish to process new data about them, share their data with other categories of people or companies and/or use their data in ways other than those necessary for the specified purposes for which they were originally collected.<sup>80</sup>

### 3.7.1. Facebook

As Facebook's European headquarters is based in Dublin (Facebook Ireland), Irish data protection law is applicable to the social network's dealings with all its users in the EU. On 21 September 2012, the Office of the Irish Data Protection Commissioner published the outcome of its review of how well Facebook Ireland had implemented recommendations made in the commissioner's December 2011 audit, which had assessed Facebook Ireland's compliance with Irish Data Protection law and, by extension, EU law in this area.

The audit report finds that Facebook Ireland had implemented the great majority of the recommendations to the satisfaction of the commissioner, particularly in the following areas:

<sup>78</sup> Council of Europe, Committee of Ministers (2012a).

<sup>79</sup> Council of Europe, Committee of Ministers (2012b).

<sup>80</sup> Ibid.

- the provision of better transparency for users in how their data are handled;
- the provision of increased user control over settings;
- the implementation of clear periods for the deletion of personal data or an enhanced ability for the user to delete items;
- the enhancement of the user's right to have ready access to their personal data and the capacity of Facebook Ireland to ensure rigorous assessment of compliance with Irish and EU data protection requirements.

Those recommendations which Facebook Ireland had not yet implemented by the time of the audit report were highlighted with a clear timeframe for implementation.

"I am satisfied that the Review has demonstrated a clear and ongoing commitment on the part of Facebook Ireland to comply with its data protection responsibilities by way of implementation, or progress towards implementation, of the recommendations in the Audit Report. I am particularly encouraged in relation to the approach it has decided to adopt on the tag suggest/facial recognition feature by in fact agreeing to go beyond our initial recommendations, in light of developments since then, in order to achieve best practice."<sup>81</sup>

Billy Hawkes, Irish Data Protection Commissioner, 21 September 2012

The Irish Data Protection Authority invited the student group Europe-v-facebook.org, whose detailed complaints about Facebook Ireland were addressed as part of the audit, to indicate if the changes brought about by the audit dealt adequately with their complaints, and the group provided detailed comments. The group<sup>82</sup> concluded that the Irish Data Protection Authority had taken very important first steps but that full compliance with the law was not yet ensured. The group noted that the Irish Data Protection Authority did not have a technical expert or a single legally trained official while it faced "a whole armada of lawyers from Facebook".<sup>83</sup>

Not all data protection authorities in the EU shared the opinion of the Irish Data Protection Authority. The Independent Centre for Privacy Protection of Schleswig-Holstein, Germany, publicly criticised the Irish authority's audit report and announced that it would continue its efforts to ensure full compliance with the law.<sup>84</sup>

### Promising practice

## Providing data protection guidelines for direct marketing companies

The Estonian Data Protection Inspectorate has produced another update to its non-binding guidelines on data protection rules to help companies involved in direct marketing improve their practical implementation of these rules. The guidelines do not offer legal analysis; they aim instead to inform the data processors of their responsibilities in detailed and easy-to-understand language. The guidelines are intended to prevent breaches of data protection rules. Direct marketers have previously made use of earlier versions of the guidelines.

For more information, see: Estonian Data Protection Inspectorate, The use of electronic contact information in direct marketing. Guidelines, available at: www.aki.ee/download/2025/Elektrooniliste%20kontaktandmete%20kasutamine%20otseturustuses.pdf

### 3.7.2. Google

In March 2012, Google opted to merge 60 separate privacy policies for individual Google-owned sites into one single policy for all its services. The move allowed it to combine data from different sites – including YouTube, social network Google+ and smartphone system Android – in order to better target its advertising.

