UN & CoE

12 January – In *Szabó and Vissy v. Hungary* (No. 37138/14), the European Court of Human Rights (ECtHR) holds that Hungarian legislation on secret surveillance violates the right to respect for correspondence, home and private life, as it failed to provide adequate safeguards against abuse (Article 8 of the ECHR)

12 January – In *Bărbulescu v. Romania* (No. 61496/08), the ECtHR holds that an employer may under certain circumstances monitor the employees' use of the internet at their workplace and may use the collected data to justify their dismissal, concluding that there was no violation of the right to respect for private and family life (Article 8 of the ECHR); the case was later referred to the Grand Chamber

13 January – Council of Europe (CoE) Committee of Ministers adopts Recommendation CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality

26 January – CoE Parliamentary Assembly (PACE) adopts Resolution 2090 (2016) on combating international terrorism while protecting CoE standards and values

January

2 February – In *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary* (No. 22947/13), the ECtHR holds that imposing strict liability on internet portals for offensive comments posted by their readers, which did not amount to hate speech or direct threats to physical integrity, violates their right to freedom of expression and to impart information (Article 10 of the ECHR)

February

8 March – United Nations (UN) Special Rapporteur on the Right to Privacy issues his first report to the Human Rights Council

30 March – CoE issues its 2016-2019 Internet Governance Strategy

March

13 April – CoE Committee of Ministers adopts Recommendations CM/Rec(2016)4 and CM/Rec(2016)5, relating to internet freedom and the protection of journalism and safety of journalists and other media actors, respectively

April

19 May – In *D.L. v. Bulgaria* (No. 7472/14), the ECtHR holds that the automatic and blanket monitoring of the correspondence and telephone calls of minors placed in an educational centre violates the right to respect for correspondence (Article 8 of the ECHR)

May

7 June – In *Cevat Özel v. Turkey* (No. 19602/06), the ECtHR holds that the unjustified lack of ex post facto notification of the applicant of a temporary phone-tapping measure violates the right to respect for private and family life and for correspondence (Article 8 of the ECHR)

7 June – In *Karabeyoğlu v. Turkey* (No. 30083/10), the ECtHR holds that the use of data in disciplinary proceedings – which originated from a lawful telephone tapping in criminal proceedings – violates the right to respect for private and family life (Article 8 of the ECHR)

17 June – International conference on the globalisation of the Council of Europe convention for the protection of individuals with regard to automatic processing of personal data gathers 80 countries

June

July

30 August – UN Special Rapporteur on the Right to Privacy issues his second report, criticising British and German surveillance measure reforms

August

1 September – Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data is published

15 September – CoE Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data adopts an opinion on the 'Data protection implications of the processing of Passenger Name Records'

16 September – CoE adopts the Bratislava Declaration and Roadmap

September

October

8 November – In *Magyar Helsinki Bizottság v. Hungary* (No. 18030/11), in a Grand Chamber judgment, the ECtHR finds a violation of Article 10 of the ECHR for police stations' refusal to provide an NGO with certain information about public defenders; the government's obligation to impart information held by a public authority may arise where disclosure has been imposed by a judicial order and access to information is instrumental for exercising the right to freedom of expression, and where its denial constitutes an interference with that right

24 November – European Judicial Cybercrime network is launched

November

13 December – In *Eylem Kaya v. Turkey* (No. 26623/07), the ECtHR holds that the prison authorities' systemic physical monitoring of the applicant's correspondence with her lawyer was not proportionate to the aim pursued and thus violated the right to respect for correspondence (Article 8 of the ECHR)

20 December – In *Radzhab Magomedov v. Russia* (No. 20933/08), the ECtHR holds that the national courts' rejection – without sufficient reasoning – of the applicant's request for disclosure of the warrant authorising the interception of his telephone communications in criminal proceedings violated his right to respect for private life (Article 8 of the ECHR)

December

EU

25 January – Europol creates the European Counter Terrorism Centre (ECTC), which focuses on foreign fighters, sharing intelligence on terrorism financing, online terrorist propaganda, illegal arms trafficking and international cooperation among counter-terrorism authorities

January

2 February – European Commission and US Government reach a political agreement on a new framework regarding exchanges of personal data for commercial purposes ("EU-US Privacy Shield")

29 February – European Commission presents the draft Adequacy Decision for free data flow from the EU to the US Privacy Shield companies in the US

February

March

6 April – European Commission issues Communication on Stronger and Smarter Information Systems for Border and Security

12 April – European Commission launches Public Consultation on the Evaluation and Review of the ePrivacy Directive until 5 July 2016

13 April – Article 29 Working Party delivers its Opinion on EU-US Privacy Shield

20 April – European Commission issues Communication on Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union

21 April – Council of the EU adopts Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

27 April – Council of the EU and European Parliament (EP) adopt Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

April

5 May – Police Directive enters into force (transposition period until 6 May 2018)

24 May – GDPR enters into force (to be applied from 25 May 2018)

26 May – EP issues resolution on EU-US Privacy Shield

30 May – European Data Protection Supervisor (EDPS) delivers Opinion 4/2016 on EU-US Privacy Shield – More robust and sustainable solution needed

May

16 June – EDPS issues a background paper on necessity – a toolkit for assessing the necessity of measures that interfere with fundamental rights

June

12 July – European Commission adopts the decision on the adequacy provided by the EU-US Privacy Shield (EU) 2016/1250

18 July – EDPS issues guidelines for Data Protection and Whistleblowing in the EU institutions

22 July – EDPS delivers Opinion 5/2016 on e-Privacy: rules should be smarter, clearer, stronger

July

1 August – European Commission publishes a guide to the EU-US Privacy Shield for citizens, explaining available remedies for individuals who believe their personal data were used without taking into account data protection rules

4 August – European Commission publishes summary report on the Public Consultation on the Evaluation of the e-Privacy Directive

August

8 September – Advocate General Mengozzi delivers Opinion 1/15, requested by the EP, on the PNR Agreement between EU and Canada: agreement partly incompatible with Articles 7, 8 and 52 (1) of the EU Charter of Fundamental Rights

14 September – European Commission issues Communication COM(2016) 602 on 'Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders'

16 September – European Council adopts the Bratislava Declaration and Roadmap

16 September – In *Digital Rights Ireland v. Commission* (Case T-670/16), Digital Rights Ireland challenges the Commission's adoption of the EU-US Privacy Shield decision before the General Court, alleging that it lacks adequate privacy protections

23 September – EDPS delivers Opinion 8/2016 on coherent enforcement of fundamental rights in the age of Big Data

September

12 October – First report by the European Commission on progress towards an effective and sustainable Security Union

19 October – In *Breyer v. Bundesrepublik Deutschland* (Case C-582/14), the Court of Justice of the EU (CJEU) rules that a dynamic IP address of a website visitor constitutes personal data with respect to the operator of the visited website, if the operator has the legal means to identify the visitor with additional information about the visitor held by an internet access provider; the decision notes that website operators may have a legitimate interest in storing personal data relating to visitors to their websites to protect themselves against cyberattacks

20 October – EDPS delivers Opinion 9/2016 on Personal Information Management Systems

26 October – Proposal for a Directive of the EP and the Council of the EU on combating terrorism

October

16 November – European Commission issues second report on progress towards an effective and sustainable Security Union

28 November – European Commission releases a Staff Working Document on the Implementation Plan for the Passenger Name Records (PNR) Directive

November

21 December – In *Tele2 Sverige* (C-203/15) and *Watson v. Home Secretary* (C-698/15), the CJEU rules in joined cases that Article 15 (1) of Directive 2002/58/EC, read in light of Articles 7, 8 and 11 and Article 52 (1) of the EU Charter of Fundamental Rights, precludes national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication

December

6 Information society, privacy and data protection

The year's terrorist attacks in Brussels, Nice and Berlin further intensified debates about ways to effectively fight terrorism in compliance with the rule of law. A number of steps were taken in this respect at both EU and national levels. They include national reforms on surveillance measures, consultations on encryption, and the adoption of the Passenger Name Record (PNR) Directive. Meanwhile, the adoption of the General Data Protection Regulation (GDPR) and the Data Protection Directive for the police and criminal justice sector (Police Directive) constituted a crucial step towards a modernised and more effective data protection regime. The EU in 2016 did not propose revised legislation in response to the Court of Justice of the European Union's (CJEU) earlier invalidation of the Data Retention Directive, but new CJEU case law further clarified how data retention can comply with fundamental rights requirements.

6.1. Responding to terrorism: surveillance, encryption and passenger name records – international standards and national law

The EU faced a continued wave of terrorist attacks throughout 2016. France, Belgium and Germany were particularly affected, with the most devastating attacks killing 86 in Nice, 32 in Brussels and 12 in Berlin. Such attacks threaten various fundamental values, including the right to life, which states are obliged to protect. Coupled with the continuing threat posed by returning foreign terrorist fighters,[1] the attacks underscored the security challenges faced by Member States and, consequently, by the EU. As a result, counter-terrorism remained high on both national and EU agendas and sparked diverse discussions and policy responses, including regarding intelligence and law enforcement agencies; encryption of data; and the collection of passenger name records (PNR) data.

Policy responses included efforts to provide intelligence and law enforcement agencies with increased powers and to improve their cooperation at both national and European levels. Although these services play a vital role in safeguarding national security and individuals' right to life and security, Member States should ensure that their activities – such as surveillance – are conducted in a democratic, lawful manner.

The European Parliament asked FRA to research fundamental rights protection in the context of large-scale surveillance, prompting the following observations about developments in this field in 2016.

