UN & CoE

January

February

March

1 April – CoE Committee of Minsters adopts Recommendation CM/Rec(2015)5 on processing personal data in the context of employment

21 April – CoE Parliamentary Assembly (PACE) adopts Resolution 2045 (2015) and Recommendation 2067 (2015) on mass surveillance

April

May – UN High Commissioner for Refugees publishes the Policy on the Protection of Personal Data of Persons of Concern to UNHCR

May

16 June – In *Delfi AS v. Estonia* (No. 64569/09), the European Court of Human Rights (ECtHR) rules that a company running an internet news portal is to be held liable for user-generated anonymous comments that amount to unlawful forms of speech, and that such liability is a justified and proportionate restriction on its right to freedom of expression (Article 10 of the ECHR)

23 June – PACE adopts Resolution 2060 (2015) on improving the protection of whistle-blowers

June

3 July – UN Human Rights Council appoints the first-ever Special Rapporteur on the right to privacy

July

August

September

27 October – 37th International Privacy Conference of Data Protection and Privacy Commissioners issues the "Amsterdam Declaration" on the oversight of intelligence services, stating that no single oversight model works for all states

October

November

1 December – In *Cengiz and Others v. Turkey* (Nos. 48226/10 and 14027/11), the ECtHR rules that a blanket order blocking access to YouTube unlawfully interferes with the applicants' rights to receive and impart information, guaranteed by Article 10 of the ECHR

4 December – In *Roman Zakharov v. Russia* (No. 47143/06), the ECtHR concludes that the lack of adequate and effective safeguards against arbitrariness and the risk of abuse inherent in the Russian law on secret interception of mobile telephone communications violate the applicant's rights under Article 8 of the ECHR

December

EU

January

February

2 March – European Data Protection Supervisor (EDPS) Strategy 2015–2019 summarises the main data protection and privacy challenges over the coming years, and specifies three objectives and 10 actions to address them

March

April

6 May – European Commission announces a Digital Single Market Strategy for Europe

May

15 June – Council of the European Union agrees on a general approach to the General Data Protection Regulation

June

July

August

8 September – EU and US finalise negotiations on the data protection "Umbrella Agreement", covering the exchange of data for law enforcement purposes

September

1 October – In *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság* (C-230/14), the Court of Justice of the European Union (CJEU) holds that a national data protection authority (DPA) has jurisdiction over companies processing data within the DPA's territory, even if the companies' headquarters are in another country

6 October – In *Maximillian Schrems v. Data Protection Commissioner* (C-362/14), the CJEU invalidates the European Commission's Adequacy Decision on the Principles of Safe Harbour and clarifies that the Commission's decision cannot prevent an individual from lodging a complaint or limit a DPA's powers to check whether a data transfer complies with Directive 95/46/EC

October

6 November – European Commission issues a communication to the European Parliament and the Council of the European Union, providing guidance on transatlantic data transfers and urging the prompt establishment of a new framework following the *Schrems* ruling

November

15 December – European Commission, Council of the European Union and European Parliament provisionally agree on the EU data protection reform package, which includes a General Data Protection Regulation and a directive on data protection in the police and criminal justice sectors

December

5 Information society, privacy and data protection

The terrorist attacks on the offices of Charlie Hebdo *magazine, a Thalys train and various locations throughout Paris in November 2015 intensified calls to better equip security authorities. This included proposals to enhance intelligence services' technological capacities, triggering discussions on safeguarding privacy and personal data while meeting security demands. EU Member States confronted this challenge in debates on legislative reforms, particularly regarding data retention. The EU legislature made important progress on the EU data protection package, but also agreed to adopt the EU Passenger Name Record (PNR) Directive, with clear implications for privacy and personal data protection. Meanwhile, the Court of Justice of the European Union (CJEU) reaffirmed the importance of data protection in the EU in a landmark decision on data transfers to third countries.*

5.1. Mass surveillance remains high on the agenda

5.1.1. United Nations and Council of Europe respond to surveillance concerns

After vocally condemning mass surveillance in recent years,[1] the United Nations (UN) in 2015 further underscored its commitment to protecting privacy at a global level: in July, the UN Human Rights Council appointed the first-ever UN Special Rapporteur on the right to privacy.[2] The Special Rapporteur, an independent expert 'body', will provide insights into key privacy issues relating to new technologies, the challenges confronted in the digital age, and human rights infringements by mass surveillance practices.[3] More specifically, the Special Rapporteur will address relevant issues at the international level by gathering information on national and international practices, making recommendations, exchanging information with stakeholders, singling out shortcomings and raising awareness regarding the effective promotion and protection of the right to privacy.[4] The mandate also includes reporting on violations of the right to privacy as protected by Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Joseph Cannataci, who was appointed as the first Special Rapporteur on the right to privacy, identified four areas as requiring particular attention: defining the notion of privacy, developing a universal surveillance law, challenging the conduct of global IT companies, and raising awareness among the public.[5]

At the European level, the Parliamentary Assembly of the Council of Europe (PACE) adopted two important resolutions in 2015: a resolution on mass surveillance[6] and a resolution on protecting whistle-blowers.[7] The resolution on mass surveillance acknowledges the need for "effective, targeted surveillance of suspected terrorists and other organised criminal groups". However, it also urges Member States to ensure that their intelligence services are subject to effective judicial and/or parliamentary oversight, and calls on them to protect whistle-blowers who expose illicit surveillance activity.[8] In addition, the resolution proposes developing an "intelligence codex" that outlines rules governing cooperation between intelligence services in the fight against terrorism and organised crime. The Committee of Ministers of the Council of Europe (CM) rejected this

last suggestion. Nevertheless, acknowledging FRA's work on the protection of fundamental rights in the context of large-scale surveillance, the CM emphasised its aim to intensify cooperation with EU bodies concerning such protection.[9]

The PACE resolution on improving the protection of whistle-blowers provides Member States with guidance on setting up comprehensive national frameworks to ensure the protection of public interest whistle-blowers, and emphasises that secrecy based on grounds such as "national security" does not justify covering up misconduct.

Reacting to revelations regarding cooperation between different intelligence authorities, such as the German *Bundesnachrichtendienst* (BND) and the US National Security Agency (NSA), various Council of Europe (CoE) bodies called for stronger parliamentary oversight of secret services.[10] The Commissioner for Human Rights advised CoE Member States to better equip national bodies in charge of overseeing intelligence services and to provide them with effective means for safeguarding human rights, particularly the right to privacy.[11] The commissioner indicated that the mere existence of a general parliamentary oversight body does not suffice. While acknowledging the role played by the existing oversight bodies in Germany, the commissioner also raised concerns about their powers, resources and technical expertise. In addition, the commissioner noted that the system's fragmentation and the absence of effective remedies also called for reforms.[12]

> *"Terrorism is a real threat and it requires an effective response. But adopting surveillance measures that undermine human rights and the rule of law is not the solution."*
>
> *Nils Muižnieks, Council of Europe Commissioner for Human Rights, 'Europe is spying on you', The International New York Times, 27 October 2015*

In December, the European Court on Human Rights (ECtHR) issued an important judgment that significantly clarified its case law on secret surveillance measures. In *Roman Zakharov v. Russia* (No. 47143/06),[13] the court thoroughly assessed Russian legislation on mobile phone interception and concluded that the law violated the applicant's rights under Article 8 of the ECHR (right to respect for private and family life). The decision particularly illuminated its case law on applicants' status as victim. Specifically, the court held that, where the applicable legal framework does not provide enough safeguards and effective remedies are absent at national level, it can assess the overall legal framework even when an applicant cannot prove that he or she was under surveillance.[14] *Zakharov* also reiterates the minimum safeguards to be set out in law to avoid abuses of power, and recalls the safeguards that secure proper limitation and supervision.

Minimum legal safeguards in secret surveillance

- Delimitation of the nature of offences that may give rise to an interception order
- Definition of the categories of people whose telephones may be tapped
- Time limit for the tapping of telephones
- Principles and safeguards for the processing of collected data as well as their transfer to third parties
- Criteria for the deletion of collected data
- Effective oversight mechanisms
- Availability of remedies

Source: ECtHR, Roman Zakharov v. Russia, *No. 47143/06, 4 December 2015, paras. 229–234*

5.1.2. CJEU and European Parliament emphasise rights protection

The 2013 revelations by Edward Snowden continued to prompt discussion at the EU level in 2015. The issue of data transfers to third countries received considerable attention, with a landmark CJEU ruling underscoring the importance of privacy safeguards in the EU.

Extensive and indiscriminate large-scale surveillance is often justified with references to national security, and the legal scope of that justification at EU level remains somewhat uncertain.[15] In October, the CJEU issued a decision – *Maximillian Schrems v. Data Protection Commissioner* (C-362/14) – that shed some light on the issue, focusing on situations involving personal data transfers to companies in third countries and subsequent access to the data by national intelligence services for reasons of national security.[16] Specifically, the court looked into personal data transfers to the USA on the basis of the European Commission's Safe Harbour Adequacy Decision,[17] which it retroactively invalidated.