The Article 29 Working Party mandated the **French** data protection authority, Commission on Information Technology and Liberties (*Commission nationale de l'informatique et des libertés*, CNIL) to carry out an investigation into Google's new privacy policy. The EU Data Protection Authorities published their common findings in a joint letter on 16 October 2012.<sup>85</sup>

They established that Google's changes had neglected to give users an opt-out option. In addition, Google had failed to place any limit on the "scope of collection and the potential uses of the personal data", meaning that it might be in breach of several data protection principles, such as purpose limitation, data quality, data minimisation, proportionality and right to object. They further highlighted the wide range of potential uses that Google might have for the data, including product development or advertising. EU data protection laws place limits on such activities, they said.

Although Google has not been directly accused of acting illegally, EU Data Protection authorities have expressed concerns about "insufficient information to its users (especially its passive users)" and "about the

<sup>81</sup> Ireland, Office of the Data Protection Commissioner (2012).

<sup>82</sup> Europe-v-facebook.org (2012).

<sup>8&</sup>lt;sub>3</sub> Ibid

<sup>84</sup> Germany, Independent Centre for Privacy Protection Schleswig-Holstein (2012).

<sup>85</sup> Article 29 Data Protection Working Party (2012c).

combination of data across services".86 They therefore instructed Google to give clearer information about what data are collected for what purpose. They also instructed Google to: modify its tools in order to avoid excessive data collection and to take effective and public measures to comply quickly with the recommendations. Otherwise authorities in several countries could take action against it.87

### Promising practice

## Recognising the best and the worst in privacy and data protection

In Belgium, the NGOs Ligue des droits de l'Homme and Liga voor Mensenrechten gave awards in January for the best and worst annual initiatives in privacy and data protection. As innovations that threaten privacy enter society each year, an awards ceremony for the best and worst initiative, a Winston and a Big Brother, respectively, can serve as a useful watchdog. Nominees sent spokespersons to defend and justify their positions. Citizens can vote for their candidates. In 2012, the Belgian Data Protection Authority took part, as did the media.

For more information, see: www.bigbrotherawards.be/index.php/fr; www.liguedh.be; and www.mensenrechten.be

Following an investigation, <sup>88</sup> Google promised to delete collected data that remained from its Street View service as part of their Wi-Fi mapping exercise in the United Kingdom. This latter practice, which resulted in the gathering and storage of fragments of personal data including emails, complete URLs and passwords, raised fundamental rights concerns because under data protection principles only specific data for specific purposes may be collected.

The company, in a letter dated 27 July 2012 to the United Kingdom Data Protection Authority, the Information Commissioner's Office (ICO), admitted that a "small portion" of the information that had been collected from its Street View cars when they had toured the United Kingdom was still "in its possession". 89 In response, the ICO said it would examine the contents of the information Google had discovered. The ICO said that Google may have breached the terms of the agreement following a 2010 investigation into the issue.

86 Ibid.

"We are also in touch with other data protection authorities in the EU and elsewhere through the Article 29 Working Party and the GPEN [Global Privacy Enforcement Network] network to coordinate the response to this development. The ICO is clear that this information should never have been collected in the first place and the company's failure to secure its deletion as promised is cause for concern," the ICO added.90

### **Outlook**

EU institutions are expected to debate the reform of EU data protection legislation in 2013, particularly in the Council Working Party on Information Exchange and Data Protection and in the European Parliament's LIBE committee. It remains to be seen to what extent EU institutions will take up the fundamental rights concerns expressed by FRA, EDPS and Article 29 Working Party.

Besides the discussion surrounding this major reform package, more specific policy measures will also continue to dominate data protection debates.

Since the evaluation of the Data Retention Directive found that there was a need to clarify the relationship between the Data Retention Directive and Article 15 of the EU e-Privacy Directive 2002/58/EC, it is likely that the revision of the Data Retention Directive will only take place once the Data Protection Reform has been adopted.

With regard to the draft PNR directive, the European Parliament has ended its suspension of cooperation and the debate in the European Parliament will thus gain momentum in 2013. It remains to be seen if the LIBE committee, and the Plenary of the European Parliament, will align themselves with the draft report of the rapporteur and support the proposed PNR directive or oppose it on fundamental rights grounds.