6.1.1. International organisations call for restraint on surveillance

Member States' efforts to strengthen intelligence and law enforcement agencies triggered calls for restraint by various international organisations, who also reminded all parties to respect relevant international and European legal standards.

> *"Whatever we do to counter terrorism must be consistent with the values which unite us: human rights, democracy and the rule of law."*
>
> *Terrorism: #NoHateNoFear, a Council of Europe Parliamentary Assembly (PACE) initiative*

The UN Special Rapporteur on the right to privacy, Joseph Cannataci, who took on his role in July 2015, has since issued two reports. In his March 2016 report,

he proposed a shift in approach to the tensions of the field – from speaking of "privacy versus security" to instead speaking of "privacy and security", with both rights seen as "enabling rights rather than ends in themselves".[2] He also noted that many countries had rushed privacy-intrusive legislation through parliament.[3] Meanwhile, the UN Special Rapporteur on human rights and counter-terrorism, Ben Emmerson, in a report issued in April 2016, stated that the "demonstrable inadequacy of a strict security approach to countering terrorism" had led states to shift their focus to measures that address the root causes of terrorism and radicalisation.[4]

The Council of Europe Parliamentary Assembly (PACE) echoed this approach in a resolution calling on Member States to "refrain from indiscriminate mass surveillance, which has proven to be inefficient"[5] and instead improve national and international cooperation.[6] In the same spirit, PACE also launched the #NoHateNoFear initiative to counter terrorism. It aims to draw attention to the complexity of the problem to avoid fuelling populist movements, which "play on security as a simplistic option to combat terrorism".[7] (For more on this issue, see Chapter 3 on Racism, xenophobia and related intolerance.)

To help further clarify the legal framework applicable to Member States, the Secretary General of the Council of Europe pledged to work with states in launching a process before the end of 2016, aiming to codify international standards, good practices and guidance relating to mass surveillance.[8] In March, the Venice Commission also adopted a so-called Rule of Law Checklist, providing, among others, specific rule of law benchmarks on the collection of data and surveillance.[9]

The UN Human Rights Council (HRC) called upon states to review their practices and legislation relating to surveillance and ensure that they are in line with their obligations under international human rights law. It underlined that any interference with the right to privacy must be regulated by "publicly accessible, clear, precise, comprehensive and non-discriminatory" laws.[10] Data protection in the context of surveillance has also featured throughout the Universal Periodic Review of EU Member States (**Belgium**,[11] **Estonia**,[12] **Latvia**[13]) and was stressed in the UN Human Rights Committee's concluding observations on **Denmark**,[14] **Poland**[15] and **Sweden**.[16] Regarding **Sweden**, for example, the committee stated that it was concerned by the limited transparency about the scope of surveillance powers and the safeguards in place both regarding their application and the sharing of raw data with other intelligence services.[17]

Meanwhile, in January 2016, the European Court of Human Rights (ECtHR) delivered an important judgment on secret surveillance. In *Szabó and Vissy v. Hungary*, the court found that the 2011 **Hungarian** legislation on secret anti-terrorist surveillance violated Article 8 of the ECHR because it failed to provide adequate safeguards against abuse. Referring to the Court of Justice of the European Union's (CJEU) judgment in *Digital Rights Ireland v. Minister of Communications & Others*, the ECtHR stated that, where national rules enable large-scale or strategic interception and where this interference "may result in particularly invasive interferences with private life", the "guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices".[18]

Contrary to claims that the ECtHR outlawed mass surveillance with *Szabó and Vissy*, it in fact did "not seem to have taken a final position on the legality of the massive and indiscriminate collection of personal data (i.e. non-targeted bulk collection)".[19] Several cases pending before the court are likely to further clarify its stance on surveillance by intelligence services.[20]

6.1.2. Fear of terrorism prompts calls for increased powers for, and cooperation between, intelligence and law enforcement services

As noted above, the year's terror attacks served as a stark reminder of the security challenges faced by Member States and, by extension, the EU. For policymakers looking to devise effective responses and security measures, doing so while complying with fundamental rights was a central challenge.

On 23 March, one day after the attacks in Brussels, Commission President Juncker announced that, to counter terrorism effectively, the EU would need to establish a Security Union.[21] Reflecting the importance attached to security, in September 2016 the Council of the EU appointed Julian King to the newly created post of Commissioner for Security Union. The commissioner aims to create an effective and sustainable Security Union, with fundamental rights at the heart of the framework.[22]

From a data protection perspective, the calls and efforts to increase the interoperability of EU information technology (IT) systems appear to focus predominantly on technical matters, and have – so far – only cursorily addressed fundamental rights aspects. (For more on such systems, see Chapter 5.) FRA is a member of the Commission's High Level Expert Group on Information Systems and Interoperability, and in this role has sought to underline how fundamental rights should be embedded in any IT-based responses.[23] Another criticism of the proposed measures, voiced in the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, relate to their effectiveness.[24] The committee pointed out that perhaps it is not blanket collection and retention of data – mostly on people

who are not suspected of any crimes or involvement in terrorist activities – that is necessary to counter terrorism, but rather better analysis of existing data and more investment in local authorities' capacities.[25]

Regarding information exchanges between and among law enforcement and intelligence services, the Commission deemed urgent the need to address existing gaps between these two communities.[26] One option it suggested is opening the Counter Terrorism Group (CTG) to 'interaction' with law enforcement authorities through the existing Europol framework.[27] The CTG is a platform for informal cooperation among intelligence services, functioning outside the EU framework. It includes the services of EU Member States, Switzerland and Norway.[28] The Commission also emphasised the need for increased cooperation between these institutions and the EU Intelligence and Situation Centre (IntCen), with a view to creating an information exchange hub.[29]

In September, the European Council adopted the Bratislava Roadmap.[30] Key elements of this working programme include proposed measures to increase cooperation and intelligence exchanges between Member State security services to help the EU ensure the internal security of Member States and fight terrorism.[31]

Much activity also occurred at Member State-level throughout the year. A number of Member States enacted legislation that affects surveillance by intelligence services. In many, reform was in progress. Key subjects included the mandates of intelligence services and measures available to them; their cooperation with national law enforcement authorities; and the national oversight systems. Member States that took action faced the challenge of striking an appropriate balance between complying with their obligation to protect the life and integrity (security) of their citizens against ever more apparent threats, and respecting citizens' privacy in line with European standards. These balancing efforts often occurred amidst a trend Commission President Juncker had warned against:[32] simplification of issues and solutions, populism and disregard for evidence in decision-making.

Regulating surveillance at national level: consultation and transparency

One of the persisting issues at national level is a lack of transparency and public dialogue, whether relating to the adoption of new laws or to the functioning of the intelligence services. In **Poland**, for example, the new Anti-terrorist Act[33] was introduced in a fast-track legislative process, without official public consultation. The act substantially extends the powers of the intelligence services without providing any additional safeguards against the abuse of those powers. In **Romania**, although a public consultation took place, provisions expanding the powers of the Romanian Intelligence Service (RIS) (*Serviciul Român de Informații*, SRI) appeared only in the final version of the Emergency Ordinance[34] and were not part of the document submitted for public debate.

On the other hand, a number of Member States engaged in legislative and oversight reforms with a view to gaining trust via transparency. In the **United Kingdom**, extensive consultation preceded the passing of the Investigatory Powers Act. The Joint Committee on the Draft Investigatory Powers Bill heard 59 people in 22 public panels,[35] including public authorities, non-governmental organisations, academia and private companies.[36] The government also sought expert advice from the Independent Reviewer of Terrorism Legislation.[37]

The **Irish** government in January 2016 appointed a retired judge to carry out an independent review of a law relating to public authorities' access to communications data of journalists.[38] The **Belgian** parliament established a temporary 'Fight against Terrorism' Commission to examine the bills implementing some of the measures put forward by the government following the terrorist attacks in Paris.[39] After the March attacks in Brussels, a Parliamentary Investigative Commission was also set up to examine the circumstances that led to the attacks.[40]

Member States also endeavoured to increase the transparency and legality of the functioning of their intelligence services by regulating previously unregulated areas. For example, in **Germany**, a law regulating the German intelligence service's (BND) gathering of intelligence on foreigners abroad came into force – a substantial step towards transparency.[41] Similarly, in **Italy**, a draft law aims to regulate the police's and judicial authorities' use of wiretapping and 'Trojan programs', malicious programs used to hack computers.[42] The Chamber of Deputies has already approved the law. Moreover, in **Cyprus**, the Cyprus Intelligence Service (CIS) was also brought within a regulatory framework in April.[43]

Intelligence services' operations and oversight

As previously noted, Member State efforts to increase the effectiveness of security services involved two main approaches in 2016: expanding their powers, competences or resources; and facilitating cooperation between relevant actors, both at national and EU levels.