Recalling its April 2014 decision in *Digital Rights Ireland and Seitlinger and Others* (C-293/12 and C-594/12) [18] – which invalidated the Data Retention Directive (2006/24/EC) – the CJEU assessed the lawfulness of interferences with fundamental rights when personal data are stored and accessed by national intelligence services. It held that:

> *"legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which*

to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail".[19]

The CJEU further held that legislation must provide effective oversight and redress mechanisms. An individual must be able to pursue legal remedies, either administrative or judicial, to access his or her own personal data and, if necessary, to obtain rectification or erasure of such data. Failing to provide these options compromises the essence of the right to an effective remedy enshrined in Article 47 of the EU Charter of Fundamental Rights. The CJEU also emphasised that data protection authorities (DPAs) play a vital role in ensuring compliance with data protection rules. Secondary legislation, such as the Commission's Safe Harbour Adequacy Decision, cannot limit the powers available to DPAs under Article 8 of the Charter and the Data Protection Directive (95/46/EC). Thus, even if the Commission's decision provides otherwise, DPAs must be able to examine, with complete independence, whether or not the transfer of personal data to a third country complies with the requirements laid down in EU law.

The *Schrems* case lent increased urgency to EU-US negotiations on a new data protection regime for transatlantic exchanges of personal data for commercial purposes. Sparked by the 2013 revelations on mass surveillance operations by the United States, and continuing ever since, the negotiations intensified during the last three months of 2015 – but no political agreement was reached by the end of the year.

While *Schrems* deals with the adequacy of levels of protection in a third country to which personal data are transferred in accordance with Article 25 of the Data Protection Directive, it entails broader consequences. The decision may also affect other international data transfer mechanisms – such as standard contractual clauses adopted by the European Commission to ensure adequate safeguards for personal data transferred from EU countries to countries that do not provide adequate data protection, and the binding corporate rules agreed on by a multinational group of companies regarding international transfers of personal data to such countries.[20] Following the judgment, the Article 29 Working Party – which brings together representatives of national data protection authorities, the European Data Protection Supervisor and the European Commission – pledged to examine the consequences of the judgment on these mechanisms. The Working Party also noted that it would take "all necessary and appropriate" actions, including coordinated enforcement actions, if no solution enabling data transfers while respecting fundamental rights was found with US authorities by January 2016.[21]

In the meantime, the European Parliament – which issued a resolution[22] on the matter in 2014 – continued to emphasise the importance of protecting EU citizens' fundamental rights in the context of mass

FRA ACTIVITY

In November 2015, FRA published a report on Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU. Drafted in response to the European Parliament's call for thorough research on fundamental rights protection in the context of surveillance, the report maps and analyses the legal frameworks on surveillance in place in EU Member States.

FRA's analysis draws on existing international human rights standards as developed by the UN and the Council of Europe, including the ECtHR. The report shows that intelligence services operate in very diverse settings and legal frameworks. It also summarises the various safeguards in place, and analyses the work of oversight bodies.

The report also outlines remedies available to individuals, and shows that the lack of an obligation to notify individuals that they are subject to surveillance, along with strict rules on providing evidence of being subject to surveillance, can make remedies ineffective. In a number of Member States, there either is no notification obligation or the obligation can be restricted on national security or similar grounds. Only 10 Member States have oversight bodies reviewing such restrictions.

To better understand how surveillance laws are implemented in practice and how privacy and data protection are guaranteed in the context of intelligence services' work, FRA launched a new study in December. The in-depth study will include fieldwork interviews with members of parliamentary committees, data protection supervisory authorities and other relevant national actors; the preliminary results should be available towards the end of 2016 or the beginning of 2017.

Source: FRA (2015), Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU, *Luxembourg, Publications Office.*

surveillance. Its 2014 resolution called for a full investigation by EU institutions, and urged Member States not to remain silent on the issue. In 2015, discussions focused on the measures taken by the Council and the Commission, as well as legislative reforms by Member States. In a follow-up resolution issued in October, the European Parliament deemed the Commission's actions in response to its 2014 resolution "highly inadequate given the extent of the revelations" and "call[ed] on the Commission to act on the calls made in the resolution by December 2015".[23] The European Parliament also called for a full investigation of the matter by national governments and parliaments, as well as EU institutions, and raised concerns regarding legal reforms in several Member States. The 2015 resolution also mentions FRA's report on surveillance – Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU[24] – with the European Parliament expressing its intention to consider the study's findings concerning the protection of fundamental rights, particularly regarding remedies available to individuals.[25]

5.1.3. EU Member States revisit their intelligence laws

A 2015 Eurobarometer survey on data protection showed that the protection of personal data remains a very important concern for European citizens. Technological developments and surveillance practices can threaten such protection. This reality prompted considerable discussion in 2015, and triggered important judicial decisions and legislative proposals. At the same time, many of the legislative reforms pursued throughout the year sought to extend the powers of intelligence services – a trend that intensified following multiple terrorist attacks.

Special Eurobarometer 431: data protection

According to the survey, only a minority (15 %) of Europeans feel they have complete control over the information they provide online; 31 % think they have no control over it at all. Two thirds of respondents (67 %) are concerned about not having complete control over the information they provide online. A majority of respondents are concerned about the recording of their activities via payment cards and mobile phones (55 % in both cases). The survey results show that half of Europeans have heard about revelations concerning mass data collection by governments. Awareness ranges from 76 % in Germany to 22 % in Bulgaria.

Source: European Commission (2015), Special Eurobarometer 431: Data Protection*, Brussels, June 2015*

In the **United Kingdom,** the 18-month inquiry conducted by the Intelligence and Security Committee (ISC) in response to the Snowden revelations came to the conclusion that the national legal frameworks needed reform. The ISC's findings were published in March 2015, mapping the relevant legislative frameworks and intelligence services' activities.[26] The report stated that the current law needed to be replaced by a more detailed and comprehensive act of parliament. A concurring report also called for reform.[27] In November, the government presented the Investigatory Powers Bill to parliament.[28] The bill aims to consolidate and update the surveillance powers of intelligence services while enhancing the safeguards in place. In particular, the bill would set up a 'double-lock' authorisation procedure through which warrants are administered by a secretary of state and must also be authorised by a judicial commissioner before coming into force.[29] Moreover, it distinguishes between targeted and bulk equipment interference, and includes safeguards to guarantee that bulk equipment interference is used in a proportionate manner and access to data is controlled.[30] The bill also intends to improve the system of judicial redress by introducing a domestic right of appeal to the Investigatory Powers Tribunal (IPT).[31]

Several other Member States – such as **Austria**, the **Czech Republic**, the **Netherlands**, **Poland**, and **Portugal** – began the process of reforming their intelligence laws.

The **Dutch** government in July published a draft bill to reform the Intelligence and Security Act 2002 that would extend the intelligence service's surveillance capabilities.[32] The draft law prompted criticism from the European Parliament because it would potentially infringe on fundamental rights.[33] Similarly, the **Austrian** government presented a bill to reform the surveillance powers of the intelligence service; the State Protection Act (*Staatsschutzgesetz*) is to constitute the federal law on the organisation, tasks and competences of the state protection authority (*Staatsschutz*).[34] In the **Czech Republic**, an amendment to the Act on Intelligence Services, which introduces new powers for intelligence services, came into effect on 25 September 2015.[35]

The constitutional court of **Portugal** ruled against some aspects of the national laws that allow specific surveillance measures. It deemed unconstitutional Article 78(2) of Parliament Decree No. 426/XII, a draft article that allows officials of the Portuguese Security Information Service and Defence Strategic Information Service to access metadata, such as traffic and location data.[36] The court established that, in light of technological developments, the concept of telecommunications includes metadata. Thus, access to metadata constitutes an interference with telecommunications. Furthermore, the court concluded that "prior authorisation" and the "mandatory Preliminary Control Commission" are not equivalent to existing controls in criminal proceedings and that the required constitutional guarantees were therefore not satisfied.

The *Charlie Hebdo* terrorist attacks hastened the adoption of a new intelligence law in **France**; the Law on Intelligence entered into force in July 2015.[37] The law was submitted to the constitutional court before its adoption, and the court found that most of it complied with the French Constitution. However, it did censure one draft article on international surveillance, stating that parliament had not determined in enough detail the fundamental rights guarantees to be provided to individuals in case of international surveillance.[38] Following the court's decision, parliament discussed a new draft bill on the surveillance of international electronic communication, and the new law – enshrining additional safeguards, including an authorisation procedure – was adopted in November.[39] In the meantime, the National Commission on Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement*, CNCTR), an oversight body set up by the new Law on Intelligence, began its work in October. By mid-December, it had received more than 2,700 requests for opinions on various surveillance techniques. According to the CNCTR, the so-called "black boxes" – the most controversial intelligence technique provided for in the new law – had not yet been used by then.[40] By mid-December, the prime minister also had not made use of the law's absolute emergency procedure (which does not require an *ex ante* CNCTR opinion), and had complied with all negative CNCTR opinions (about 1 % of the total).[41]

Following November's terrorist attacks in Paris, the French president ordered a state of emergency,[42] which was prolonged by law for an initial three-month period.[43] In December, the French government submitted to parliament a constitutional bill aiming to insert the state of emergency into the French Constitution.[44] While the state of emergency only marginally affects the powers of intelligence services, it significantly increases law enforcement's powers, especially regarding ordering house arrests for persons under suspicion. A large number of NGOs called for a prompt suspension of the state of emergency.[45] With the support of Defender of Rights (*Défenseur des droits*)[46] and the national human rights institution (*Commission nationale consultative des droits de l'homme*, CNCDH),[47] the Law Commission of the National Assembly established a continuous watch (*veille continue*) over the implementation of the state of emergency.[48] As a result, members of parliament regularly meet to discuss and assess the measures implemented by law enforcement agencies and call on the government to justify them.

The terrorist attacks that shook **France** in 2015 created a knock-on effect at both EU and national levels, prompting the Council of the European Union to reaffirm the fight against terrorism as a priority objective in the Renewed EU Internal Security Strategy for 2015–2020, and the governments of many Member States to launch efforts to expand security measures. These developments reinforce the need, consistently emphasised by FRA, to promote exchanges between actors to encourage promising practices. Legislative frameworks that govern intelligence services need to be adopted, strengthened, and periodically assessed. Effective oversight mechanisms are especially vital to ensure that powers do not become abusive and that intrusive methods are not legitimised.

5.2. Fostering data protection in Europe

5.2.1. Co-legislators reach agreement on reforming the EU data protection package

Following four years of negotiations, the European Parliament and the Council of the European Union reached an agreement on the reform of the EU data protection package in December.[49] Completing this reform was a key priority for 2015. The final texts are expected to be formally adopted by the European Parliament and Council in 2016, after which EU Member States will have two years before the new rules fully apply.

The new framework aims to give individuals control over their personal data and reduce the complexity of the regulatory environment for businesses.[50] It consists of two legal acts: a regulation establishing a general EU legal framework for data protection (General Data Protection Regulation, GDPR) and a directive on protecting personal data processed for purposes of preventing, detecting, investigating or prosecuting criminal offences and related criminal justice activities (Police Directive). The GDPR updates the principles set out in the 1995 Data Protection Directive (95/46/EC) – which it replaces – to keep pace with technological developments and changes in data processing, such as online shopping, social networks and e-banking services.[51] The regulation reflects some of the recommendations suggested by FRA in its 2012 Opinion on the data reform package. It provides for specific exemptions relating to freedom of expression, strengthens the right to an effective remedy, and enhances standing by enabling organisations acting in the interests of individuals to lodge complaints.[52] The Police Directive replaces the 2008/977/JHA Framework Decision on cross-border processing in police and judicial cooperation. It covers both domestic data processing and cross-border transfers of data, and sets a high level of data protection for individuals.[53] Figure 5.1 outlines the main elements of the new data protection package.

In an opinion issued in September, the European Data Protection Supervisor (EDPS) noted that reforming the regulatory framework was "a good step forward",[54] but emphasised that other aspects of the impact of a data-driven society on dignity need to be further addressed, and stated that legal frameworks need to be underpinned with an ethical dimension to ensure that human dignity is respected and safeguarded.[55] Towards the end of the year, the EDPS launched a call to establish an independent Ethics Advisory Group, which will be tasked with looking at the relationship between human rights, technology, markets and business models from an ethical perspective, paying particular attention to implications for the rights to privacy and data protection in the digital environment.[56] The members of the group will be announced at the end of January 2016.

On the international level, EU and US representatives initialled the EU–US data protection "Umbrella Agreement" in September.[57] The agreement covers transfers of personal data between the EU or its Member States and the USA for the purpose of law enforcement. It does not itself provide a legal basis for the data transfers, which should be established elsewhere, but specifies the data protection rules that apply to such personal data transfers. According to the Commission, the "Umbrella Agreement" intends

Figure 5.1: Main elements of the new data protection package

Empowerment of individuals

- Right of data subjects to know how their personal data are handled is augmented
- Data portability: transferability of personal data between service providers
- "Right to be forgotten" is clarified and codified through the introduction of a "right to erasure"
- Information about when personal data has been hacked, if the breach is likely to result in a high risk to the individual's rights and freedoms
- Non-profit organisations may represent individuals in exercising their rights with regard to administrative and judicial remedies

New rules for businesses

- One-stop-shop: businesses with establishments in more than one Member State will in many cases have to deal with one supervisory authority (lead supervisory authority) only
- European rules on European soil: companies based outside of Europe will have to apply the same rules when offering services in the EU
- Risk-based approach: no one-size-fits-all obligation, obligations now tailored to potential risks
- Data protection by design: the regulation guarantees that data protection safeguards are built into data processing from the earliest stage of development; producers of products and services are encouraged to take into account the right to data protection when developing new products and services that are based on or intended to process personal data
- No more obligation to notify data processing to supervisory authorities
- Obligation to notify data breaches to supervisory authorities, in some instances also to individuals
- Businesses are exempt from the obligation to appoint a data protection officer insofar as data processing is not their core business activity and this does not require regular and systematic monitoring of data subjects on a large scale, or the core business activities do not consist of processing on a large scale special categories of data. Other Union or national law may however extend this obligation.
- Businesses will have no obligation to carry out an impact assessment unless there is a high risk to individuals' rights and freedoms

Data protection in the area of law enforcement

- Law enforcement authorities (LEAs) can exchange information more efficiently and effectively
- LEAs must comply with the principles of necessity, proportionality and legality when processing personal data
- Supervision must be ensured by independent national data protection authorities
- Effective judicial remedies must be provided
- Rules for transfering personal data to third countries are clarified
- Member States may introduce a higher level of protection into their national laws

Source: *FRA, 2016; based on European Commission (2015), 'Agreement on Commission's EU data protection reform will boost Digital Single Market', Press release, 15 December 2015*

to set up a high-level data protection framework for EU–US law enforcement cooperation.[58] From a fundamental rights perspective, several clarifications are vital. In light of the CJEU's recent judgment in *Schrems* (C-362/14), it should be clarified that any onward transfer to, or access by, national intelligence services complies with the EU Charter of Fundamental Rights. In addition, it should be clarified that provisions that affect individuals, including those on judicial redress, do not apply only to nationals of the contracting parties, and generally comply with Articles 7, 8 and 47 of the Charter. Finally, because the agreement provides for independent oversight mechanisms, it should be ensured that these mechanisms are all completely independent in terms of their organisation – as required by the Charter, EU data protection legislation and CJEU jurisprudence.[59]

Promising practice

In **Poland**, the Inspector General for the Protection of Personal Data and the Chief of Police signed a cooperation agreement, agreeing to cooperate in the area of data protection and committing to helping each other in performing tasks set out in law. The cooperation covers research, educational, promotional and publishing activities. The partnership aims to exchange experiences and increase police officers' professional qualification in the area of data protection.

For more information, see 'The memorandum of cooperation of the Inspector General and the Chief of Police and the Police Academy in Szczytnie' *(Porozumienie o współpracy GIODO z Komendantem Głównym Policji i Wyższą Szkołą Policji w Szczytnie)*

5.2.2. Privacy strengthened in national legal frameworks

Several Member States reinforced their legal frameworks for data protection in 2015, either by introducing sectoral laws or by modernising their general legislation.

In **Belgium**, the recently appointed secretary of state for matters of privacy and data protection announced in June that he would present a new bill on privacy and data protection. On 16 December 2015, following the announcement of the agreement on an EU data protection regulation, he stated that he would not wait for the regulation to come into force, and that Belgium was already working on adapting its legislation to the regulation.[60] The Belgian regulation envisions granting the Belgian DPA (the Privacy Commission) the same status as a judicial body.

Malta adopted specific regulations in January 2015 that outline data protection rules for the educational sector.[61] In **Latvia**, the government on 12 May 2015 adopted the Cabinet of Ministers' Regulations No. 216 'On the procedure for preparing and submitting compliance assessment of personal data processing' (*Ministru kabineta noteikumi Nr. 216 "Kārtība, kādā sagatavo un iesniedz personas datu apstrādes atbilstības novērtējumu"*).[62] The regulations are binding for state and municipal institutions and private persons who have been delegated public administration tasks. The assessment allows individuals to ascertain whether existing personal data processing and protection complies with the regulatory framework, and whether the data processor really needs to undertake personal data processing for a specific purpose. It includes a risk analysis concerning the rights and freedoms of personal data subjects. The compliance assessment can be conducted by a data protection specialist or by persons who meet specific professional or academic requirements.

In **Germany**, the Second Act amending the Federal Data Protection Act (*Zweites Gesetz zur Änderung des Bundesdatenschutzgesetzes*) was adopted on 25 February 2015.[63] With this amendment, the Federal Commissioner for Data Protection and Freedom of Information becomes a supreme federal authority that enjoys the same status as, for example, federal ministries, the *Deutsche Bundesbank* or the Federal Constitutional Court once the act comes into force on 1 January 2016. The reform aims to guarantee the full independence of the Federal Data Protection Commissioner, who was previously attached to the Federal Ministry of Interior and under its administrative supervision.

In **Hungary**, the Information Act was extensively amended by Act CXXIX of 2015.[64] Modifications of the act include, among others, the establishment of binding corporate rules. In the **Netherlands**, the Senate in May adopted new legislation that amends the Personal Data Protection Law.[65] The new legislation obliges organisations – both public and private – that process personal data to report to the Dutch DPA (*College Bescherming Persoonsgegevens*, CBP) serious data breaches that result in the risk of loss or illegitimate processing of personal data. When a data breach has or may have negative consequences for those involved, organisations are also obliged to inform these individuals. The CBP may impose administrative fines on organisations that fail to report serious data breaches – an important legal change in the DPA's role. On 21 September 2015, the CBP published draft guidelines about this new obligation for consultation.[66]

In addition, several significant judgments were delivered in the course of 2015. One of these – *President of the Belgian Commission for the protection of privacy v. Facebook Inc., Facebook Belgium SPRL and Facebook Ireland Limited* (Case No. 15/57/C)[67] in **Belgium** – prompted a showdown between Belgian authorities and

the company. In June 2015, the president of Belgium's Privacy Commission revealed that a court proceeding had been launched against Facebook for breaching the Belgian Privacy Act by placing the so-called 'datr cookie' on the computers of people who were not members of Facebook when they clicked the 'Like' button on a website. In October, the chief of security at Facebook emphasised in an online article that the incriminated 'datr cookie' plays a fundamental role in protecting the online safety of Facebook and its users. Nevertheless, the president of the Tribunal of First Instance of Brussels in November issued a summary judgment ordering Facebook to stop tracking Belgian citizens who are not members of Facebook's social network within 48 hours. The tribunal found that the 'datr cookie' used by Facebook contains personal data, the collection of which constitutes the processing of personal data. In the court's view, processing such data for millions of Belgian non-members of Facebook clearly violates Belgian privacy law, irrespective of what Facebook does with the collected data. Furthermore, the tribunal rejected Facebook's argument concerning security, stating that any criminal can easily work around this and prevent the placement of this cookie, and that there are less invasive measures available to achieve Facebook's security objectives. Finally, the court held that the Belgian data protection law applies, as the data-processing operation is carried out in the context of activities of the establishment of Facebook in Belgium. In doing so, the court interpreted the law on the basis of the CJEU's 2014 judgement in *Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*.[68] Facebook immediately stated that it will appeal. The case also had repercussions at EU level: the Contact Group – a sub-entity established within the Article 29 Working Group that is in charge of dealing with Facebook's new terms of service – declared that it acknowledged the judgment and expected Facebook to comply with it.

5.2.3. Data retention regime remains in flux

The CJEU invalidated the Data Retention Directive (2006/24/EC) in 2014, holding – in *Digital Rights Ireland and Seitlinger*[69] – that it provided insufficient safeguards against interferences with the rights to privacy and data protection. This decision triggered considerable activity at both judicial and legislative levels in 2015.

In the absence of a valid Data Retention Directive, Member States may still provide for a data retention scheme under Article 15 (1) of the ePrivacy Directive (2002/58/EC),[70] which addresses the processing of electronic communications data. However, such schemes must also comply with the rules regarding the rights to privacy and personal data protection set out in Article 15 of the ePrivacy Directive, the EU Charter of Fundamental Rights and the CJEU ruling.

While the court's holding in *Digital Rights Ireland and Seitlinger* prompted several national legislators to revisit the issue of data retention, it did not bring about the widespread revocation of national data retention regimes. Instead, the year's developments indicated that governments are looking to reconcile the precedent set by the CJEU with the need to protect internal security and efficiently prosecute crimes by revising their data retention regimes. Many Member States that annulled data retention laws were actively considering replacement measures. The reluctance to forgo data retention was made explicit at the December Council of Justice and Home Affairs, where a majority of EU Member States indicated that data retention would benefit from reformed EU legislation.[71]

Meanwhile, where the obligation to retain data remained in force, companies were confronted with the dilemma of whether or not to comply – at the risk of violating their customers' rights.

Domestic courts voice considerable scepticism about data retention

In 2014, FRA mapped the Member States' reactions to the data retention laws introduced by the Data Retention Directive. This showed that all constitutional courts that addressed their respective national data retention regimes deemed these either partly or entirely unconstitutional. The validity of data retention laws was also questioned in criminal cases in which retained data were used as evidence. In addition, cases involving telecommunication companies – initiated after the *Digital Rights Ireland* judgment – were still pending in 2015.

The constitutional courts of **Belgium** and **Bulgaria**[72] and the High Court of Justice of the **United Kingdom** all took the position in 2015 that their countries' respective data retention regimes are unconstitutional, and in the **Netherlands** the District Court of The Hague handed down a similar judgment.[73]

The **Belgian** Constitutional Court concluded on 11 June 2015 that the Belgian data retention law disproportionately infringed on the right to privacy. In light of the *Digital Rights Ireland* finding, it highlighted as a particular problem the excessively wide scope of concerned data subjects, undetermined periods of retention, the lack of differentiation with regard to the type of data retained and their uses, and insufficient control mechanisms for access to the data.

The **Bulgarian** Constitutional Court deemed the Electronic Communications Act – the national data retention regulation – unconstitutional on 12 March 2015. The court's judgment emphasised that the law should contain accurate, clear and predictable rules to create secure guarantees for protection and security, given that, objectively, all citizens use modern communications and the vast

majority of them are not suspected of serious and/or organised crime or terrorism.[74] The judgment prompted the government to introduce several amendments to the Electronic Communications Act. The ruling also directly influenced the outcome of a case involving a telecom service provider charged with failing to comply with the obligation to retain data. In that case, an administrative court concluded that the abolition of the requirement to retain data justified repealing sanctions imposed for violating the requirement. However, this would not be applied retroactively, meaning that sanctions already enforced would remain valid.[75]

In the **United Kingdom**, the High Court of Justice ruled on 17 July 2015 that certain sections of the Data Retention and Investigatory Powers Act of 2014 (DRIPA) were incompatible with the right to respect for private life and communications, and to protection of personal data. The case – *R on the application of David Davis MP, Tom Watson MP, Peter Brice and Geoffrey Lewis v. SSHD* – was initiated by two members of parliament. The court also issued a judicial order declaring that sections prescribing indiscriminate data retention are incompatible with EU law and would be inapplicable from 31 March 2016 onwards. It also ordered the government to come up – by the specified date – with a new draft law that serves the purposes of DRIPA without violating the right to privacy.[76] The British government responded by publishing a draft bill in November. It requires judicial authorisation for warrants (in addition to authorisation by a Commissioner) and sets up a system of "retention notices", by which the Secretary of State obliges the telecom industry to retain data; these notices must specify the exact motivation and conditions for the retention.[77]

The unsettled legal landscape also triggered litigation involving telecom service providers; two cases are currently pending. In **Hungary**, an NGO – the Civil Liberties Union (*Társaság a Szabadságjogokért*) – brought a case against the telecom sector for continuing to retain data. In **Sweden**, Tele2, a telecom company, informed the Swedish Post and Telecoms Authority that it would stop storing data to comply with the CJEU judgement. However, the police informed the Post and Telecoms Authority that this would undermine the effectiveness of their work, so the authority requested the company to continue retaining data. Tele2 filed proceedings against the state, arguing that its failure to abolish data retention conflicted with EU law and the Charter of Fundamental Rights. The case is now pending before the CJEU and is expected to shed light on whether or not the mandatory retention of electronic communications data unlawfully interferes with the right to privacy and protection of personal data.[78]

Although no national courts have found that their respective data retention regimes can be reconciled with applicable fundamental rights standards, none has concluded that the Data Retention Directive's invalidation renders inadmissible the evidence gathered via data retention. This question was raised in the Supreme Courts of both **Ireland**[79] and **Estonia**[80] in 2015.

Courts took divergent views on whether or not law enforcement or intelligence authorities can legally access traffic and location data retained by electronic communications providers for billing purposes. In **Austria**, the Supreme Court – which actually revoked the national law implementing the Data Retention Directive – concluded that accessing location data (including network cells) retained for billing purposes is necessary for investigating crimes, meaning that refusing to grant access would violate the law.[81] By contrast, the Constitutional Court of **Romania**, which also revoked the applicable data retention law in 2014, additionally nullified the Romanian Law on Cyber Security (*Legea privind securitatea cibernetică a României*),[82] which enabled intelligence services and law enforcement to access personal data, including traffic data already processed and stored by electronic communications providers for billing and interconnection purposes.[83]

Diverse legislative initiatives aim to uphold data retention

Throughout the year, court decisions critical of the current data retention regime triggered various legislative proposals, which largely aimed to uphold the general regime by introducing additional safeguards.

In **Poland**, where the Constitutional Tribunal declared the respective national regulation partially null and void in 2014, the Senate followed up by submitting a new draft act in 2015.[84] NGOs and the Parliamentary Bureau of Analysis responded critically, noting that the revised law does not offer independent control mechanisms or limit data collection to the most serious crimes, and provides for an imprecise and discretionary period of retention.[85] In **Slovakia**, the Constitutional Court suspended the obligation to retain data in 2014, and ultimately deemed the applicable data retention law unconstitutional on 19 April 2015.[86] Following this decision, the government prepared a draft act that aims to enhance control over the data retention process and clearly details the situations in which data can be retained, stored and requested by state bodies. Specifically, the proposed law permits this only for the most serious crimes, such as terrorism or threats to the integrity of the country.

Shortly after the **Belgian** Constitutional Court struck down bulk data retention, the government – in the commentary on the new Draft Bill on Data Retention – concluded, after having consulted with other European governments, that data retention can be efficient only

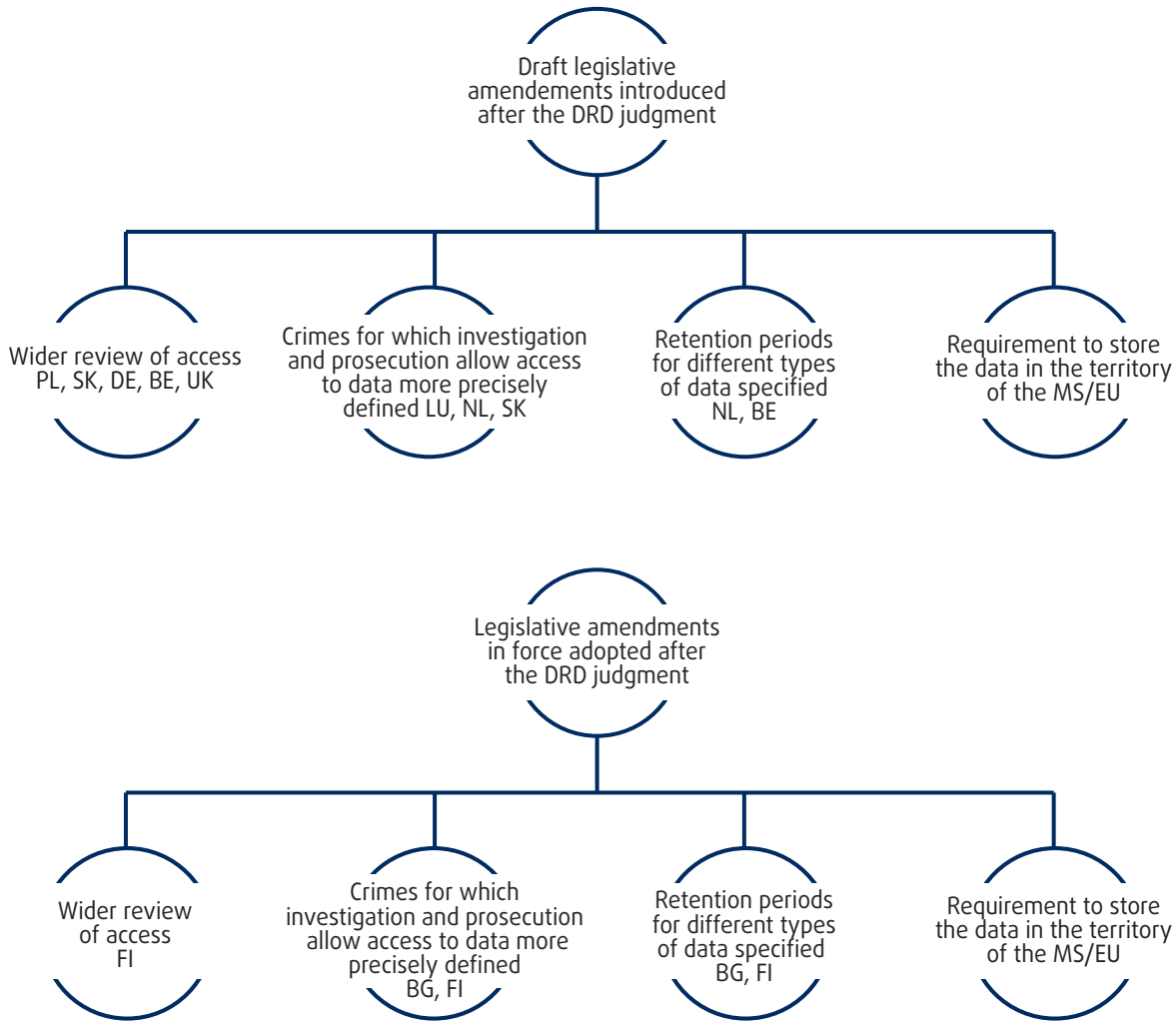
when it is indiscriminate. However, while the government asserted that blanket retention is inevitable, it acknowledged that stricter safeguards should be in place and that more stringent regulation on access conditions and retention periods for different types of data should be set up.[87]

In some Member States – including **Croatia**,[88] **Denmark**, **Estonia**,[89] **Finland** and **Lithuania**[90] – administrative bodies or legislators initiated reviews of the applicable data retention regimes. Among these, only **Finland** has so far enacted legislative amendments. The Information Society Code[91] specifies the retention periods for different types of communications data and requires individual, case-by-case reviews of access requests by the Ministry of the Interior; the new law also gives telecom operators more freedom in decisions regarding the technical implementation of requests.

Some Member States struck down data retention early on. In **Germany**, the parliament adopted legislation to reintroduce it in 2015. However, the proposal includes several safeguards, including the obligation to encrypt and log file access. In addition, it requires applying the "four-eyes principle", which means two persons must always authorise technical access to the data. Moreover, the content of communications, websites accessed and metadata of email traffic are explicitly excluded from the scope of the retained data.[92]

While the issue of whether or not to retain data predominated in 2014, 2015's developments made clear that most EU governments see data retention as an efficient way to protect national security and public safety and address crime. The debate has therefore focused on how to make data retention consistent with the CJEU's ruling in *Digital Rights Ireland*. As illustrated by Figure 5.2, which outlines amendments proposed

Figure 5.2: Amendments to national data retention laws in 2015



Source: FRA, 2016

or enacted in 2015, most governments are attempting to resolve the issue by introducing stricter access controls, specifying what types of crime permit access to retained data, clearly delineating retention periods and requiring data to be retained within the EU.

5.2.4. Terrorism pushes adoption of Passenger Name Record data collection systems

After lengthy and intense negotiations, the European Commission, the Council and the European Parliament's Civil Liberties Committee (LIBE) approved an agreement on a proposal for an EU system for the use of Passenger Name Record (PNR) data in 2015. The draft directive is to be put to a vote by the European Parliament as a whole early in 2016, and then is expected to be formally approved by the EU Council of Ministers.

The European Commission presented its proposal for a directive on using PNR data to combat terrorism and serious crime in 2011. PNR data are collected by airlines from passengers during check-in and reservation procedures.[93] However, the legislative procedure was blocked when the LIBE Committee rejected the proposal in April 2013, questioning its proportionality and necessity, as well as the lack of data protection safeguards and transparency towards passengers.[94] The CJEU's ruling in *Digital Rights Ireland and Seitlinger* (C-293/12 and C-594/12) was also considered relevant for the directive.[95]

However, challenges relating to "foreign terrorist fighters" and the Paris attacks in January 2015 pushed the question of an EU PNR data collection system up the political agenda as a possible measure to prevent and fight terrorism. Member States jointly called for an urgent adoption of the directive as a tool to detect and disrupt terrorist-related travel, particularly that of "foreign terrorist fighters".[96] On the other hand, both the Article 29 Working Party and the EDPS expressed concerns regarding the extent and indiscriminate nature of the processing proposed for the fight against terrorism and serious crime; they urged compliance with the fundamental requirements of necessity and proportionality, and ensuring the respect and protection of the rights set out in Articles 7 and 8 of the EU Charter of Fundamental Rights.[97] The Council of Europe also discussed the PNR data collection scheme in 2015.[98]

The compromise text agreed on by the EU co-legislators in December 2015 incorporates some of FRA's recommendations in its 2011 opinion on the EU PNR data collection system.[99] Taking into consideration the requirements of foreseeability and accessibility, as well as the principle of proportionality, it provides a clearer list of criminal offences that justify the use of PNR data by law enforcement authorities.[100] Moreover, in comparison with the 2011 draft directive, it introduces additional data protection safeguards, such as the duty to create dedicated data protection officers within the national units responsible for processing PNR data.[101] In addition, it does address certain aspects of the necessity and proportionality of the PNR system raised by FRA's opinion.[102]

On the other hand, while the new text envisages a review of the system by the European Commission that will be more comprehensive and based on additional statistical data, these statistics will not include fundamental rights-relevant indicators – such as, for example, the number of persons unjustifiably flagged by the system – as suggested by FRA's opinion.[103] Furthermore, the text opens the possibility of also applying the system to internal flights between EU Member States by leaving this matter up to individual Member States' discretion, potentially multiplying the tool's scope.[104]

> *"An EU PNR scheme programme would be the first large-scale and indiscriminate collection of personal data in the history of the Union. [...] The EDPS as well as the group of data protection authorities in Europe, the Article 29 Working Party, do not oppose any measure which is targeted and for a limited period of time [...] Our freedoms cannot be protected by undermining the right to privacy."*
>
> *European Data Protection Supervisor, Statement, 'EDPS supports EU legislator on security but recommends re-thinking on EU PNR', 10 December 2015*

Concerns about terrorism also affected developments at the national level, with several Member States announcing their intention to present or speed up draft laws to establish domestic PNR data collection systems.

In **Belgium**, following the attack on a *Thalys* train in August, the Minister of the Interior stated that he wished to have a PNR law adopted by the end of the year.[105] On 4 December 2015, the government approved the first draft of a bill on PNR,[106] which was then submitted to the Privacy Commission and the Council of State for their opinions. The Human Rights League criticised the draft text's scope, which also covers serious crimes, as too broad.[107] Similarly, in **Bulgaria**, draft amendments presented to the State Agency for National Security Act would transfer the tasks of collecting and processing PNR data from the National Counterterrorism Centre (CNN) to the State Agency for National Security (SANS).[108] Through this transfer, the Bulgarian government intends to broaden the scope of PNR data collection from the sole ground of terrorism to also include the grounds of preventing, detecting and prosecuting specific criminal offences. The amendments have been subject to public and inter-agency consultations and are pending for adoption by the government and submission to parliament.

In **Denmark**, the government presented an action plan called 'A Strong Defence against Terror', which contains a list of 12 initiatives, including the use of PNR data, to protect against and counter terrorism. The plan provides for access to PNR data by the Danish Intelligence and Security Service (PET). Consequently, a bill amending the PET Act was introduced, which intends to give PET access to PNR collected by the Danish Tax and Customs Authority (SKAT).[109] In **Spain**, an amendment to the draft Security Bill was introduced to provide a legal basis for the use of PNR data. The Bill on Protection of Civil Security was adopted in March 2015[110] and will be complemented by further regulation to launch the collection and processing of PNR data.

Most of the new proposed regulations were influenced by discussions at EU level. In **Latvia**, for instance, the draft law on passenger data processing presented by the Ministry of the Interior in June 2015[111] sets out that processing sensitive data of passengers will be prohibited, that the unit responsible for collecting and processing the data will be able to request passenger data from airlines about intra-EU flights, and that data should be retained for a maximum of five years.

Meanwhile, in three EU Member States (**Finland**, **Hungary** and **Romania**), legislation establishing PNR systems already entered into force in 2015.

In most Member States that had not yet established PNR systems (see Figure 5.3), the terrorist attacks in France revived the political debate on the need to establish such systems at national level. Several governments responded to internal questions by reaffirming that any PNR system should first be established at EU level. This was the case in **Ireland**, for instance, where the government described the proposed directive as a priority for EU security and sought its adoption during 2015.[112] Similarly, in **Luxembourg**, in response to a parliamentary question, the Minister for Internal Security affirmed the need for a European regulation on PNR before drafting a national regulation.[113] **Sweden** has taken a similar approach: although its Police Act[114] provides a legal basis for collecting PNR data in the country, it has not established a database so far and is awaiting the EU directive to properly launch the process at national level.

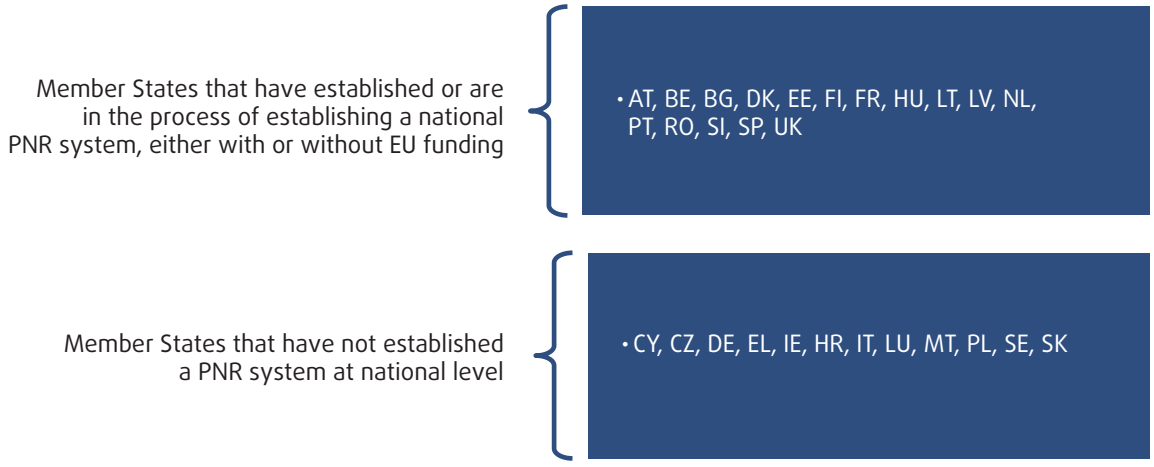
Promising practice

Fostering exchanges between a law enforcement agency and data protection authority while assessing new privacy-invasive practices

In **Slovenia**, when the police started the test phase of the national scheme for collecting and processing PNR information, the Criminal Police Directorate collaborated with the Slovenian DPA (the Information Commissioner) and for the first time decided to make use of guidelines drafted by the entity (*Privacy Impact Assessment guidelines for the introduction of new police powers*). Such a prior assessment of the impact of new police powers on privacy and protection of personal data represents a notable shift towards more transparency in the use of police powers.

For more information, see: Slovenia, Information Commissioner (Informacijski Pooblaščenec) (2014), Privacy Impact Assessment (PIA) guidelines for the introduction of new police powers *(Presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil).*

Figure 5.3: Overview of national PNR systems in 2015



Source: *FRA, 2016, based on the European Parliament Briefing (April 2015), European Parliamentary Research Service, 'The proposed EU passenger name records (PNR) directive revived in the new security context'*

FRA opinions

A number of EU Member States are in the process of reforming their legal framework for intelligence, as FRA research shows, which is based on a European Parliament request to undertake a fundamental rights analysis in this field. Security and intelligence services receiving enhanced powers and technological capacities often trigger such reforms. These, in turn, might increase the intrusive powers of the services, in particular as concerns the fundamental rights on privacy and protection of personal data, guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights, Article 8 of the European Convention on Human Rights (ECHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights, as well as access to an effective remedy, enshrined in Article 47 of the EU Charter and Article 13 of the ECHR.

The CJEU and the ECtHR require essential legal safeguards when intelligence services process personal data for an objective of public interest, such as the protection of national security. These safeguards include: substantive and procedural guarantees of the necessity and proportionality of a measure; an independent oversight and the guarantee of effective redress mechanisms; and the rules about providing evidence of whether an individual is being subject to surveillance.

FRA opinion

To address the identified challenges to privacy and the protection of personal data, it is FRA's opinion that, when reforming legal frameworks on intelligence, EU Member States should ensure to enshrine fundamental rights safeguards in national legislation. These include: adequate guarantees against abuse, which entails clear and accessible rules; demonstrated strict necessity and proportionality of the means that aim to fulfil the objective; and effective supervision by independent oversight bodies and effective redress mechanisms.

Since January 2012, EU institutions and Member States have been negotiating the EU data protection package. The political agreement reached in December 2015 will improve the safeguards of the fundamental right to the protection of personal data enshrined in Article 8 of the EU Charter of Fundamental Rights. The data protection package should enter into force in 2018. Data protection authorities will then play an even more significant role in safeguarding the right of data protection. Potential victims of data protection violations often lack awareness of their rights and of existing remedies, as FRA research shows.

FRA opinion

To render the protection of privacy and personal data more efficient, it is FRA's opinion that EU Member States should ensure to provide independent data protection authorities with adequate financial, technical and human resources, enabling them to fulfil their crucial role in the protection of personal data and raising victims' awareness of their rights and remedies in place. This is even more important as the new EU regulation on data protection is going to further strengthen data protection authorities.

Whereas developments in 2014 focused on the question of whether or not to retain data, the prevalent voice among EU Member States in 2015 is that data retention is the most efficient measure to ensure protection of national security, public safety and fighting serious crime. Based on recent CJEU case law, discussions have started anew on the importance of data retention for law enforcement authorities.

FRA opinion

Notwithstanding the discussions at EU level concerning the appropriateness of data retention, it is FRA's opinion that, within their national frameworks on data retention, EU Member States need to uphold the fundamental rights standards provided for by recent CJEU case law. These should include strict proportionality checks and appropriate procedural safeguards so that the essence of the rights to privacy and the protection of personal data are guaranteed.

The European Parliament Civil Liberties, Justice and Home Affairs Committee rejected the proposal for an EU PNR Directive in April 2013 in response to questions about proportionality and necessity, lack of data protection safeguards and transparency towards passengers. In fighting terrorism and serious crime, the EU legislature nonetheless reached an agreement on adopting an EU PNR Directive in 2015. The compromise text includes enhanced safeguards, as FRA also suggested in its 2011 opinion on the EU PNR data collection system. These include enhanced requirements for foreseeability, accessibility and proportionality, as well as introducing further data protection safeguards. Once it enters into force, the directive will have to be transposed into national law within two years.

FRA opinion

It is FRA's opinion that, while preparing to transpose the future EU Passenger Name Record (PNR) Directive, EU Member States could take the opportunity to enhance data protection safeguards to ensure that the highest fundamental rights standards are in place. In the light of recent CJEU case law, safeguards should be particularly enhanced as regards effective remedies and independent oversight.

Index of Member State references

Endnotes

1 United Nations (UN), General Assembly (2014), *The right to privacy in the digital age*, A/RES/69/166, 18 December 2014.

2 UN, Human Rights Council (2015), *The right to privacy in the digital age*, A/HRC/RES/28/16, 1 April 2015.

3 UN, General Assembly (2015), *The right to privacy in the digital age*, A/HRC/28/L.27, 24 March 2015.

4 *Ibid.*

5 *The Guardian* (2015), 'Digital surveillance "worse than Orwell", says new UN privacy chief', 24 August 2015.

6 Council of Europe, Parliamentary Assembly (2015), Resolution 2045 (2015) on mass surveillance, 21 April 2015.

7 Council of Europe, Parliamentary Assembly (2015), Resolution 2060 (2015) on improving the protection of whistle-blowers, 23 June 2015.

8 Council of Europe, Parliamentary Assembly (2015), Resolution 2045 (2015) on mass surveillance, 21 April 2015.

9 Council of Europe, Committee of Ministers (2015), Reply to REC 2067 (2015) on mass surveillance, 14 October 2015, para. 8.

10 Council of Europe, Parliamentary Assembly (2015), 'Rapporteur on mass surveillance reacts to revelations of collusion between NSA and BND', 4 April 2015; Council of Europe, Committee on Legal Affairs and Human Rights, Rapporteur Mr Pieter Omtzigt, Netherlands, EPP/CD (2015), Report doc. 13734, Mass surveillance, 18 March 2015.

11 Council of Europe, Commissioner for Human Rights (2015), *Democratic and effective oversight of national security services*, May 2015.

12 Council of Europe, Commissioner for Human Rights (2015), *Report by Nils Muižnieks following his visit to Germany, on 24 April and from 4 to 8 May 2015*, 1 October 2015.

13 ECtHR, *Roman Zakharov v. Russia*, No. 47143/06, 4 December 2015.

14 *Ibid.*

15 European Union Agency for Fundamental Rights (FRA) (2015), *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the European Union: Mapping Member States' legal frameworks*, Luxembourg, Publications Office, pp. 24–25.

16 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, paras. 41 and 66.

17 European Commission, Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215, p. 7.

18 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014.

19 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 93.

20 European Commission, *Overview on binding corporate rules*.

21 Article 29 Working Party (2015), *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*, 16 October 2015.

22 European Parliament (2014), Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, T7-0230/2014, Strasbourg, 12 March 2014.

23 European Parliament (2014), Resolution of 29 October on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens, T8-0388/2015, Strasbourg, 29 October 2015.

24 FRA (2015), *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the European Union: Mapping Member States' legal frameworks*, Luxembourg, Publications Office.

25 European Parliament (2015), Resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens, T8-0388/2015, Strasbourg, 29 October 2015, para. 52.

26 United Kingdom, Intelligence Services Commissioner (2015), *Report of the intelligence services commissioner (covering the period of January to December 2014)*, No. HC 225 SG/2015/74, June 2015.

27 United Kingdom, Anderson, D., Independent Reviewer of Terrorism Legislation (2015), p. 8.

28 United Kingdom (2015), Draft Investigatory Powers Bill, 4 November 2015.

29 United Kingdom (2015), *Factsheet: Targeted interception*.

30 United Kingdom (2015), *Factsheet: Bulk equipment interference*.

31 United Kingdom (2015), Draft Investigatory Powers Bill, 4 November 2015.

32 Netherlands (2015), Draft law on the Intelligence and Security Services 20XX (*Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX*), 2 July 2015.

33 European Parliament (2015), Resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens, T8-0388/2015, Strasbourg, 29 October 2015.

34 Austria, State Security Bill (*Entwurf Polizeiliches Staatsschutzgesetz*, PStSG), 1 July 2015.

35 Czech Republic, Amendment to the Act on Intelligence Services, as amended, and some other laws (*Zákon č. 219/2015 Sb., kterým se mění zákon o zpravodajských službách České republiky, ve znění pozdějších předpisů, a některé další zákony*), 25 September 2015.

36 Constitutional Court of Portugal.

37 France, Law No. 2015-912 on intelligence (*Loi n°2015-912 relative au relative au renseignement)*, 24 July 2015.

38 France, Constitutional Court (*Conseil constitutionnel*), Decision No. 2015-713 DC, 23 July 2015.

39 France, Law on international electronic communication surveillance (*Loi relative aux mesures de surveillance des communications électroniques internationales*), 30 November 2015.

40 Libération, *Surveillance: 2700 demandes adressées à la commission de contrôle en deux mois*, 17 December 2015.

41 *Ibid.*

42 France, Decree No. 2015-1475 on the application of Law No. 55-385 of 3 April 1955 (*Décret n° 2015-1475 du 14 novembre 2015 portant application de la loi n° 55-385 du 3 avril 1955*), 14 November 2015.

43 France, *Loi n° 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions.*

44 France, Draft constitutional law on the protection of the nation (*Projet de loi constitutionnelle de protection de la Nation*), 23 December 2015.

45 France, Nous ne cèderons pas, 'Sortir de l'état d'urgence', 17 December 2015.

46 France, Defender of Rights (*Le Défenseur des Droits*), *State of emergency* (*L'état d'urgence*).

47 France, National Consultative Commission on Human Rights (*Commission nationale consultative des droits de l'homme*) (2015), State of emergency control (*Contrôle de l'état d'urgence*), 21 December 2015.

48 France, National Assembly (*Assemblée nationale*), *Parliamentary control of the state of emergency* (*Contrôle parlementaire de l'état d'urgence*).

49 European Parliament (2015), *Data protection package: Parliament and Council now close to a deal*, Press release, 15 December 2015.

50 European Commission (2016), 'Protection of personal data'.

51 European Parliament (2015), 'Q&A on EU data protection reform', 24 June 2015.

52 FRA (2012), *Data protection reform package FRA opinion: October 2012*, Vienna, FRA, October 2012, p. 33.

53 European Parliament (2015), 'Q&A on EU data protection reform', 24 June 2015.

54 European Data Protection Supervisor (EDPS) (2015), *Towards a new digital ethic* (Opinion 4/2015), 11 September 2015, p. 4; EDPS (2015).

55 EDPS (2015), 'EDPS to set up an Ethics Board', Press release, 11 September 2015.

56 *Ibid.*

57 European Commission (2015), *Questions and answers on the EU-US data protection "Umbrella Agreement"*, Brussels, 8 September 2015.

58 *Ibid.*

59 CJEU, C-147/03, *Commission of the European Communities v. Republic of Austria*, 7 July 2005; see FRA (2014), *Annual activity report 2014*, Luxembourg, Publications Office.

60 Belgium, State Secretary (2015), 'Tommelein zal niet wachten op europese privacywetgeving', Press release, 16 December 2015.

61 Malta, Processing of Personal Data (Education Sector) Regulations, Subsidiary Legislation 440.09 of the Laws of Malta, 9 January 2015.

62 Latvia, Cabinet of Ministers (*Ministru kabinets*) (2015), Cabinet of Ministers Regulation No. 216 'On the procedure for preparing and submitting compliance assessment of personal data processing' (*Ministru kabineta noteikumi Nr. 216 "Kārtība, kādā sagatavo un iesniedz personas datu apstrādes atbilstības novērtējumu"*), 12 May 2015.

63 Germany, Second Act Amending the Federal Data Protection Act: Strengthening the independence of data protection supervision by establishing a supreme federal authority (*Zweites Gesetz zur Änderung des Bundesdatenschutzgesetzes – Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund durch Errichtung einer obersten Bundesbehörde*), 25 February 2015.

64 Hungary, Act CXII of 2011 on information self-determination and freedom of information (*2011. évi CXII törvény az információs önrendelkezési jogról és az információszabadságról*), 2011.

65 Netherlands, Personal Data Protection Law (*Wet bescherming persoonsgegevens*), 6 July 2000.

66 Netherlands, Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*, CBP) (2015), 'CBP vraagt reacties op conceptrichtsnoeren meldplicht datalekken', Press release, 21 September 2015.

67 Belgium, Dutch-speaking court of first instance Brussels *(Nederlandstalige rechtbank van eerste aanleg Brussel)*, case no. 15/57/C, *President of the Belgian Commission for the protection of privacy v. Facebook Inc., Facebook Belgium SPRL and Facebook Ireland Limited,* 9 November 2015.

68 CJEU, C-131/12, *Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*, 13 May 2014.

69 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014.

70 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive), OJ L 201, 31 July 2002.

71 Council of the European Union (2015), 'Outcome of the Council meeting', Press release, 3 and 4 December 2015.

72 Bulgaria, Constitutional Court (Конституционен съд) (2015), Decision No. 2 of 12 March 2015 on constitutional case No. 8/2014 *(Решение № 2 от 12 март 2015 г. по конституционно дело № 8/2014)*, 12 March 2015.

73 Netherlands, District Court The Hague (*Rechtbank Den Haag*) (2015), Case No. C/09/480009 / KG ZA 14/1575, ECLI:NL:RBDHA:2015:2498, 11 March 2015.

74 Bulgaria, Constitutional Court (Конституционен съд) (2015), Decision No. 2 of 12 March 2015 on constitutional case No. 8/2014 (Решение № 2 от 12 март 2015 г. по конституционно дело № 8/2014), 12 March 2015.

75 Bulgaria, Administrative Court – Sofia (ACS) (Административен съд – София, АСС), Decision No. 3861 of 04.06.2015 on administrative case No. 1134/2015 (Решение № 3861 от 04.06.2015 г. по административно дело № 1134/2015 г.), 4 June 2015.

76 United Kingdom, High Court of Justice, Case No. CO/3665/2014, CO/3667/2014, CO/3794/2014, *David Davis and others v. Secretary of State for the Home Department*, 17 July 2015.

77 United Kingdom, HM Government (2015), Draft Investigatory Powers Bill, 4 November 2015, section 71(9) (f).

78 CJEU, Case C-203/15, *Tele2 Sverige AB v. Post- och telestyrelsen*, request for a preliminary ruling from Kammarrätten i Stockholm (Sweden), lodged on 4 May 2015.

79 Ireland, *Director of Public Prosecutions v. Graham Dwyer*, CCDP0012/2014.

80 Estonia, Criminal Chamber of the Supreme Court judgment no. 3-1-1-51-14, 23 February 2015.

81 Austria, Supreme Court (*Oberster Gerichtshof*), 12Os93/14i (12Os94/14m).

82 Romania, Constitutional Court (*Curtea Constituțională*), Decision no. 17, 21 January 2015.

83 *Ibid.*

84 Poland, Senate (*Senat*), Draft act amending the Act on police and certain other acts (*Projekt ustawy o zmianie ustawy o Policji i niektórych innych ustaw*), draft no. 967, 25 June 2015.

85 Poland, Helsinki Foundation for Human Rights (*Helsińska Fundacja Praw Człowieka*) (2015), 'Uwagi Helsińskiej Fundacji Praw Człowieka do senackiego projektu ustawy

o zmianie Ustawy o Policji i niektórych innych ustaw', 26 August 2015.

86 Slovakia, Constitutional Court of the Slovak Republic (Ústavný *súd Slovenskej Republiky*) (2015), Resolution No. PL. ÚS 10/201478, 29 April 2015.

87 Belgium, Draft Bill on data retention in the sector of telecommunications (*Voorontwerp van wet betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie/Avant-projet de loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques*), p. 11.

88 Croatia, Tportal.hr (2014), 'Communication data in Croatia are retained despite the judgment of the European Court', 23 July 2014.

89 Estonia, Chancellor of Justice (Õiguskantsler) (2015), 'Õiguskantsler: Elektroonilise side faktide kogumine sideettevõtete poolt ei ole eraldi võetuna Põhiseadusega vastuolus', Press release, 20 July 2015; Estonia, Chancellor of Justice (Õiguskantsler) (2015), 'Õiguskantsleri seisukoha edastamine', Letter to the Minister of Justice, 20 July 2015.

90 Lithuania, Minister of Justice of the Republic of Lithuania (*Lietuvos Respublikos teisingumo ministras)* (2014), the Order on the Formation of Working Group No. 1R-200 (Įsakymas dėl darbo grupės sudarymo Nr. *1R-200*), 27 June 2014.

91 Finland, Information Society Code (*Tietoyhteiskuntakaari/ Informationssamhällsbalken*, 917/2014).

92 Germany, Law on data retention (*Vorratsdatenspeicherung*), Art. 113.

93 European Commission (2015), *EU Passenger Name Record (PNR) proposal : an overview*, 14 December 2015.

94 European Parliament (2013), 'Civil Liberties Committee rejects EU Passenger Name Record proposal', Press release, 24 April 2013.

95 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014.

96 European Council (2015), 'Informal meeting of the Heads of State or Government Brussels, 12 February 2015, Statement by the members of the European Council', Press release, 12 February 2015.

97 Article 29 Working Party (2015), *Letter on EU PNR*, 19 March 2015; EDPS (2015), *Second Opinion 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* (Opinion 5/2015), 24 September 2015.

98 Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), 37th meeting, 9-11 December 2015, Strasbourg, Council of Europe.

99 FRA (2011), *Opinion on the proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, FRA Opinion 01/2011, Vienna, FRA.

100 *Ibid.,* pp. 16, 22.

101 *Ibid.*, p. 20.

102 *Ibid.*

103 *Ibid.,* p. 21.

104 European Parliament (2015), *EU Passenger Name Record (PNR) proposal: an overview*, 14 December 2015.

105 RFI.fr (2015), 'Belgium to collect data on travellers of planes, trains and ferries', 1 September 2015.

106 Jambon.belgium.be (2015), 'Feu vert pour le PNR belge et européen', 4 December 2015.

107 RTBF.be (2015), 'PNR à la Belge: le gouvernement Michel approuve son propre contrôle des données des passagers', 5 December 2015.

108 Bulgaria, Ministry of the Interior (Министерство на вътрешните работи) (2015), Letter No. 33374/2-12.10.2015 to the Centre for the Study of Democracy (Писмо № 33374/2-12.10.2015 г. до Центъра за изследване на демокрацията), 12 October 2015; Bulgaria, State Agency for National Security (Държавна агенция „Национална сигурност") (2015), Letter No. И-кр-690/11.09.2015 to the Centre for the Study of Democracy (Писмо *№ И-кр-690/11.09.2015* г. до Центъра за изследване на демокрацията), 11 September 2015.

109 Denmark, Bill no. 23 of 7 October 2015 and passed on 21 December 2015 amending the Act on the Danish Security Intelligence Service (PET) and the Customs Act (The Danish Security and Intelligence Service's access to information on airline passengers in terrorism cases etc. and SKAT's handling of information on airline passengers for customs inspections etc.) (*Lovforslag nr. 23 af 7. oktober 2015, om Lov om ændring af lov om Politiets Efterretningstjeneste (PET) og toldloven (Politiets Efterretningstjenestes adgang til oplysninger om flypassagerer i terrorsager m.v. og SKATs håndtering af oplysninger om flypassagerer i forbindelse med toldkontrol m.v.*), 7 October 2015.

110 Spain, Official State Gazette (*Boletín Oficial del Estado*, BOE), Law 4/2015 on protection of civil security (*Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana*), 30 March 2015.

111 Latvia, Ministry of the Interior (*Iekšlietu ministrija*), Draft law 'on passenger data processing' (*Likumprojekts "Pasažieru datu apstrādes likums"*), 4 June 2015.

112 Ireland, Irish Naturalisation and Immigration Service (2015), 'Minister Fitzgerald discusses international terrorism, security and migration with EU ministers', 10 July 2015; Buckley, D. (2015), 'Further delays expected in making EU air travel safer', *Irish Examiner*, 11 August 2015.

113 Luxembourg, Minister for Internal Security (*Ministre de la Sécurité intérieure*), Parliamentary question No. 842, reply of 17 February 2015.

114 Sweden, Ministry of Justice (*Justitiedepartementet*), Police Data Act (*Polisdatalagen*), SFS 2010:361, 20 May 2010.