Important signals can also be expected from the CJEU in Luxembourg. The CJEU is expected to deliver a judgment in the case against Hungary addressing once more the requirement of independence for data protection authorities and to further develop and elaborate its line of jurisprudence on this aspect of effective data protection in practice. Cases on data retention referred to the CJEU might offer further insights into the fundamental rights dimensions of this EU measure. Rulings concerning biometric passports will play an important role in determining the legality of including biometrics in EU passports and travel documents.

Apart from such developments in EU legislation, policies and case law, the wider public will continue to see debates on the data protection dimension of internet-based services.

<sup>87</sup> France, CNIL (2012).

<sup>88</sup> United Kingdom, Information Commissioner's Office (ICO) (2010).

<sup>89</sup> Letter of Google France SARL to ICO, available at: www. ico.gov.uk/news/latest\_news/2012/~/media/documents/ library/Corporate/Notices/20122707\_letter\_Google\_to\_ICO. ashx.

<sup>90</sup> United Kingdom, ICO (2012).

### References

All hyperlinks were accessed on 2 May 2013.

Article 29 Data Protection Working Party (2012a), Opinion 01/2012 on the data protection reform proposals, WP 191, Brussels, 23 March 2012, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191\_en.pdf.

Article 29 Data Protection Working Party (2012b), Opinion 08/2012 providing further input on the data protection reform discussions, WP 199, Brussels, 5 October 2012, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199 en.pdf.

Article 29 Data Protection Working Party (2012c), Joint letter by EU Data Protection Authorities, Brussels, 16 October 2012, available at: www.cnil.fr/fileadmin/documents/en/20121016-letter\_google-article\_29-FINAL.pdf.

Austria, AK Vorrat (2012a), '11.139 BürgerInnen klagen gegen die Vorratsdatenspeicherung', 15 June 2012, available at: www.akvorrat.at/node/61.

Austria, AK Vorrat (2012b), 'Nach Weiterleitung der Bürgerinitiative an den Justizausschuss: Arbeitskreis Vorratsdatenspeicherung reagiert mit noch mehr Bürgerbeteiligung', 4 June 2012, available at: www.akvorrat. at/BI-im-Justizauschuss-Mehr-Buergerbeteiligung.

Austria, Constitutional Court (*Verfassungsgerichtshof*) (2012), 'VfGH hat Bedenken gegen Vorratsdatenspeicherung und wendet sich an EuGH', Press release, 18 December 2012.

Belgium, Chamber of Representatives (2012), Subsidiarity Opinion (*Subsidiariteitsadvies*), Doc. 53, 2145/001, 6 April 2012.

Committee of the Regions (2012), *Draft Opinion of the Commission for Education, Youth, Culture and Research on the data protection package*, EDUC-V-022, Brussels, 6 July 2012, available at: http://cor.europa.eu/en/news/highlights/Documents/data-protection-package-draft-opinion.pdf.

Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 1981.

Council of Europe (2005), Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, available at: www.coe.int/t/dghl/standardsetting/dataprotection/Reports\_and\_studies\_en.asp.

Council of Europe, Bureau of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD-BUR) (2010), Report on the lacunae of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) resulting from technological developments (Part I), T-PD-BUR(2010)09, September 2010, available at: www.coe.int/t/dghl/standardsetting/dataprotection/tpd\_documents/T-PD-BUR\_2010\_09\_en.pdf.

Council of Europe, Committee of Ministers (2012a), Recommendation CM/Rec(2012)3 to member States on the protection of human rights with regard to search engines, 4 April 2012.

Council of Europe, Committee of Ministers (2012b), Recommendation Rec(2012)4 to member States on the protection of human rights with regard to social networking services, 4 April 2012.

Council of Europe, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (2012), Modernisation of Convention 108: Give us your opinion!, 29 November 2012, available at: www.coe.int/t/dghl/standardsetting/dataprotection/Consultation\_Modernisation\_Convention\_108\_EN.pdf.

Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, as amended by Regulation (EC) No. 444/2009 of the European Parliament and of the Council of 6 May 2009.

CJEU, C-518/07, European Commission v. Federal Republic of Germany, 9 March 2010.

CJEU, C-288/12, European Commission v. Hungary, action brought on 8 June 2012.

CJEU, C-614/10, European Commission v. Republic of Austria, 16 October 2012.

CJEU, C-329/12, European Commission v. Federal Republic of Germany, action brought on 11 July 2012.

CJEU, C-293/12, Reference for a preliminary ruling from the High Court of Ireland lodged on 11 June 2012 – Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, 25 August 2012, OJ 2012 C 258.

CJEU, C-291/12, Reference for a preliminary ruling from the *Verwaltungsgericht Gelsenkirchen* (Germany) lodged on 12 June 2012 – *Michael Schwarz v. Stadt Bochum*, 8 September 2012, OJ 2012 C 273.

CJEU, C-446/12, Reference for preliminary ruling from the *Raad van State* (Netherlands) lodged on 3 October 2012 – *Willems v. Burgemeester van Nuth,* 26 January 2013, OJ 2013 C 26.

CJEU, C-447/12, Reference for preliminary ruling from the *Raad van State* (Netherlands) lodged on 5 October 2012 – *H.J. Kooistra v. Burgemeester van Skarsterlân*, 26 January 2013, OJ 2013 C 26.

CJEU, C-448/12, Reference for preliminary ruling from the *Raad van State* (Netherlands) lodged on 8 October 2012 – *Roest v. Burgemeester van Amsterdam*, 26 January 2013, OJ 2013 C 26.

CJEU, C-449/12, Reference for preliminary ruling from the *Raad van State* (Netherlands) lodged on 8 October 2012 – *van Luijk v. Burgemeester van Den Haag*, 26 January 2013, OJ 2013 C 26.

CJEU, C-360/10, Sabam v. Netlog NV, 16 February 2012.

Cyprus, Cyprus Presidency of the Council of the European Union (2012), Informal Meeting of the Justice and Home Affairs Ministers, Data Protection Reform, Discussion Paper, 27 July 2012, available at: www.cy2012.eu/index. php/el/file/csP2tz62gFj2nxX09+AUZw==.

Czech Republic, Committee for EU Affairs of the Senate of the Parliament of the Czech Republic (Výbor pro evropské záležitosti Poslanecké sněmovny Parlamentu České republiky) (2012), Usnesení č. 213 z 27. schůze konané dne 5. dubna 2012 k Návrhu směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů /kód dokumentu 5833/12, KOM(2012) 10 v konečném znění/, Prague, available at: www.psp.cz/sqw/text/tiskt.sqw?o=6&v=VEZ&ct=213&ct1=0.

Czech Republic, Senate of the Parliament of the Czech Republic (Senát Parlamentu České republiky) (2012), Usnesení Senátu č. 614 ze 22. schůze, konané dne 24. května 2012 k novému rámci ochrany dat, senátní tisky č. N 144/08, N 145/08, 24 May 2012, Prague, available at: www.senat.cz/xqw/xervlet/pssenat/htmlhled?acti on=doc&value=64651.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks amending Directive 2002/58/EC, OJ 2006 L 105.

Estonia, State Chancellery (*Riigikantselei*) (2012), '*Eesti seisukohad isikuandmete kaitset puudutavate Euroopa Komisjoni algatuste suhtes*', available at: http://valitsus.ee/et/uudised/istungid/istungite-paevakorrad/57902/valitsuse-29.03.2012-istungi-kommenteeritud-p %C3 %A4evakord.

Europe-v-facebook.org (2012), 'Irish Data Protection Authority was unable to resolve privacy dispute. Austrian students are preparing to fight "Facebook" in courts', Media update, 4 December 2012, available at: www.europe-v-facebook.org/PR\_4\_12\_en.pdf.