For example, in the **United Kingdom**, the Investigatory Powers Act gives the services the power to require the retention of internet connection records indiscriminately when it relates to any of a list of purposes, including national security. This means that internet providers must keep track of each connection to the internet through a website or an instant messaging application.[44]

In **Poland** and **Hungary**, measures to increase executive control and centralise information management were implemented. In **Poland**, a new law on the Prosecutor's Office was adopted in March 2016. Pursuant to its provisions, the previously independent office of the Prosecutor General is now held by the Minister of Justice. The legislation also allows the Prosecutor General to order the competent authorities to conduct surveillance if it is related to ongoing investigations. Thus, the minister is now responsible for both providing oversight of the special services and ordering operational surveillance.[45] **Hungary** established a new information centre – the Counter-Terrorism Information Analysis Centre (*Terrorelhárítási Információs és Bűnügyi Elemző Központ*, TIBEK) – to collect and systematise information derived from various surveillance operations conducted by the different national security services.[46]

Legislative changes and other measures also addressed the oversight systems for intelligence services. The **United Kingdom** Investigatory Powers Act creates a new oversight system with a single Investigatory Powers Commissioner, who is to be assisted by Judicial Commissioners.[47] The act introduces a so-called double-lock system: alongside approval by the Secretary of State, warrants for surveillance measures also need to be authorised by a Judicial Commissioner.[48]

Meanwhile, in **France**, the state of emergency introduced after the November 2015 Paris attacks was prolonged for a fourth time. According to the law enacted at the last extension, it is to be lifted on 15 July 2017.[49] The state of emergency extends intelligence services' powers relating to, for example, the real-time monitoring of individuals.[50]

Promising practice

Providing relevant advice before authorising certain surveillance efforts

A draft bill for a new Act on the Intelligence and Security Services is currently under discussion in the **Netherlands**. In the meantime, a temporary commission advises ministers before they authorise intelligence services to apply special powers to lawyers and journalists. It was established to comply with a domestic court judgment (District Court of The Hague (*Rechtbank Den Haag*), Case No. C/09/487229, 2015) as well as with an ECtHR judgment (*Telegraaf Media Nederland B.V. and others v. the Netherlands*, No. 39315/06, 2012). The commission is staffed by the Chair of the Review Committee and a deputy. Its advice is binding.

For more information, see Minister of the Interior and Kingdom Relations & Minister of Defence (Minister van Binnenlandse Zaken en Koninkrijksrelaties & Minister van Defensie) (2015), Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten

6.1.3. Encryption sparks debate

The issue of encryption dominated debates at international, European and national levels throughout 2016. Encryption is a privacy-enhancing technology that allows the secure processing of data. Data and communications are converted into a code that allows access only to those who have a key or password or, in case of end-to-end encryption, only to those for whom the data are intended.

The debate presently revolves around whether or not the interests of national security and crime prevention justify requiring companies to insert back doors into their programs to make the encrypted data accessible. The argument for access by intelligence and law-enforcement services is that terrorists or other criminals could otherwise avoid detection and police authorities could be prevented from obtaining crucial evidence. The counter-arguments, as developed by a group of pre-eminent cryptographers, computer scientists and security specialists, are that "the costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict".[51]

Thus, weakening encryption software may have a number of unintended consequences. For example, it may adversely affect the security of online transactions, people's trust in these, and, consequently, the appropriate functioning of the EU's Digital Single Market. Another such consequence relates to the security of journalists' sources and so to journalism as a whole. Recognising this aspect of the encryption debate, in its resolution on 'The safety of journalists', the UN Human Rights Council called upon states not to interfere with the use of technologies providing encryption and anonymity.[52]

Likewise, the UN Special Rapporteur on the right to privacy condemned the direction of ongoing reforms in the field in the **United Kingdom**,[53] and stated that "the security risks introduced by deliberately weakened encryption are vastly disproportionate to the gains".[54] The rapporteur commended the **Dutch** government for accepting and endorsing the importance of encryption in providing internet security and thereby ensuring the protection of the privacy and confidentiality of communications, whether pertaining to citizens, the government or companies.[55]

The Council of Europe's Recommendation CM/Rec(2016)5 on Internet freedom noted that "[t]he State does not prohibit, in law or in practice, anonymity, pseudonymity, confidentiality of private communications or the usage of encryption technologies", adding that "[i]nterference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 of the [ECHR]."[56]

That encryption may hamper the prevention, detection and prosecution of all kinds of crime is recognised at EU level. So is its effectiveness in providing secure data processing, a key element of data protection.[57] The terrorist attacks and questions about whether encryption software may have helped the perpetrators particularly prompted debates on the issue. In August, the interior ministers of **Germany** and **France** identified encrypted communication as a major challenge for investigations. They underlined the need to identify solutions that permit both effective investigations and the protection of privacy and the rule of law. To that end, they called on the Commission to consider putting forward legislation imposing uniform obligations on internet and electronic communication providers in terms of cooperation with authorities and, in particular, law enforcement agencies.[58]

In November, concerns about encryption triggered two developments at EU level. First, the European Judicial Cybercrime Network (EJCN) was launched.[59] It aims to facilitate the exchange, among judicial authorities, of information and good practices regarding cybercrime and cyber-enabled crime.[60] Encryption is a key challenge in investigating and prosecuting such crime.[61] Second, the Slovak Presidency prepared a report with a survey on Member States' experiences with, and views on, encryption-related matters.[62] Of the 25 Member States that responded, the majority thought that the EU should play a practical and facilitative – rather than legislative – role, focusing on improving technical skills among national authorities, exchanging information, and cooperation between national police, Eurojust, Europol and the EJCN.[63] In this respect, the Commission's Joint Research Centre, together with Europol and national law enforcement authorities, is already engaged in developing solutions for decryption techniques compliant with EU law.[64]

Towards the end of 2016, the Commission established a working group to look at the role of encryption in criminal investigations. It asked FRA to contribute alongside Europol, Eurojust and ENISA. The issue is likely to remain high on the agenda in 2017.

6.1.4. PNR Directive adopted but implementation proceeds slowly

The PNR Directive entered into force in May 2016, and Member States have two years to transpose it.[65] The Commission emphasised the importance of quickly implementing the instrument, which it considers important for achieving an effective and sustainable Security Union.[66] To this end, as part of the European Security Agenda, the Commission provided € 70 million in additional funding for Member States to establish national PNR systems.[67]

Despite improvements, fundamental rights concerns remain

The final text of the directive reflects some of the recommendations FRA outlined in its 2011 opinion on the EU PNR data collection system.[68] As reported in FRA's *Fundamental Rights Report 2016*,[69] the directive includes an exhaustive list of what is considered serious crime for purposes of the directive, so that the grounds for law enforcement authorities' use of PNR data are foreseeable and accessible by every individual. That said – although the grounds permitting the use of PNR data are restricted to terrorist offences and serious crime – the list of offences is quite extensive, including 26 different offences.[70]

The directive also reflects some points FRA's 2011 opinion made concerning necessity, proportionality and data protection safeguards of the PNR system.[71] Data protection safeguards in the final text are more enhanced than in the Commission's initial proposal in 2011. A good example is the addition of the requirement for Member States to appoint data protection officers to their national Passenger Information Units.[72] However, despite considering necessity and proportionality, the text does not include fundamental rights-relevant indicators as part of the Commission's procedure for annually reviewing the statistical information on PNR data provided to the Passenger Information Units, as FRA initially recommended.[73] Accordingly, any interferences with the right to privacy and data protection or the right to non-discrimination when applying the directive are not reviewed.

For retention of PNR data to be proportionate and not go beyond what is necessary, legal frameworks must distinguish categories of data according to their usefulness and outline objective criteria that determine the duration of retention.[74] The PNR Directive envisages data retention for five years.[75] That said, it refers neither to specific categories of data nor to any specific grounds for such a long retention period. The Advocate General highlighted the absence of these elements, among others, in the Opinion on the *Agreement between the EU and Canada for transfer of PNR data*[76] when examining its compatibility with the EU Charter of Fundamental Rights.[77] The Advocate General concluded that, insofar as the agreement does not meet the necessity and proportionality requirements, as well as other data protection safeguards, it cannot enter into force in its current form. The CJEU will deliver its ruling in this case in 2017. Although it concerns the EU-Canada PNR scheme, the court's finding will certainly be relevant to the EU PNR scheme as well as the PNR Directive.

The application of the PNR Directive will ultimately depend on how Member States incorporate its provisions into national law. In light of the potential

deficiencies, Member States could, for example, add to their national laws the missing fundamental rights-relevant indicators for the review procedure by the Commission. Furthermore, the directive allows Member States to extend the application of the PNR system to flights within the EU at their own discretion.[78] It remains to be seen how Member States will exercise this discretion, considering that the right to free movement must be unequivocally respected and may be restricted only on grounds of public policy, public security or public health, taking into account necessity and proportionality.[79]

Implementation proceeds at slow pace

Despite the Commission's emphasis on fast implementation, the majority of Member States have not advanced particularly far in transposing the directive.

Of the 12 Member States that received financial support from the Commission in 2015 to establish national PNR systems,[80] only **Bulgaria**, **Latvia**[81] and **Slovenia** have proceeded to do so. **Bulgaria**'s new rules, in force since February 2016, include many provisions implementing the PNR Directive.[82]

Four Member States established national PNR systems before adoption of the PNR Directive: **Belgium**, **France**, **Hungary** and the **United Kingdom**. While Belgium and France are currently adjusting their legislation to the EU PNR system, the **United Kingdom** has not taken any steps towards implementation of the new directive. **Belgium** is finalising the legislation for its national PNR system; several members of the Belgian parliament and the European Commission have expressed concern about the legal text, questioning its appropriateness because it goes far beyond the European directive by including rail, maritime and road transport.[83] **France** finalised the technical adaptations to the PNR Directive; the new rules entered into force and will apply gradually from the end of 2016 onwards.[84] **Hungary** already adopted its first national PNR legislation in 2013[85] and the parliament adopted the necessary amendment for the implementation of the PNR Directive in November 2016.[86]

Of the Member States without national PNR systems, only four have already taken steps to initiate legislative procedures to implement the PNR Directive or are in the process of doing so. These are **Cyprus**, **Germany**,[87] **Luxembourg**[88] and **Slovakia**.

Although Member States pushed for the creation of an EU PNR data collection system as a response to 'foreign terrorist fighters' and the Paris attacks, 17 Member States do not appear to prioritise implementing the PNR Directive. The slow pace of implementation could relate to differing terrorism threat levels and the varying importance of personal data protection in Member States.

On 28 November 2016, the Commission published a detailed EU PNR implementation plan[89] "to tackle some of the problems that have emerged in preparing for effective implementation by spring 2018".[90] Meanwhile, the Council of Europe Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data in September adopted an opinion on the "Data protection implications of the processing of Passenger Name Records";[91] it provides complementary guidance on data protection safeguards applicable to third countries that are parties to the convention.

6.2. EU legal framework attunes itself to digitalisation, Member States slowly adapting

> *"Being European means the right to have your personal data protected by strong, European laws. Because Europeans do not like drones overhead recording their every move, or companies stockpiling their every mouse click. This is why Parliament, Council and Commission agreed in May this year a common European Data Protection Regulation. This is a strong European law that applies to companies wherever they are based and whenever they are processing your data. Because in Europe, privacy matters. This is a question of human dignity."*
>
> *European Commission, Juncker, J.-C. (2016), 'State of the Union address 2016', Speech/16/3043, 14 September 2016*

6.2.1. A modern and strengthened European data protection law

In April 2016, after more than four years of negotiation, the EU legislators adopted the data protection reform. The reform has the ambitious goal of adapting the European legal framework governing the protection of personal data to the realities and challenges arising from an ever more data-driven society. It consists of the General Data Protection Regulation (GDPR)[92] and the Police Directive.[93] The GDPR will apply as of 25 May 2018, and Member States have until 6 May 2018 to incorporate the Police Directive into national law.

The first crucial clarification brought about by the GDPR concerns the territorial application of EU law. The regulation now clearly states that it applies to all processing of EU residents' personal data, regardless of whether or not such processing takes place in the territory of the Union. The GDPR also simplifies several procedures. For example, it removes companies' obligation to notify data protection authorities (DPAs) of their processing activities: undertakings are now required to record such processing, and are to deliver them to DPAs only upon request. Small and medium-size businesses or organisations are exempted from this requirement, except in certain enumerated situations.

Moreover, the regulation increases the availability of effective remedies. Notable novelties include the possibilities for individuals to seek remedies in their country of residence and for third parties to initiate collective claims. DPAs are now also able to impose significant fines on data controllers: while current national legislation implementing the 1995 directive generally sets up maximum fines under € 1 million, the GDPR allows for compensation up to € 20 million or 4 % of the total worldwide annual turnover, whichever is greater.

The Police Directive seeks to facilitate information exchange in criminal law enforcement. Criteria for exchanges of information between national police and judicial authorities are harmonised to facilitate processes and ultimately increase efficiency in this field. The Police Directive includes many of the reforms introduced by the GDPR, such as the implementation of 'data protection by design' measures, the obligation to notify people of breaches, and clarifications of the processor's liability and requirements.

The reforms also enhanced the powers of DPAs. They emphasise cooperation and coordination among these authorities to ensure consistent application of the data protection legislation across EU Member States. Several mechanisms pursue this aim: the establishment of a lead supervisory authority (referred to as the 'one-stop-shop' principle); the consistency mechanism; and the replacement of the Article 29 Working Party with a new independent EU body, the European Data Protection Board (EDPB). The Police Directive also clarifies DPAs' tasks and powers. In particular, DPAs are granted corrective powers over controllers and processors, and they may impose temporary or permanent bans on illegal data processing. DPAs are also entrusted with dealing with complaints lodged by data subjects. While this broadened range of powers is welcome, it will require additional resources for DPAs.

Overall, the GDPR aims to eliminate most discrepancies in Member States' legal frameworks, such as regarding legally enforceable rights; obligations and responsibilities of data controllers and processors; powers and competences of DPAs; and available sanctions in case of violations. It reforms and enhances key principles ensuring effective personal data protection.

Moreover, the regulation will significantly affect any future developments in the data protection field. All new legislation has to reflect the changes brought by the GDPR – as, for instance, in the cases of the recently adopted Network and Information Systems (NIS) Directive[94] and the EU-US Privacy Shield, once the GDPR applies fully.[95] The CJEU will ultimately decide on the latter's compliance with the new principles of the GDPR in a case brought by the advocacy group Digital Rights Ireland in September 2016.[96] In the meantime, Maximilian Schrems is continuing his case[97] against Facebook before both the Irish courts and the CJEU – this time seeking to invalidate the ''Standard Contractual Clauses', the preapproved contractual agreements that Facebook uses to transfer the data of EU citizens to the USA.

6.2.2. Towards national reforms

The GDPR will apply uniformly across the EU. However, several opening clauses leave room for Member States to further develop some of the principles in the regulation. The **German** Ministry of the Interior has assessed the feasibility of making use of these clauses.[98] In most Member States, such as **Belgium**, **Finland**, **Germany**, **Greece** and **Sweden**, governments have set up working groups tasked with assessing whether or not new legislation will be needed.

Some Member States, such as **Bulgaria**, **Latvia** and **Poland**,[99] have announced that draft laws will be published in 2017 and are currently assessing the required adaptations, sometimes through stakeholder consultations (**Poland**). In **Belgium**, the government announced that the DPA will undergo an in-depth reform to ensure its transformation into a fully independent regulator.[100]

DPAs are both actors in, and beneficiaries of, the reform. Their mandate and responsibilities will expand. Therefore, most authorities are raising awareness about, and advising data controllers to facilitate, the reform. Recent studies in Lithuania, however, show that there is little awareness of the new regulation among both the general population and the private sector.[101]

In some Member States, such as **Hungary**,[102] **Lithuania**[103] and the **United Kingdom**,[104] DPAs developed a dedicated webpage on the regulation with special advice aimed at companies. Several DPAs, such as in **Lithuania**, **Luxembourg** and **Portugal**, organised public events or seminars on the reform. In some Member States, DPAs were already undergoing internal reforms prior to adoption of the GDPR, and are now continuing such reforms following the principles established by the new regulation. This is the case in **Ireland**, where the Data Protection Commissioner (DPC) is conducting an in-depth reform and expansion in terms of human, financial and operational resources.[105]

However, despite the large new set of competences granted to DPAs by the GDPR (see Section 6.2.1),[106] some Member States – such as **Croatia** and the **Czech Republic** – do not plan any reforms or adaptations of their DPAs.

6.2.3. An enhanced privacy framework

One of the key initiatives of the Digital Single Market (DSM) Strategy was to assess the e-Privacy Directive and adapt it to the digital and technological

developments of the market. The e-Privacy Directive was introduced in 2002 to address the requirements of new digital technologies and ease the advancement of electronic communications services by regulating spam, cookies, confidentiality of information and other specific issues that were not covered by the Data Protection Directive.

Between April 2016 and July 2016, the Commission conducted a public consultation and a Eurobarometer survey, aiming to assess the principles currently regulating electronic communication. The outcomes highlight the differences in the viewpoints of industry and civil society. Respondents from the industry were generally confident that the current directive is sufficient and has so far achieved its goals. Citizens and civil society, however, pointed out its narrow scope, the imprecision of the rules and the lack of strong enforcement incentives.[107] The failure to protect citizens from so-called 'cookie-walls', which prevent users from accessing online services if they do not consent to the storage of their data, was also noted.

A 2016 Eurobarometer survey on e-privacy showed that European residents value their privacy and expect it to be protected online. The privacy of their personal information, online communications and online behaviour was very important to the majority of the survey respondents.[108] This is in line with the 2015 Eurobarometer results, which showed that personal data protection is a very important concern for Europeans.

Eurobarometer survey underlines importance of e-privacy to Europeans

In a 2016 Eurobarometer survey on e-privacy, more than nine in 10 respondents said that it is important that personal information – such as pictures and contact lists – on their computer, smartphone or tablet can be accessed only with their permission, and that it is important that the confidentiality of their emails and online instant messaging is guaranteed (both 92 %). More than eight in 10 also said that it is important that tools for monitoring their activities online – such as cookies – can be used only with their permission (82 %). Six in 10 respondents already changed the privacy settings on their internet browser (e.g. to delete browsing history or cookies) (60 %). Respondents find it unacceptable to have their online activities monitored in exchange for unrestricted access to a certain website (64 %), or to pay not to be monitored when using a website (74 %). Almost as many say that it is unacceptable for companies to share information about them without their permission (71 %).

Source: European Commission (2016), Flash Eurobarometer 443: e-Privacy, Brussels, December 2016

The European Data Protection Supervisor (EDPS) and the Article 29 Working Party also agreed on the need to review the current legal framework with respect to e-privacy.[109] They highlighted the need to avoid any data retention requirement in the new legal framework, in conformity with the CJEU's *Digital Rights Ireland* ruling; pointed out that end-to-end encryption must be allowed; and recalled that consistency with, and non-duplication of, the GDPR standards should be ensured. To ensure such consistency and non-duplication, the EDPS recommended that legislators opt for a regulation instead of a directive as the legal basis for the updated act. The European Commission is expected to present a proposal in early 2017.

6.3. In search of a data retention framework

6.3.1. European regime on data retention still absent

As discussed in previous FRA Fundamental Rights Reports, whereas developments in 2014 focused on the question of whether or not to retain data, the prevalent voice among EU Member States in 2015 was that data retention is an efficient measure for ensuring national security and public safety and for fighting serious crime. In 2016, with an EU legal framework on data retention still lacking, the CJEU further clarified what safeguards are required for data retention to be lawful.

The joined cases *Tele2 Sverige* and *Home Secretary v. Watson*[110] scrutinised the conformity of the compulsory retention of electronic communications data with the e-Privacy Directive and the EU Charter of Fundamental Rights. The cases were brought as a consequence of the *Digital Rights Ireland* judgment, in which the CJEU laid down the requirements for data retention to be legal. The question was whether or not requiring telecommunication companies to store data on telephone calls, emails and websites visited by their clients violates the right to privacy and personal data protection. The court concluded that Member States cannot impose a general obligation on providers of electronic telecommunications services to retain data, but did not ban data retention altogether. Such retention is compatible with EU law if deployed against specific targets to fight serious crime. Retention measures must be necessary and proportionate regarding the categories of data to be retained, the means of communication affected, the persons concerned and the chosen duration of retention. Furthermore, national authorities' access to the retained data must be conditional and meet certain data protection safeguards. Table 6.1 presents an overview of the requirements.

This important judgment raises a number of questions in connection with other key acts, particularly the recently adopted PNR Directive (see Section 6.1.4). It provides guidance to legislators of the forthcoming proposed e-privacy reform but also further clarifies the safeguards needed in national or European data retention frameworks. In the absence of a European data retention regime, it remains to be seen how national legislators will react to the CJEU judgment, which could trigger additional litigation at Member State level.

Table 6.1: Data retention obligations in light of *Tele2 Sverige* and *Home Secretary v. Watson*

Targeted retention for purpose of fighting serious crime	
Required safeguards	**How to establish safeguards in national legislation**
Strictly necessary categories of retained data AND Strictly necessary means of communications affected AND Strictly necessary persons concerned AND Strictly necessary retention period	Clear and precise rules for scope and application of data retention measures AND Objective criteria establishing connection between data to be retained and objective pursued AND Objective evidence establishing a link with a public and serious crime, including by using a geographical criterion

Source: *FRA, 2017 (based on CJEU, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for Home Department v. Watson and Others, Joined Cases C-203/15 and C-698/15, 21 December 2016, paras. 108–112)*

The CJEU delivered another important judgment in *Breyer*,[111] which examined whether or not dynamic Internet Protocol (IP) addresses can qualify as personal data, and whether pursuing a legitimate interest can suffice to justify storing and processing personal data or this can be done only for the specific purposes outlined in the (now invalidated) Data Retention Directive. The CJEU concluded that such addresses may constitute personal data where the individual concerned can be identified, even where a third party must obtain additional data for the identification to take place.[112] (The French Court of Cassation similarly concluded in November 2016 that IP addresses constitute personal data.[113]) The CJEU also held that data retention is allowed as long as website operators are pursuing a legitimate interest when retaining and using their visitors' personal data. This is of major importance for data retention rules; it follows that online media service providers can lawfully store their visitors' personal data to pursue a legitimate interest, rather than just for the purposes previously outlined in the invalidated Data Retention Directive. Thus, the grounds justifying data retention have become broader.

6.3.2. Ambiguity persists at national level

Member States made only limited progress in adopting new legal frameworks for data retention to incorporate the requirements and safeguards set out in the CJEU's case law. Most seem reluctant to amend their national laws to conform to the *Digital Rights Ireland* and *Tele2* judgments. In the meantime, challenges against domestic data retention laws in Member States generally abated, though three characteristic cases challenging data retention were brought in **Germany**, the **Netherlands** and the **United Kingdom** in 2016.

In **Germany**, the Federal Constitutional Court rejected several expedited actions[114] brought by lawyers, doctors, journalists, members of parliament and media associations – i.e. professionals bound by professional secrecy – as users of telecommunication services for private or business purposes. The applicants were seeking to annul the new provisions on the retention of telecommunication metadata introduced by a 2015 law.[115] The court held that suspending the disputed provisions was not justified because the mere storage of data does not automatically cause serious disadvantages, even to persons bound by professional secrecy. The court further stressed that the conditions set out in the legislation for the use of data for criminal investigations meet the standards laid down in previous case law.

In the **Netherlands**, the Administrative Jurisdiction Division of the Council of State decided on an administrative action[116] against the Passport Act (*Paspoortwet*),[117] which allows the Dutch authorities to store in a database digital fingerprints obtained for new passports or identity cards. The Council of State referred the case to the CJEU for a preliminary ruling, but the court concluded that it could not review the matter because it does not fall within the scope of the European Passport Regulation.[118] The Council of State then decided that the long-term decentralised storage of digital fingerprints by the authorities is illegitimate.[119] However, this cannot prevent the authorities from refusing to issue a passport.

Finally, the **United Kingdom** Court of Appeal[120] reviewed a claim alleging that the retention of, and access to, sensitive personal data – in particular, on gender reassignment – by certain officials breached

the right to private life (Article 8 of the ECHR). The court dismissed the appeal, holding that although there was an interference with Article 8, it was proportionate. Specifically, the data were already in the public domain and would mostly be of no interest to those assessing them, and they would typically have no contact with the applicant. Additionally, disciplinary measures were provided for in case of any abuse of access by the officials.

Member States hesitant to revise national data retention laws

As previously noted, the majority of Member States consider data retention an efficient way to protect national security and public safety as well as to address crime. Given the CJEU's judgment in *Digital Rights Ireland*, although there is no strict legal obligation to do so, to ensure full respect for fundamental rights, the next step for Member States would be to reform their domestic legal frameworks and provide for the safeguards laid down by the CJEU. However, only four Member States enacted legislative amendments following the judgment and only six Member States are pursuing such amendments.

Figure 6.1 outlines the amendments in progress or enacted in 2016. As it illustrates, most governments responded to the CJEU's holding by introducing stricter access controls and specifying the types of crime justifying access to retained data. The remaining Member States have taken no steps to introduce fundamental rights safeguards in their domestic data retention regimes.

In **Belgium**, a new law has been in force since July 2016.[121] Given the concerns expressed during the legislative process,[122] it added strict safeguards and security measures. The law also clearly defines which authorities can access and retain data and for how long, and specifies the requirements for accessing three different categories of data.[123] However, the blanket retention of data by telecommunication providers has not been removed.[124] In **Slovakia**, a new law entered into force on 1 January 2016, abolishing the preventative blanket retention and storage of data by telecommunications companies and introducing all the safeguards prescribed by the CJEU.[125]

In **Denmark**, the government announced that preparations for revising data retention rules are underway, stating that the revised rules are currently under consideration and planned to be introduced in the fall of 2017.[126] The revised rules will take into consideration the CJEU's *Tele2* judgment.

In **Luxembourg**, the government introduced a bill amending the data retention regime in accordance with *Digital Rights Ireland* and restricting the possibilities of retaining data to the grounds specifically listed in the bill.[127] It was debated whether or not the bill contains a wider list of offences justifying retention beyond what is strictly necessary.[128] In the **United Kingdom**, the Investigatory Powers Act[129] provides for the Secretary of State to require communication service providers to retain relevant communications data for one or more of the statutory purposes for a period up to 12 months and specifies a number of safeguards in respect of data retention.

In **Hungary**, the government has not taken any steps to amend the Act implementing the Data Retention Directive.[130] However, the Hungarian parliament amended the Act on certain questions of electronic commercial services and information society services[131] to expand the scope of data retention. It introduced data retention obligations for electronic and IT service providers similar to those applicable under the Act implementing the Data Retention Directive. The new law obliges electronic and IT service providers that allow encrypted communication through their services to store all metadata related to such communications for one year.[132] It thus widens the scope of data retention.

All in all, Member States' progress on the issue since the CJEU's invalidation of the Data Retention Directive remains limited. This may partly be due to the absence of harmonised rules at EU level. Eurojust, the EU agency for judicial cooperation in criminal matters, has stated that, while data retention schemes are considered necessary tools in the fight against serious crime, there is a need to create an EU regime on data retention that complies with the safeguards laid down by the CJEU.[133] In any event, regardless of whether at European or national level: as long as data retention measures continue to be deployed, adequate protection measures must soon be implemented to prevent fundamental rights violations.

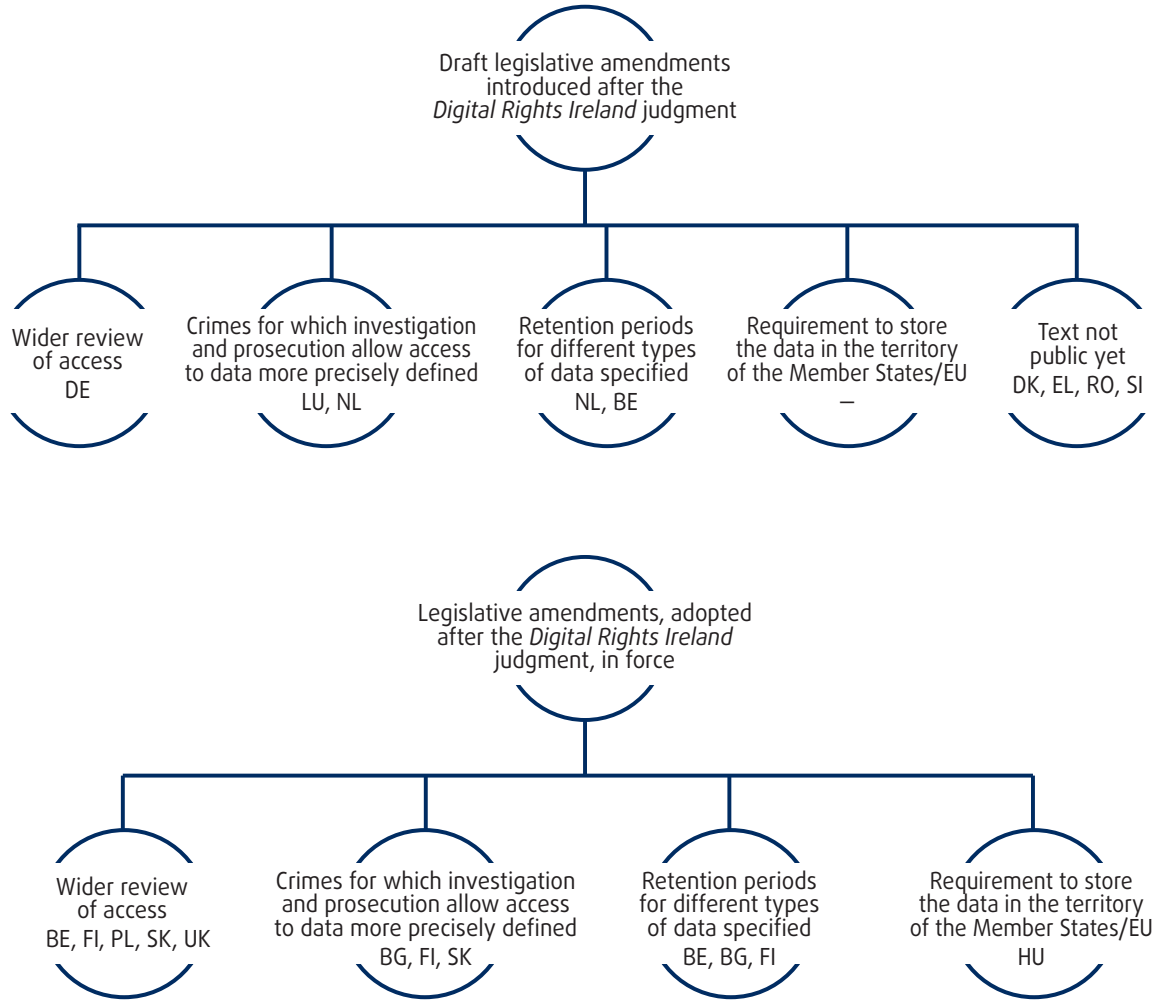
Promising practice

Auditing state bodies with access to communications data

In 2014, the Office of the Data Protection Commissioner (DPC) in **Ireland** completed an audit into the handling of information in the Garda Síorhána (police force), which included an examination of practices in relation to access to retained communications data. In 2016, the DPC expanded on this by auditing all state bodies with access to retained communications data. This is the first time that a comprehensive review of access to retained data has been carried out across the agencies.

For more information, see Lally, C. (2016), 'Garda use of powers to access phone data to be audited', Irish Times, 20 January 2016

Figure 6.1: Amendments to national data retention laws in 2016



Source: *FRA, 2017*

FRA opinions

FRA evidence, which builds on research on the protection of fundamental rights in the context of large-scale surveillance carried out at the European Parliament's request, shows that a number of EU Member States reformed their legal frameworks relating to intelligence gathering throughout the year. Enacted amid a wave of terrorist attacks, these changes enhanced the powers and technological capacities of the relevant authorities and may increase their intrusive powers – with possible implications for the fundamental rights to privacy and personal data protection. The Court of Justice of the European Union and the European Court of Human Rights provide essential guidance on how to protect best these rights. Legal safeguards include: substantive and procedural guarantees of a measure's necessity and proportionality; independent oversight and the guarantee of effective redress mechanisms; and rules on providing evidence of whether an individual is being subjected to surveillance. Broad consultations can help to ensure that intelligence law reforms provide for a more effective, legitimate functioning of the services and gain the support of citizens.

FRA opinion 6.1

EU Member States should undertake a broad public consultation with a full range of stakeholders, ensure transparency of the legislative process, and incorporate relevant international and European standards and safeguards when introducing reforms to their legislation on surveillance.

Encryption is perhaps the most accessible privacy enhancing technique. It is a recognised method of ensuring secure data processing in the General Data Protection Regulation (GDPR) as well as the e-Privacy Directive. However, the protection it provides is also used for illegal and criminal purposes. The spread of services providing end-to-end encryption further adds to the tension between securing privacy and fighting crime, as they, by design, prevent or make more difficult access to encrypted data by law enforcement authorities. To overcome this challenge, some Member States have started considering – or have already enacted – legislation that requires service providers to have built-in encryption backdoors that, upon request, allow access to any encrypted data by law enforcement and secret services. As noted by many, however, such built-in backdoors can lead to a general weakening of encryption, since they can be discovered and exploited by anyone with sufficient technical expertise. Such exposure could run counter to what data protection requires and could indiscriminately affect the security of communications and stored data of states, businesses and individuals.

FRA opinion 6.2

EU Member States should ensure that measures to overcome the challenges of encryption are proportionate to the legitimate aim of fighting crime and do not unjustifiably interfere with the rights to private life and data protection.

The General Data Protection Regulation, which will apply as of 2018, lays down enhanced standards for achieving effective and adequate protection of personal data. Data protection authorities will play an even more significant role in safeguarding the right to data protection. Any new legal act in the field of data protection will have to respect the enhanced standards set out in the regulation. For example, in 2016 the EU adopted an adequacy decision for the purpose of international data transfers: the EU-U.S. Privacy Shield. This decision explicitly states that the European Commission will regularly assess whether the conditions for adequacy are still guaranteed. Should such assessment be inconclusive following the entry into application of the General Data Protection Regulation, the decision asserts that the Commission may adopt an implementing act suspending the Privacy Shield. Furthermore, in 2016, the EU adopted its first piece of legislation on cyber security – the Network and Information Security Directive – and, in early 2017, in the context of the Digital Single Market Strategy, the Commission proposed an e-Privacy Regulation to replace the e-Privacy Directive.

FRA opinion 6.3

EU Member States should transpose the Network and Information Security Directive into their national legal frameworks in a manner that takes into account Article 8 of the EU Charter of Fundamental Rights and the principles laid down in the General Data Protection Regulation. Member States and companies should also act in compliance with these standards when processing or transferring personal data based on the EU-U.S. Privacy Shield.

Whereas developments in 2014 focused on the question of whether or not to retain data, it became clear in 2015 that Member States view data retention as an efficient measure for ensuring protection of national security, public safety and fighting serious crime. There was limited progress on the issue in 2016: while the EU did not propose any revised legislation in response to the Data Retention Directive's invalidation two years earlier, the CJEU developed its case law on fundamental rights safeguards that are essential for the legality of data retention by telecommunication providers.

FRA opinion 6.4

EU Member States should, within their national frameworks on data retention, avoid general and indiscriminate retention of data by telecommunication providers. National law should include strict proportionality checks as well as appropriate procedural safeguards so that the rights to privacy and the protection of personal data are effectively guaranteed.

The European Parliament Civil Liberties, Justice and Home Affairs Committee (LIBE) rejected the proposal for an EU Passenger Name Record (PNR) Directive in April 2013 due to concerns about proportionality and necessity, and a lack of data protection safeguards and transparency towards passengers. Emphasising the need to fight terrorism and serious crime, the EU legislature in 2016 reached an agreement on a revised EU PNR Directive and adopted the text. Member States have to transpose the directive into national law by May 2018. The adopted text includes enhanced safeguards that are in line with FRA's suggestions in its 2011 Opinion on the EU PNR data collection system. These include enhanced requirements, accessibility and proportionality, as well as further data protection safeguards. There are, however, fundamental rights protection aspects that the directive does not cover.

FRA opinion 6.5

EU Member States should enhance data protection safeguards to ensure that the highest fundamental rights standards are in place. This also applies to the transposition of the EU Passenger Name Record (PNR) Directive. In light of recent CJEU case law, safeguards should particularly address the justification for retaining Passenger Name Record data, effective remedies and independent oversight.

Index of Member State references

Endnotes

1 European Parliament, European Parliamentary Research Service (2016), *Foreign fighters – Member State responses and EU action*, Briefing, March 2016.

2 United Nations (UN), Human Rights Council, Cannataci, J. (2016), *Report of the Special Rapporteur on the right to privacy*, A/HRC/31/64, 8 March 2016, para. 23.

3 *Ibid.*, para. 9.

4 UN, Human Rights Council, Emmerson, B. (2016), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/HRC/31/65, 29 April 2016 para. 9.

5 Council of Europe, Parliamentary Assembly (PACE) (2016), *Combating international terrorism while protecting Council of Europe standards and values*, Resolution 2090 (2016), 27 January 2016, para. 16.7.

6 *Ibid.*

7 PACE (2016), *Terrorism: #NoHateNoFear, a PACE initiative*, 20 June 2016.

8 Council of Europe, Jagland, T. (2016), *State of Democracy, Human Rights and the Rule of Law – A Security Imperative for Europe*, p. 8.

9 Council of Europe, European Commission for Democracy through Law (Venice Commission) (2016), *Rule of law checklist*, CDL-AD(2016)007, 18 March 2016, pp. 31–33.

10 UN, Human Rights Council (2016), *Resolution on the protection of human rights and fundamental freedoms while countering terrorism*, A/HRC/33/L.27/Rev.1, 28 September 2016, para. 25.

11 UN, Human Rights Council (2016), *Report of the Working Group on the universal periodic review – Belgium*, A/HRC/32/8, 11 April 2016, Recommendations 138.71, 139.17 and 141.14.

12 UN, Human Rights Council (2016), *Report of the Working Group on the universal periodic review – Estonia*, A/HRC/32/7, 12 April 2016, Recommendation 123.45.

13 UN, Human Rights Council (2016), *Report of the Working Group on the universal periodic review – Latvia*, A/HRC/32/15, 14 April 2016, Recommendation 120.68.

14 UN, Human Rights Committee (2016), *Concluding observations on the sixth periodic report of Denmark*, CCPR/C/DNK/CO/6, 15 August 2016, paras. 27–28.

15 UN, Human Rights Committee (2016), CCPR/C/POL/CO/7, *Concluding observations on the seventh periodic report of Poland*, 23 November 2016, paras. 39–40.

16 UN, Human Rights Committee (2016), *Concluding observations on the seventh periodic report of Sweden*, CCPR/C/SWE/CO/7, 28 April 2016, paras. 36–37.

17 UN, Human Rights Committee (2016), *Concluding observations on the seventh periodic report of Sweden*, CCPR/C/SWE/CO/7, 28 April 2016, para. 36.

18 ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 January 2016, para. 70.

19 Article 29 Data Protection Working Party (2016), Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 April 2016, p. 8.

20 ECtHR, *Centrum För Rättvisa v. Sweden*, No. 35252/08; ECtHR, *Big Brother Watch and Others v. the United Kingdom*, No. 58170/13; ECtHR, *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*, No. 62322/14; ECtHR, *10 Human Rights Organisations and Others v. the United Kingdom*, No. 24960/15; ECtHR, *Breyer v. Germany*, No. 50001/12. All these cases are at the stage of having been communicated to the respective governments.

21 European Commission, Juncker, J.-C. (2016), 'Juncker after Brussels terror attacks: "We need a security union"', Press conference, 24 March 2016.

22 King, J. (2016), 'Introductory remarks by Commissioner-designate Sir Julian King to the LIBE Committee', Press release, Strasbourg, 12 September 2016.

23 European Commission (2016), *High Level Expert Group on Information Systems and Interoperability – Interim report by the chair of the high-level expert group*, December 2016, pp. 2–3.

24 European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2016), 'Exchange of views with Gilles de Kerchove, EU Counter-Terrorism Coordinator (CTC) on the fight against terrorism and recent attacks in Member States', Committee meeting, LIBE/8/02582, 26 September 2016.

25 *Ibid.*

26 European Commission, (2016), *Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders*, COM(2016) 602 final, Brussels, 14 September 2016, p. 14.

27 *Ibid.*, pp. 14–15.

28 *Ibid.*, p. 12 and fn. 30.

29 European Commission (2016), *Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union*, COM(2016) 230 final, Brussels, 20 April 2016, p. 10.

30 European Council (2016), *Bratislava Declaration and Roadmap*, 16 September 2016.

31 *Ibid.*

32 European Commission, Juncker, J.-C. (2016), *State of the Union*, 14 September 2016, p. 6.

33 Poland, Anti-terrorist Act (*Ustawa o działaniach antyterrorystycznych*), 10 June 2016.

34 Romania, Emergency Ordinance No. 6/2016 on Certain Measures for the Enforcement of Technical Surveillance Warrants in Criminal Cases (*Ordonanța de urgență nr. 6/2016 privind unele măsuri pentru punerea în executare a mandatelor de supraveghere tehnică dispuse în procesul penal*), 11 March 2016.

35 United Kingdom, Joint Committee on the Draft Investigatory Powers Bill (2016), *Draft Investigatory Powers Bill – Report*, 11 February 2016, p. 26.

36 See, for example, United Kingdom, Joint Committee on the Draft Investigatory Powers Bill (2015–2016), *Oral Evidence*; United Kingdom, Joint Committee on the Draft Investigatory Powers Bill (2015–2016), *Written Evidence*.

37 Anderson, D., Q.C. (2015), *A Question of Trust*; Anderson, D., Q.C. (2016), *Report of the Bulk Powers Review*.

38 Ireland, Department of Justice and Equality (2016), 'Statement by the Minister for Justice and Equality in relation to access to telephone records', 19 January 2016.

39 House of Representatives (2016), 'Magazine La chambre', *LaChambre.be*, p. 3; House of Representatives, Text adopted by the temporary 'Fight against Terrorism' Commission – Bill concerning complementary measures related to the fight against terrorism (*Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme/ Wetsontwerp inzake aanvullende maatregelen ter bestrijding van terrorisme*), 14 April 2016.

40 Belgium, Proposition to establish a Parliamentary Investigative Commission responsible for examining the circumstances leading to the terrorist attacks of

22 March 2016 in Brussels National Airport and Maelbeek metro station (*Proposition visant à instituer une commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste/Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven BrusselNationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging*), 11 April 2016.

41 Germany, Act on Signals Intelligence Gathering in Germany of Foreigners Abroad (*Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes*), 2016, Section 2.

42 Italy, Draft Law No. 2067 concerning the Reform of the Criminal Code and Criminal Procedure Code in order to enhance judicial guarantees and the right to a fair length of judicial proceeding and to the re-integration aim of detention (*Modifiche al codice penale e al codice di procedura penale per il rafforzamento delle garanzie difensive e la durata ragionevole dei processi nonché all'ordinamento penitenziario per l'effettività rieducativa della pena*), 3 August 2016.

43 Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (*Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών*), No. 75(I)/2016.

44 United Kingdom, Investigatory Powers Act 2016, 29 November 2016, Sections 61–62.

45 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Art. 1.2., 57.2 and 57.3.

46 Hungary, Act LXIX of 2016 on the amendment of certain acts related to counter-terrorism (*2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról*), 17 July 2016, Article 16.

47 United Kingdom, Investigatory Powers Act 2016, 29 November 2016, Sections 227 and 240.

48 *Ibid.*, Section 23.

49 France, Law No. 2016-1767 of 19 December 2016 extending the application of Law No. 55-385 of 3 April 1955 concerning the state of emergency (*Loi n° 2016-1767 du 19 décembre 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence*), 19 December 2016.

50 France, Interior Security Code (*Code de la sécurité intérieure*), Art. 851-2.

51 Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Neumann, P.G., Landau, S., Rivest, R.L., Schiller, J.I., Schneier, B., Specter, M. and Weitzner, D.J. (2015), 'Keys Under Doormats: mandating insecurity by requiring government access to all data and communications', Journal of Cybersecurity, p. 10.

52 UN, Human Rights Council (2016), *Resolution on the safety of journalists*, A/HRC/33/L.6, 26 September 2016, para. 13. See also UN, Human Rights Council, Kaye, D. (2016), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/32/38, 11 May 2016, para. 62.

53 UN, General Assembly (GA) (2016), *Report of the Special Rapporteur on the right to privacy*, A/71/368, 30 August 2016, para. 34.

54 *Ibid.*, para. 32.

55 Netherlands, Ministry of Security and Justice (2016), 'Cabinet's view on encryption', Letter from the Ministry of Security and Justice to the President of the House of Representatives of the States General, 4 January 2016.

56 Council of Europe, Committee of Ministers (2016), Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom, 13 April 2016, para. 4.1.7.

57 See, for example, Europol (2016), The Internet Organised Crime Threat Assessment (IOCTA) 2016, p. 46; Europol/European Union Agency for Network and Information Security (ENISA) (2016), 'On lawful criminal investigation that respects 21st Century data protection – Europol and ENISA Joint Statement', 20 May 2016; Eurojust (2016), 'Conclusions of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union', 11th Meeting, The Hague, 3 June 2016, pp. 2–3.

58 France, Ministry of the Interior (2016), 'Initiative franco-allemande sur les enjeux clés de la coopération européenne dans le domaine de la sécurité intérieure', 23 August 2016, pp. 3–4.

59 Eurojust (2016), 'Kick-off meeting for the European Judicial Cybercrime Network', Press release, 25 November 2016.

60 Council conclusions on the European Judicial Cybercrime Network, Luxembourg, 9 June 2016.

61 Eurojust (2016), 'Kick-off meeting for the European Judicial Cybercrime Network', Press release, 25 November 2016.

62 Council of the European Union (2016), *Encryption: Challenges for Criminal Justice in Relation to the Use of Encryption*, 14711/16, 23 November 2016.

63 *Ibid.*

64 European Commission (2016), 'Encrypted material: a challenge for law enforcement investigations', 10 June 2016.

65 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119 (PNR Directive).

66 European Commission (2016), 'European Agenda on Security: First report on progress towards an effective and sustainable Security Union', Press release, IP/16/3367, Brussels, 12 October 2016.

67 *Ibid.*

68 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, p. 113.

69 FRA (2016), *Information Society, Privacy and Data Protection,* Vienna.

70 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, pp. 16, 22.

71 *Ibid.*, p. 113.

72 *Ibid.*, p. 20.

73 *Ibid.*, p. 21.

74 CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014, paras. 63–64.

75 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119 (PNR Directive), Art. 12.

76 European Commission (2013), *Proposal for a Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of passenger name record data*, COM(2013) 528 final, Brussels, 18 July 2013.

77 CJEU, 'Opinion of Advocate General Mengozzi',Opinion 1/15, 8 September 2016.

78 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119 (PNR Directive), Art. 2.

79 Directive (EC) 2004/38 of the European Parliament and of the Council of 29 April 2004 on the rights of citizens of the Union and their family members to move and reside freely within the territory of the Member States, OJ 2004 L 158 (Free Movement Directive), Art. 27; Court of Justice of the European Union (CJEU), *ZZ v. Secretary of State for the Home Department*, Case C-300/11, 4 June 2013.

80 European Parliament, European Parliamentary Research Service (2015), 'The proposed EU Passenger Name Records (PNR) Directive revived in the new security context', Briefing, April 2015.