European Commission (2011), Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 2 February 2011, available at: http://eur-lex.europa.eu/smartapi/cgi/sga\_doc?smartapi!celexplus!prod!DocNumber&lg=EN&t ype\_doc=COMfinal&an\_doc=2011&nu\_doc=32.

European Commission (2012a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, Safeguarding privacy in a connected world – A European Data Protection Framework for the 21<sup>st</sup> Century, COM(2012) 9 final, Brussels, 25 January 2012, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en: NOT.

European Commission (2012b), 'Data retention: Commission takes Germany to Court requesting that fines be imposed', Press release, 31 May 2012, available at: http://europa.eu/rapid/press-release\_IP-12-530\_en.htm.

European Commission (2012c), '3,162<sup>nd</sup> Council meeting Justice and Home Affairs Luxembourg, 26 and 27 April 2012', Press release, 26 April 2012, available at: http://europa.eu/rapid/press-release\_PRES-12-172\_en.htm.

European Commission (2012d), 'Overview of the European Commission's referral of ACTA to the European Court of Justice', Press release/Memorandum for publication, available at: http://trade.ec.europa.eu/doclib/docs/2012/may/tradoc 149464.doc.pdf.

European Commission (2012e), 'European Commission officially referred ACTA to the European Court of Justice, Statement by John Clancy, EU Trade Spokesman', News item, 11 May 2012, available at: http://trade.ec.europa.eu/doclib/press/index.cfm?id=799.

European Commission, Trade (2008), *The Anti-Counterfeiting Trade Agreement*, Factsheet, November 2008, available at: http://trade.ec.europa.eu/doclib/docs/2008/october/tradoc\_140836.11.08.pdf.

European Data Protection Commissioners (2012), Spring Conference 2012 of the European Data Protection Commissioners, Resolution on the European data protection reform, Luxembourg, 2–4 May 2012, available at: www.springconference2012.lu/files/7/3/document\_id29.pdf.

European Data Protection Supervisor (EDPS) (2012a), Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package, OJ 2012 C 192/05, Brussels, 30 June 2012. The full text of the EDPS Opinion is available at: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07\_EDPS\_Reform\_package\_EN.pdf.

EDPS (2012b), 'EDPS applauds strengthening of the right to data protection in Europe, but still regrets the lack of comprehensiveness', Press release, Brussels, 7 March 2012, available at: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-07\_DPReform\_package\_EN.pdf.

EDPS (2012c), Opinion of the European Data protection Supervisor on the proposal for a Council decision on the conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America, Brussels, 24 April 2012, available at: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-24\_ACTA\_EN.pdf.

EDPS (2012d), Meeting of the Committee on Civil Liberties, Justice and Home Affairs – Presentation of the second opinion of the EDPS on ACTA, 26 April 2012, available at: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-04-26\_Speech\_GB\_ACTA\_EN.pdf.

EDPS (2012e), 'ACTA measures to enforce IP rights in the digital environment could threaten privacy and data protection if not properly implemented', Press release, EDPS/09/12, Brussels, 24 April 2012, available at: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-09\_ACTA\_EN.pdf.

Estonia, Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) (2012), Andmekaitsereform laob ettevõtja õlule lisakohustusi, available at: www.aki. ee/est/index.php?part=events&id=562.

European Digital Rights (EDRI) (2012a), EDRI's initial comments on the proposal for a data protection regulation, 27 January 2012, available at: www.edri.org/CommentsDPR.

EDRI (2012b), *Data Protection Authorities*, available at: http://protectmydata.eu/topics/data-protection-authorities.

EDRI (2012c), 'Slovak Constitutional Court receives data retention complaint', EDRi-gram Newsletter, No 10.19, 10 October 2012, available at: www.edri.org/edrigram/number10.19/slovak-constitutional-court-data-retention.

European Economic and Social Committee (2012), Opinion on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final (COD), Brussels, 23 May 2012, OJ 2012 C 229/90, available at: www.eesc.europa.eu/?i=portal.en.soc-opinions.22438.

European Parliament (2012a), 'EP decides to suspend cooperation with Council on five JHA dossiers until Schengen question is resolved', Press release, 14 June 2012, available at: www.europarl.europa.eu/news/en/pressroom/content/20120614IPR46824/html/EP-suspends-cooperation-with-Council-on-five-justice-and-home-affairs-dossiers.

European Parliament (2012b), 'ACTA before the European Parliament', Press release, 4 July 2012, available at: www.europarl.europa.eu/news/en/pressroom/content/20120217BKG38488/html/ACTA-before-the-European-Parliament.

European Parliament (2012c), Recommendation on the draft Council decision on the conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America (12195/2011 – C7-0027/2012 – 2011/0167(NLE)), 22 June 2012, available at: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0204+0+DOC+PDF+Vo//EN&language=EN.

European Parliament (2012d), 'EP debates petitions against ACTA', News item, 20 June 2012, available at: www.europarl.europa.eu/news/en/headlines/content/20120615ST046956/html/EP-debates-petitions-against-ACTA.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2012a), Draft report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)), 2012/0010(COD), 20 December 2012, available at: www.

europarl.europa.eu/meetdocs/2009\_2014/documents/libe/pr/923/923072/923072en.pdf.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2012b), Draft Report on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record date for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 - C7-0039/2011 - 2011/0023(COD)), PE480.855vo1-00, 14 February 2012.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2012c), *Amendments 204-489*, PE486.159vo1-00, 28 March 2012.

European Parliament, Committee on Foreign Affairs (2012), Opinion of the Committee on Foreign Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 - C7-0039/2011 - 2011/0023(COD)), PE483.826vo2-00, 25 April 2012.

European Parliament, Committee on Transport and Tourism (2011), Opinion of the Committee on Transport and Tourism for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011)0032 – C7-0039/2011 – 2011/0023(COD)), PE467.175v02-00, 14 December 2011.

European Parliament, Directorate-General for External Policies, Policy Department (2011), *The Anti-counterfeiting trade agreement (ACTA): an assessment*, June 2011, available at: www.edri.org/files/DG\_EXPO\_ACTA\_assessment.pdf.

FRA (European Union Agency for Fundamental Rights) (2012a), Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, FRA Opinion 2/2012, Vienna, 1 October 2012, available at: http://fra.europa.eu/en/opinion/2012/fraissues-opinion-proposed-eu-data-protection-reform-package.

FRA (2012b), FRA Symposium Report – European Union data protection reform: new fundamental rights guarantees, 10 May 2012, available at: http://fra.europa.eu/sites/default/files/fra\_uploads/2280-FRA-Symposium-data-protection-2012.pdf.

France, Commission on Information Technology and Liberties (Commission nationale de l'informatique et des libertés) (CNIL) (2012), Appendix – Google privacy policy: main findings and recommendations, available

at: www.cnil.fr/fileadmin/documents/en/GOOGLE\_ PRIVACY\_POLICY-\_RECOMMENDATIONS-FINAL-EN.pdf.

Germany, Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) (2012a), 83<sup>th</sup> Conference of the Commissioners on Data Protection of the Federation and the Länder, *'Ein modernes Datenschutzrecht für Europa!'*, Press release, 22 May 2012, available at: www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2012/83\_DSK\_EinModernes-DatenschutzrechtFuerEuropa.html?nn=409394.

Germany, Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) (2012b), 'EU Datenschutz-Paket: Wichtiger Schritt zur Modernisierung des Datenschutzes', Press release, 25 January 2012, available at: http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2012/02\_EUDatenschutzPaket.html?nn=1091786.

Germany, Federal Council (Bundesrat) (2012), Beschluss des Bundesrates – Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Drucksache 52/12 (Beschluss) (2), 30 March 2012, available at: www.umwelt-online. de/PDFBR/2012/0052\_2D12B\_282\_29.pdf.