81 Latvia, annotation of the Draft law ''On Aircraft Passenger Data Processing'Processing' (*Gaisa kuģu pasažieru datu apstrādes likums*), 14 June 2016.

82 Bulgaria, Amendments to the State Agency for National Security Act (*Закон за изменение и допълнение на Закона за Държавна агенция „Национална сигурност"*), 23 February 2016.

83 Belgium (2016), 'Le projet de loi PNR est renvoyé au Conseil d'Etat', *Le Vif*, 24 November 2016.

84 France, Interior Security Code (*Code de la sécurité intérieure*), Article L232-1; France, Government (*Gouvernement*), 'Adoption of the European PNR, an essential stage in the reinforcement of the fight against terrorism' (*Adoption du PNR européen, une étape indispensable dans le renforcement de 'a lutte contre le térrorisme*), 15 April 2016.

85 Hungary, '*2013. évi CXCVIII. törvény a nemzeti utasadat-információs rendszer létrehozása érdekében szükséges, valamint a rendőrséget érintő és egyes további törvények módosításáról*', 11 November 2013.

86 Hungary, *2016. évi CXVI. Törvény az egyes belügyi tárgyú törvények módosításáról*', 8 November 2016.

87 Germany, German Bundestag (*Deutscher Bundestag*) (2016), 'Geheimdienstkooperation gegen den Terrorismus', 1 June 2016.

88 Luxembourg, Ministry of Foreign and European Affairs (*Ministère des Affaires Etrangères et Européennes*), ''Report on the transposition of European Directives and the implementation of the law of the Union' (*Rapport sur la transposition des directives européennes et l'application du droit de l'Union*), 22 June 2016.

89 European Commission (2016), *Implementation Plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, SWD(2016) 426 final, Brussels, 28 November 2016.

90 European Commission, King, J. (2016), 'Opening remarks – Commissioner King participates in a structured dialogue at the Committee on Civil Liberties, Justice and Home Affairs in the European Parliament', Speech, Brussels, 8 November 2016

91 Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (T-PD) (2016), Opinion on the Data protection implications of the processing of Passenger Name Records, 19 August 2016.

92 Regulation (EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016.

93 Directive (EU)2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 4 May 2016.

94 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measure for a high common level of security of network and information systems across the Union, OJ 2016 L 194 (NIS Directive), OJ L 194, 19 July 2016.

95 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016 L207, 1 August 2016.

96 CJEU, *Action brought on 16 September 2016 – Digital Rights Ireland v Commission*, Case T-670/16.

97 Ireland, High Court, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems*, 2016/4809P, 19 June 2016.

98 Kühling, J., Martini, M., Heberlein, J., Kühl, B., Nink, D., Weinzierl, Q. and Wenzel, M. (2016), *Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf*, Münster, MV-Verlag.

99 Poland, Inspector General for the Protection of Personal Data (*Generalny Inspektor Ochrony Danych Osobowych*) (2016), '*Wyzwania związane z unijną reformą prawa ochrony danych osobowych*', Press release, 22 June 2016.

100 Belgium, Press Centre, '*Réforme de la Commission pour la protection de la vie privée*', Press release, 13 May 2016.

101 Lithuania, Human Rights Monitoring Institute (2016), *The Privacy Paradox: The Lithuanian Public's Perceptions of Data Protection*; Lithuania, Human Rights Monitoring Institute (2016), *The Preparedness of Lithuanian Business to Implement GDPR.The Preparedness of Lithuanian Business to Implement GDPR*.

102 National Authority for Data Protection and Freedom of Information (2016), 'Twelve steps in the preparation for the application of the General Data Protection Regulation' (*Felkészülés az Adatvédelmi Rendelet alkalmazására 12 lépésben*).

103 Lithuania, State Data Protection Inspectorate (*Valstybinė duomenų apsaugos inspekcija*) (2016), 'Data protection reform', News, 12 October 2016.

104 Information Commissioner's Office, Data protection reform.

105 Department of the Taoiseach, 'An Taoiseach and Minister Murphy Announce New Dublin Premises for the Office of the Data Protection Commissioner', 9 December 2015.

106 See also FRA (2016), *Fundamental Rights Report 2016*, Publications Office, Luxembourg, p. 108.

107 European Commission, *Full Report on the Public Consultation on the Evaluation and Review of the ePrivacy Directive*, 19 December 2016; European Commission (2016), *Flash Eurobarometer Interactive 443: e-PrivacyFlash Eurobarometer Interactive 443: e-Privacy*, 19 December 2016.

108 European Commission (2016), *Flash Eurobarometer Interactive 443: e-Privacy*, Brussels, 19 December 2016.

109 European Data Protection Supervisor, *Opinion 5/2016 Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)*, 22 July 2016; Art. 29 Working Party, *Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)*, 19 July 2016.

110 CJEU, *Tele2 Sverige AB v. Post-och telestyrelsen* and *Secretary of State for Home Department v. Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, 21 December 2016.

111 CJEU, *Patrick Breyer v. Bundesrepublik Deutschland*, Case C-582/14, 19 October 2016.

112 *Ibid.*, para. 49.

113 France, Court of Cassation (*Cour de Cassation*), *Arrêt No. 1184 du 3 novembre 2016*, 15-22.595, 3 November 2016.

114 Germany, Federal Constitutional Court (*Bundesverfassungsgericht*) (2016), 1 BvQ 55/15, 12 January 2016; Germany, Federal Constitutional Court (*Bundesverfassungsgericht*) (2016), 1 BvQ 42/15, 8 June 2016;Germany, Federal Constitutional Court (*Bundesverfassungsgericht*) (2016), 1 BvR 229/16, 8 June 2016.

115 Germany, Act for the introduction of an obligation to retain and of a maximum retention period for metadata (*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*), 18 December 2015.

116 Netherlands, Administrative Jurisdiction Division of Council of State (*Afdeling Bestuursrechtspraak Raad van State*), *Uitspraak op het hoger beroep van: [appellante], wonend te Den Haag, tegen de uitspraak van de rechtbank Den Haag van 23 maart 2011 in zaak nr. 10/5376 in het geding tussen: [appellante] en de burgemeester van Den Haag*, 25 May 2015.

117 Netherlands, Passport Act (*Paspoortwet*), 9 March 2014.

118 CJEU, CJEU*W.P. Willems and Others v. Burgemeester van Nuth and Others*, Joined Cases C-446/12 to C-449/12, 16 April 2015.

119 Netherlands, Administrative Jurisdiction Division of Council of State *(Afdeling Bestuursrechtspraak Raad van State)*, zaak nr. 201207583/1/A3 of 25 May 2016, par. 7.6.

120 United Kingdom, Court of Appeal (Civil Division), *R. (on the application of C) v. Secretary of State for Work and Pensions*, [2016] EWCA Civ 47, 9 February 2016.

121 Belgium, Act concerning the collection and retention of data in the electronic communications sector *(Loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques/Wet betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie*), 29 May 2016.

122 NURPA (2016), *Opinion from Datapanik, the Liga voor Mensenrechten, the Ligue des droits de l'Homme and NURPA concerning the data retention bill* (*Avis de Datapanik, la Liga voor Mensenrechten, la Ligue des droits de l'Homme et la NURPA concernant le projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques*), (DOC 54 1567/001), 15 February 2016.

123 Belgium, Act concerning the collection and retention of data in the electronic communications sector (*Loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques/Wet betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie*), 29 May 2016, Art. 4§3.

124 *Ibid.*

125 Slovakia, Act No. 397/2015 Coll. which for the purposes of the Criminal Code provides a list of substances with anabolic or other hormonal action and amending and supplementing certain laws (*Predpis č. 397/2015, ktorým sa na účely Trestného zákona ustanovuje zoznamlátok s anabolickým alebo iným hormonálnym účinkom a ktorým sa menia a dopĺňajú niektoré zákony*), 13 November 2015.

126 Denmark, Danish Government (*Regeringen*) (2016), *Lovgivning Folketingsåret 2016/2017*, October 2016.

127 Luxembourg, Bill 6763 to amend the Code of Criminal Procedure and the amended Act of 30 May 2005 regarding the protection of privacy in electronic communications (*Projet de Loi n°6763 portant modification du Code d'instruction criminelle et de la Loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques*), 7 January 2015.

128 Luxembourg, Parliament (*Chambre des Députés*), Legal Commission (*Commission juridique*), Minutes of the meeting of 9 March 2016 (*Procès-verbal de la réunion du 9 mars 2016*), pp. 3-4; Luxembourg, Bill 6763, Opinion by the Consultative Commission on Human Rights (*Avis de la Commission Consultative des Droits de l'Homme, CCDH*), 27 July 2015 ; Luxembourg, Bill 6763, Opinion by the Council of State (*Avis du Conseil d'Etat*), 10 July 2015, pp. 3-4.

129 United Kingdom, United Kingdom Parliament, Investigatory Powers Act 2015-16 to 2016-17, 29 November 2016.

130 Hungary, Act C of 2003 on electronic media (*2003. évi C. törvény az elektronikus hírközlésről hírközlesről),* 1 January 2004.

131 Hungary, Act CVIII of 2001 on certain questions of electronic commercial services and information society services (*az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről*), 23 January 2002.

132 Hungary, Act LXIX of 2016 on the amendment of certain acts related to counter-terrorism (*2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról*), Article 48, 17 July 2016.

133 Eurojust (2016), *Annual Report 2015*, The Hague, Eurojust, p. 59.