Germany, Independent Centre for Privacy Protection Schleswig-Holstein (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*) (2012), '*Irisches Facebook-Audit bestätigt nicht Datenschutzkonformität*', Press release, 21 September 2012, available at: www.datenschutzzentrum.de/presse/20120921-irischesfacebook-audit.htm.

Ireland, Office of the Data Protection Commissioner (2012), 'Report of review of Facebook Ireland's implementation of audit recommendations published – Facebook turns off tag suggest in the EU', Press release, 21 September 2012, available at: http://dataprotection.ie/viewdoc.asp?DocID=1233&m=f.

Lithuania, Committee on Human Rights of the Seimas of the Republic of Lithuania (*Lietuvos Respublikos Seimo Žmogaus teisių komitetas*) (2012), 'Specializuoto komiteto išvada Dėl Pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas) (ES-12-46)', 28 March 2012, available at: www3.lrs.lt/pls/inter3/dokpaieska.showdoc\_l?p\_id=421139&p\_query=bendrasis %2oduomen %F8 %2oapsaugos %20 reglamentas&p\_tr2=2, accessed on 17 September 2012.

Lithuania, Committee on Legal Affairs of the Seimas of the Republic of Lithuania (*Lietuvos Respublikos Seimo* 

Teisės ir teisėtvarkos komitetas) (2012), 'Specializuoto komiteto išvada Dėl Europos Komisijos Pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (toliau - Reglamentas) projekto ir Europos Komisijos Pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo arba baudžiamojo persekiojimo, arba bausmės vykdymo tikslais ir laisvo tokių duomenų judėjimo (toliau – direktyva) projekto atitikimo subsidiarumo ir proporcinguimo principams', 4 April 2012, available at: www3.lrs.lt/ pls/inter3/dokpaieska.showdoc l?p id=421568&p query=bendrasis %2oduomen %F8 %2oapsaugos %2o reglamentas&p\_tr2=2.

Netherlands, Bits of Freedom (2012), Letter to the Ministry of Security and Justice (Ministerie van Veiligheid en Justitie), Amsterdam, 21 June 2012.

Netherlands, Minister for European Affairs and International Cooperation (Staatssecretaris van Buitenlandse Zaken) (2012), Letter to the President of the Senate (Voorzitter van de Eerste Kamer der Staten-Generaal), No 22112-FI /33169, 2 March 2012.

Slovenia, Ministry of Justice and Public Administration (Ministrstvo za pravosodje in javno upravo) (2012), 'Sporočilo po seji Vlade RS dne 8. 3. 2012', Press release, 6 April 2012.

Sweden, Parliament (*Riksdag*) (2012), *EU proposal on the protection of personal data contrary to the principle of subsidiarity*, Decision of 29 March 2012, available at: www.riksdagen.se/sv/Debatter-beslut/Debatter-ochbeslut-om-forslag/Arendedebatter/?did=GZ01KU25&doctype=bet.

Netherlands, Minister for European Affairs and International Cooperation (Staatssecretaris van Buitenlandse Zaken) (2012), Letter to the President of the Senate (Voorzitter van de Eerste Kamer der Staten-Generaal), No 22112-FI /33169, 2 March 2012.

United Kingdom, Information Commissioner's Office (ICO) (2010), 'Information Commissioner announces outcome of Google Street View investigation', Press release, 10 November 2010, available at: www.ico. gov.uk/news/latest\_news/2011/~/media/documents/pressreleases/2010/google\_inc\_street\_view\_press\_release 03112010.ashx.

United Kingdom, ICO (2012), 'ICO statement on information received from Google about retention of Street View data', Statement, 27 July 2012, available at: www.ico.gov.uk/news/latest\_news/2012/statement-ico-response-to-information-received-fromgoogle-27072012.aspx.

United Kingdom, Ministry of Justice (2012), Summary of proposals – Call for evidence on the European Commission's data protection proposals, available at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe.