UN & CoE

January

24 January – Guidelines on big data adopted by the Consultative Committee of the Council of Europe's data protection convention (Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data)

February

24 February – UN Special Rapporteur on privacy issues a report to the UN Human Rights Council (A/HRC/34/60), focusing on the relation between privacy and surveillance activities, and the need for increased privacy-friendly oversight

March

22 March – UN Human Rights Council adopts a resolution on right to privacy in the digital age (A/HRC/34/L.7/Rev.1), calling on states to ensure that privacy rights are effectively respected, notably in context of digital communications and surveillance activities

April

28 April – Parliamentary Assembly of the Council of Europe (PACE) adopts Recommendation 2102 (2017) on Technological convergence, artificial intelligence and human rights, which calls upon the Committee of Ministers to better define regulations applying to robotics

May

5 May – UN OHCHR issues a report on ways to bridge the gender digital divide from a human rights perspective (A/HRC/35/9), which insists on the crucial importance of ensuring that new technologies do not exacerbate gender discrimination

June

22 June – In *Aycaguer v. France* (No. 8806/12), the ECtHR holds that being convicted for refusing to be registered in the national automated registry of genetic fingerprints is contrary to the right to respect for private life (Article 8 of the ECHR)

27 June – In *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (No. 931/13), the ECtHR holds that banning mass publication of personal tax data in Finland did not violate the right to freedom of expression (Article 10 of the ECHR)

July

August

September

5 September – In *Bărbulescu v. Romania* (No. 61496/08), the ECtHR holds that states should ensure that, when an employer takes measures to monitor employees' communications, these are accompanied by adequate and sufficient safeguards against abuse (Article 8 of the ECHR)

October

19 October – Report of the UN Special Rapporteur on the right to privacy to the 72nd Session of the UN General Assembly (A/72/540), focusing on Big Data and Open Data, highlights the need for better and clearer regulatory frameworks for the use of new technologies

October – Council of Europe publishes its new Internet Literacy Handbook (ILH) meant to support children, parents, teachers and policymakers of the 47 member states in making positive use of the internet

November

28 November – In *Antovic and Mirkovic v. Montenegro* (No. 70838/13), the ECtHR holds that video surveillance of university auditoriums amounted to an interference with the applicants' right to privacy and was incompatible with Article 8 of the ECHR, since domestic authorities failed to show any legal justification for the surveillance measure

December

EU

January

10 January – European Commission adopts a Proposal for a Regulation of the European Parliament (EP) and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications or e-Privacy Regulation)

10 January – European Commission adopts a Proposal for a Regulation of the EP and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No. 1247/2002/EC (EU institutions data protection Regulation)

February

March

14 March – EP adopts a Resolution on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement, insisting on crucial importance of respecting data protection principles to ensure both effectivity of, and trust in, big data techniques

April

4/5 April – Article 29 Working Party adopts final guidelines on right to data portability, designation on the lead supervisory authority and on Data Protection Officers

6 April – LIBE Committee adopts Resolution 2016/3018(RSP) on EU–US Privacy Shield: MEPs alarmed at undermining of privacy safeguards in the US

24 April – EDPS issues Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (e-Privacy Regulation)

May

June

July

26 July – CJEU issues Opinion 1/15 on the envisaged EU-Canada Agreement on the transfer and processing of passenger name record data (PNR Agreement), stating that the agreement could not be concluded as its current form is incompatible with the EU Charter of Fundamental Rights

August

September

13 September – European Commission and High Representative for Foreign Affairs and Security Policy adopt a joint communication to the European Parliament and the Council on '*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*'

October

3/4 October – Article 29 Working Party adopts final guidelines on data protection impact assessment and on administrative fines

18 October – Report of European Commission on the first annual review of the Privacy Shield concludes that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States; practical implementation of the Privacy Shield framework can be further improved to ensure that the guarantees and safeguards provided therein continue to function as intended

November

December

7 Information society, privacy and data protection

For both technological innovation and protection of privacy and personal data, 2017 was an important year. Rapid development of new technologies brought as many opportunities as challenges. As EU Member States and EU institutions finalised their preparatory work for the application of the EU Data Protection package, new challenges arose. Exponential progress in research related to 'big data' and artificial intelligence, and their promises in fields as diverse as health, security and business markets, pushed public authorities and civil society to question the real impact these may have on citizens – and especially on their fundamental rights. Meanwhile, two large-scale malware attacks strongly challenged digital security. The EU's recent reforms in the data protection and cybersecurity fields, as well as its current efforts in relation to e-privacy, proved to be timely and relevant in light of these developments.

7.1. Data protection and privacy developments

The General Data Protection Regulation (GDPR)[1] and the Data Protection Directive for Police and Criminal Justice Authorities[2] (together, the data protection reform package) were published in May 2016[3] and come into effect in May 2018. Throughout 2017, EU Member States adapted their national frameworks to the new legislation, and national data protection authorities – cooperating within the Article 29 Working Party – provided guidelines on the new rules. The European Commission presented proposals for two regulations, the EU institutions data protection Regulation and the e-Privacy Regulation. These would replace the existing regulation and directive on these matters, respectively, to update the regulatory framework in line with the GDPR.

The GDPR will apply as of 25 May 2018. As a regulation rather than a directive, it will be directly applicable. However, it allows Member States to implement national legislation through a number of so-called 'opening clauses', thereby providing some flexibility.[4]

Member States are also required to incorporate into their national law before 6 May 2018 the Data Protection Directive for Police and Criminal Justice Authorities. It seeks to facilitate information exchange and ensure a high level of personal data protection in the context of criminal law enforcement.

7.1.1. National implementation of EU data protection reform enters final stretch

The long-awaited data protection reform follows four years of difficult negotiations. The substantial changes introduced by the GDPR and the Data Protection Directive for Police and Criminal Justice Authorities justified the long implementation period of two years. **Austria**[5] and **Germany**[6] already have in place the implementing legislation for the regulation and the directive, while the majority of EU Member States have submitted legislative proposals to public consultation, as FRA recommended in its *Fundamental Rights Report 2017*.[7]

Some EU Member States addressed the potential impact of the GDPR on the tasks and powers of their national data protection authorities (DPAs), as independent oversight bodies, in 2017. The GDPR[8] and the Data Protection Directive for Police and Criminal Justice Authorities[9] reinforce the independence of DPAs, ensuring that

they have the human, technical and financial resources, premises and infrastructure necessary for the effective performance of their tasks and exercise of their powers. In the **Netherlands**, a report commissioned by the Dutch DPA highlighted the need to significantly increase the first estimate of the DPA's budget to cope with the new requirements of the GDPR.[10]

> *"Member States need to equip DPAs to act independently as centres of excellence for protecting individuals' rights and interests. At the moment, there are major disparities in the budgets for individual authorities in proportion to the number of people they are meant to protect: from 50 EUR per 1000 population in one Member State to 7,600 EUR per 1000 population in another."*
>
> *European Data Protection Supervisor, blog post, 7 December 2017*

DPAs have also been working at EU level to address the challenges in the implementation of the GDPR through the Article 29 Working Party (WP29), the institutional coordination mechanism created by Directive 95/46/EC (Data Protection Directive). The WP29 has produced different guidelines clarifying compliance requirements for controllers and processors, such as the Guidelines on the right to portability, on Data Protection Officers, on the designation of the lead supervisory authority, on Data Protection Impact Assessments, and on the administrative fines on data breach notification.[11] The adoption of the final version of those guidelines followed public consultations open to stakeholders.

Promising practice

Helping controllers conduct data protection impact assessments

The French DPA (*Commission nationale de l'informatique et des libertés*, CNIL) developed in 2017 an open software that helps controllers to conduct a Data Protection Impact Assessment (DPIA), which is a "process designed to manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them".* This software provides a contextual database accessible at any time during the execution of the impact assessment. Its contents, based on the GDPR, the DPIA guides and CNIL's Security Guide, adapt to the elements of the treatment under study.

**Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), wp248, 4 April 2017.*

For more information, see the website of the French DPA.

Senior and vulnerable citizens: enhancing awareness

The GDPR tasks DPAs with promoting public awareness and understanding of the risks, rules, safeguards and rights related to data processing. Notably, DPAs are to give particular attention to activities addressed specifically to children.[12] Children's awareness has a direct impact on their capacity to give consent for the processing of their personal data.[13]

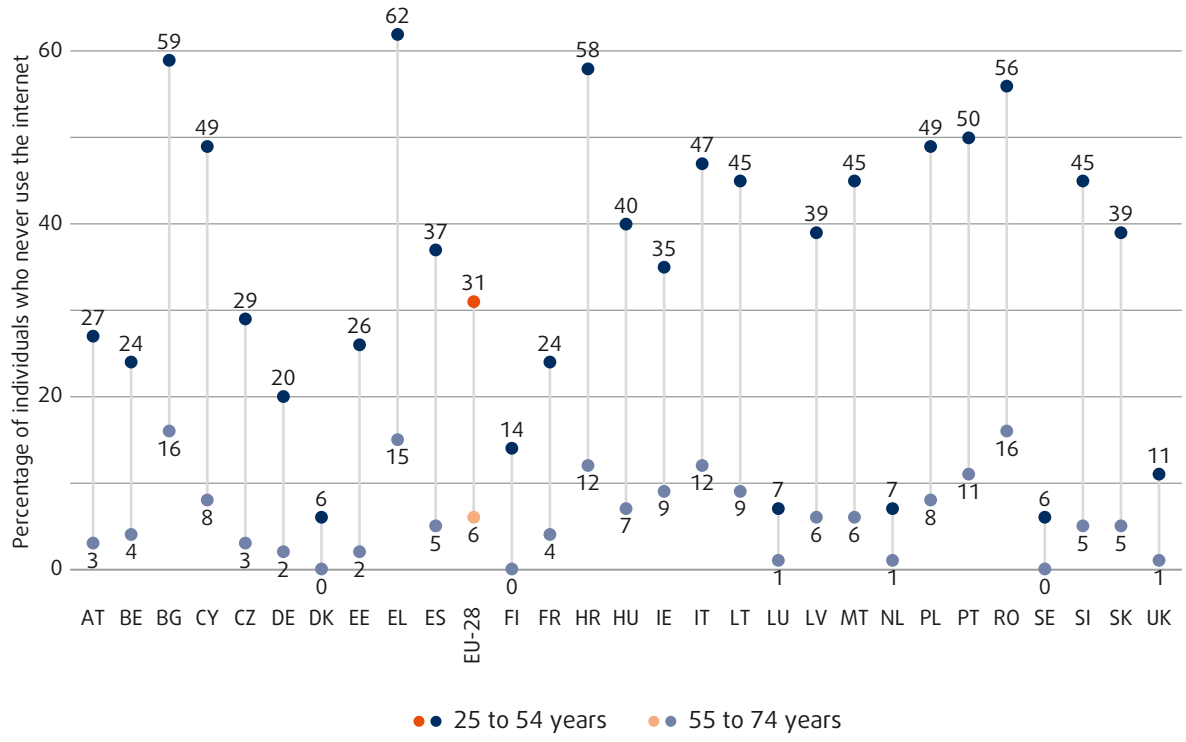
Indeed, one of the GDPR's relevant opening clauses allows Member States to specify the conditions applicable to a child's consent in relation to information society services. According to Article 8 of the GDPR, where the child is below the age of 16 years, such processing shall be lawful on the basis of consent only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. However, Member States may set by law a lower age for those purposes, provided that this is not below 13 years. Several Member States, such as the **Czech Republic**, **Denmark**, **Estonia**, **Ireland**, **Poland**, **Spain**, **Sweden** and the **United Kingdom**, proposed in 2017 to reduce the minimum age requirement to 13 years. **Austria** opted for 14 years.[14]

The age requirements for children to consent to the processing of their personal data are very diverse. (For more information, see FRA's mapping of minimum age requirements[15] concerning the rights of the child in the EU.) However, the age and maturity of the child, linked to their fundamental right to express their views freely on matters that concern them (Article 24 of the Charter), must be taken into account, and complemented with other positive obligations of public and private institutions considering the best interest of the child. Thus, Article 57 (1) (b) of the GDPR gives DPAs the task of promoting children's awareness and understanding of risks, rules, safeguards and rights related to data processing.

Age remains linked to the level of use of new technologies in most EU Member States, as shown in Figure 7.1. **Denmark**, **Luxembourg**, the **Netherlands**, **Sweden** and the **United Kingdom** have a low 'digital divide' of less than 10 % between the proportions of individuals in different generations who in 2017 had never used the internet. The average difference between generations for the EU-28 is 25 %.

The average number of people in the EU who never use the internet has decreased significantly since 2010, especially for older persons (see Figure 7.2). This is a major positive trend, as digital illiteracy is a key factor of vulnerability in relation to the level of awareness about the risks and the rights of individuals in the EU while using new technologies. In **Estonia**, the strong governmental push for digital uptake across various sectors was a key issue during the Estonian EU Presidency; FRA took part in those efforts, working to ensure recognition of fundamental rights in digitalisation.

Figure 7.1: Individuals never using the internet in 2017, by age group (%)



Source: *FRA, 2018 (based on Eurostat data extracted on 25 January 2018)*

7.1.2. Passenger Name Records collection needs safeguards

The Passenger Name Record (PNR) Directive (2016/681)[16] allows air carriers to transfer PNR data of passengers, and EU Member States (all but Denmark, who opted out) to process these data for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

At the end of 2017, significant disparities remained between EU Member States' progress in setting up their national PNR systems: **Belgium**,[17] **Germany**[18] and **Hungary**[19] have transposed the PNR Directive, while the other Member States are preparing the ground for its transposition with relevant legislation.[20]

The EU has concluded PNR agreements with the USA and Australia, and negotiated another one with Canada. However, on 26 July 2017, the CJEU[21] deemed the envisaged PNR Agreement between Canada and the EU incompatible with the Charter in so far as it does not preclude the transfer of sensitive data from the EU to Canada and the use and retention of that data. FRA raised similar concerns in its 2011 Opinion and its *Fundamental Rights Report 2017*.[22] Notably, the court declared that the continued storage of the PNR data of all air passengers after the passengers' departure was not limited to what is strictly necessary, and therefore should be limited to the data of passengers who may objectively be held to present a terrorism or serious transnational crime risk.[23]

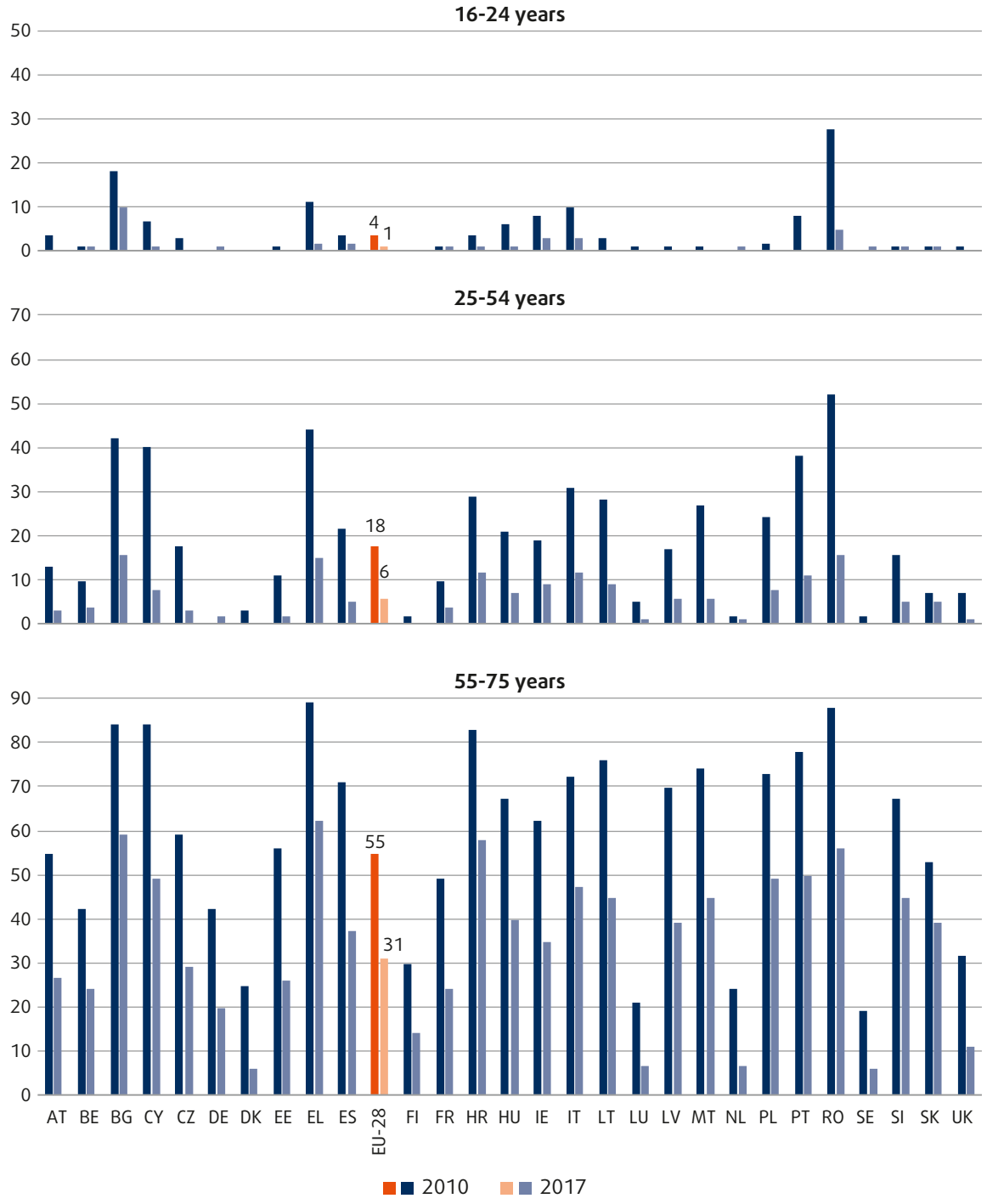
7.1.3. Draft e-Privacy Regulation: the latest EU proposal to modernise data protection rules

© Stock.adobe.com (KNEEo)

The e-Privacy Regulation Proposal[24] will adapt the previous e-Privacy Directive (2002/58/EC) to new technologies and market realities and will complement and particularise the GDPR. The e-Privacy Regulation will thus be *lex specialis* to the GDPR. The new draft regulation covers the processing of "electronic communications data", including electronic communications content and metadata that are not necessarily personal data. The territorial scope is limited to the EU, including when data obtained in the EU are processed outside it, and extends to over-the-top communications service providers, which do not provide internet networks but deliver content, services or applications over the internet – such as WhatsApp, Skype or Viber.

The Council of the EU issued its first revisions to the e-Privacy Regulation on 8 September 2017.[25] The

Figure 7.2: Individuals never having used the internet in 2010 and 2017, by age group (%)



Source: *FRA, 2018 (based on Eurostat data extracted on 25 January 2018)*

European Parliament published a draft resolution, including its report on the e-Privacy Regulation, on 23 October 2017.[26] On 5 December 2017, the Council of the Bulgarian Presidency released a progress report,[27] which summarises the work done so far in the Council as a basis for its future work. After the publication of the proposal, European Data Protection Authorities raised some points of concern.[28]

The e-Privacy Regulation Proposal repeats and widens the derogations included in the e-Privacy Directive, which allow data retention and access to data that authorities retain; it therefore has an impact on the regulation of data retention and data encryption of electronic communications. The proposal does not include any specific provisions restricting retention of, and access to, data on the basis of a targeted retention scheme and after a prior review by a court, as the

CJEU required in *Tele2* for data retention and access to conform with the fundamental rights to privacy, protection of personal data and freedom of speech.[29]

Another topical amendment to the draft e-Privacy proposal that the European Parliament proposed relates to encryption's role in strengthening privacy. Encryption allows users to shield their internet communications and safeguard their personal data against unauthorised access or leaks. FRA already suggested reinforcing privacy through encryption in its *Fundamental Rights Report 2017*,[30] as did the European Data Protection Supervisor in its Opinion 6/2017.[31] In October 2017, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) voted in favour of an amendment[32] that precludes EU Member States from imposing any obligation that would result in weakening the security of networks and electronic communication services, such as the creation of "back doors".

In 2017, the European Commission also looked at the issue of encryption in criminal investigations. While stressing the importance of encryption in ensuring appropriate security for the processing of personal data, it noted that law enforcement and judicial authorities increasingly encounter challenges posed by the use of encryption by criminals. It discussed the technical and legal aspects, including potential impact on fundamental rights, with relevant stakeholders, drawing upon the expertise of Europol, Eurojust, the European Union Agency for Network and Information Security (ENISA) and FRA, as well as Member States' law enforcement agencies, industry and civil society organisations. In October, it announced a set of technical measures aiming to support Member State authorities, without prohibiting, limiting or weakening encryption. Exchange of expertise, provision of additional funding for training of law enforcement and judicial authorities, and supporting Europol in further developing its decryption capabilities were among the envisaged measures. Measures that could weaken encryption or could have an impact on a larger or indiscriminate number of people are excluded.[33]

7.2. Intensification of cyberattacks triggers diverse cybersecurity efforts

Interlinked with the challenges that the use of encryption raises, cybersecurity became a top priority in the EU in 2017, as cyberattacks of international nature and unprecedented scale hit Member States. Cyberattacks are a borderless[34] and rapidly evolving problem, which often results in disruption of services and can undermine citizens' trust in online activities.[35] They can have serious implications for the fundamental rights to privacy and data protection, since they usually target computer systems where large amounts of (sensitive) personal data are stored, such as passwords, medical files, company documents and financial information, and may reveal those data to unknown networks.[36] The 2017 WannaCry and NotPetya malware cyberattacks affected hundreds of thousands of users and organisations, and highlighted the need for a coordinated and effective response, as well as for more strengthened protection, at both EU and national levels.[37] These malware cyberattacks acted as wake-up calls and triggered the first ever case of cyber-cooperation at EU level.

> *"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. Last year alone there were more than 4,000 ransomware attacks per day and 80 % of European companies experienced at least one cyber-security incident."*
>
> *Jean-Claude Juncker, President of the European Commission, 'State of the Union address 2017', Speech/17/3165, 13 September 2017*

7.2.1. 'WannaCry' and 'NotPetya' prompt unprecedented cooperation

Both the WannaCry and NotPetya cyberattacks had an impact on critical European infrastructure operators in the sectors of health, energy, transport, finance and telecoms, as well as service providers and computer systems dedicated to specific tasks, such as robotics, medical scanners or production manufacturing plants.[38] The virus hit several EU companies quickly: **Spain**, **France**, **Germany** and **Belgium** were amongst the first Member States where the attack was reported.

In the **United Kingdom**, for example, the WannaCry cyberattack had potentially serious implications for the National Health Service, leading to widespread disruption in at least 81 of 236 hospital trusts in England.[39] WannaCry involved a type of malware that prevents access to inform ation systems by encrypting multiple common file types and then demands a ransom for the files to be unlocked (ransomware).[40] According to the UK National Audit Office, which conducted an independent investigation into the WannaCry cyberattack, between 12 and 18 May 2017, about 19,000 medical appointments were cancelled, computers at 600 general practitioner surgeries were locked and five hospitals had to divert ambulances elsewhere. The conclusions of the independent investigation highlighted the importance of developing, among other things, a coordinated plan for responding to such threats.[41]

Following the WannaCry cyberattack, and by virtue of Article 12 of Directive 2016/1148 on security of network and information systems (the NIS Directive),[42]

an EU Computer Security and Incident Response Team (CSIRT) was set up to assess, with ENISA's dedicated taskforce, the situation and provide effective operational cooperation. The CSIRT deployed the EU Standard Operating Procedures, which ENISA and Member States developed.[43] When the subsequent global outbreak of the NotPetya malware affected IT systems mostly in Europe, the EU CSIRTs Network also responded by exchanging synchronised information in a prompt and secure manner.[44] In addition, the 'Innovation Activity' of the European Institute of Innovation and Technology started developing a cloud-based Security Operations Centre focusing on the protection of critical infrastructures against so-called advanced persistent threats.[45]

7.2.2. EU and Member States strengthen their stance

Cybersecurity strategy: enhanced resilience, deterrence and defence

Even before these attacks, cybersecurity was already at the heart of the EU agenda, ranking high in the Digital Single Market Strategy. The fight against cybercrime was one of the three pillars of the European Agenda on Security. In May 2017, the European Commission published its mid-term review of the 2013 EU Cybersecurity Strategy. The evaluation took stock of the progress made so far and outlined further actions in the field of cybersecurity.[46] It reviewed the mandate of ENISA to define its role in the changed cyberspace context and developed measures on cybersecurity standards, certification and labelling, to make systems based on information and communication technology, including connected objects, more cybersecure.[47]

Specifically, the European Commission adopted a cybersecurity package on 13 September 2017, presenting new initiatives to further improve EU cyber-resilience and responses.[48] Regarding ENISA, the package outlines a reform proposal for a permanent mandate – which the agency currently lacks – to ensure it can provide support to Member States, EU institutions and businesses in key areas,[49] including implementing the NIS Directive. The cybersecurity package provides guidance on the practical implementation of the directive and further interpretation of its provisions. In addition, the Commission developed a blueprint recommendation so that the EU has in place a well-rehearsed plan in case of a large-scale cross-border cyber incident or crisis.[50]

On 20 November 2017, the General Affairs Council adopted conclusions on the *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*,[51] as the European Council had asked it to in October 2017. Specifically, the conclusions stress the need for both the EU and Member States to enhance cyberresilience, as well as the need for strong and closer cooperation among Member States and ENISA. Therefore, the conclusions welcome the proposal for ENISA to have a strong and permanent mandate.

A 2017 Eurobarometer survey on cybersecurity showed that ever more European residents use the internet for their daily activities.[52] At the same time, they are increasingly concerned about the security of internet transactions and cybercrime. This reiterates the findings of the 2015 and 2013 Eurobarometer surveys.

Eurobarometer survey signals increasing concerns about cybersecurity and cybercrime

In a 2017 special Eurobarometer survey on cybersecurity, a majority of respondents (87 %) regarded cybercrime as an important challenge to the internal security of the EU. Half of the respondents (49 %) said that law enforcement agencies in their respective countries were doing enough to combat cybercrime. Nearly half of respondents (46 %) said that they feel well informed about the risks of cybercrime, with significant differences among Member States (e.g. 76 % in Denmark and 27 % in Bulgaria).

The two most common concerns about using the internet for online banking and purchases were the misuse of personal data (45 %) and the security of online payments (42 %). Nearly a fifth (19 %) of respondents expressed no concerns about the security of online transactions. Victimisation rates are rising, the survey suggests. This is particularly true for "phishing" (38 % in 2017, 32 % in 2013); online fraud (16 % in 2017, 10 % in 2013); online banking fraud (11 % in 2017, 7 % in 2013); encountering racial hatred (18 % in 2017, 14 % in 2013); and hacking of social media profiles (14 % in 2017, 12 % in 2013). This trend towards increased reporting of incidents may reflect the public's raised awareness of such threats in the online world, which the media highlighted during 2017.

Most of the respondents would contact the police if they experienced cybercrime, especially if they were the victim of identity theft (85 %) or online banking fraud (76 %), or if they accidentally encountered child pornography online (76 %).

Source: European Commission (2017), Special Eurobarometer 464a on Cybersecurity, Brussels, September 2017.

NIS Directive implementation: aligning security principles with privacy and data protection safeguards

To effectively prevent and combat cybercrime, the NIS Directive aims to enhance the overall level of network and information system security by, among others, imposing a variety of obligations on national "operators of an essential service" to ensure that Members States

have implemented an effective strategy across all vital sectors. It sets up a cooperation group so that Member States can coordinate prompt responses and exchange information against potential threats.[53] EU Member States have until 9 May 2018 to transpose the directive into domestic law and until 9 November 2018 to identify operators of essential services.[54]

The **Czech Republic**,[55] **Germany**[56] and **Hungary**[57] have already implemented the directive into their national legal frameworks. However, the majority of EU Member States are currently in the process of adapting the provisions of the NIS Directive, either by setting up working groups[58] or by initiating public consultations[59] to assess if they need to amend existing national laws and adopt new legislation.

Article 8 of the directive obliges Member States to designate one or more national competent authority, as well as a national single point of contact on the security of network and information systems, which "shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities".[60] National implementation efforts thus need to pay due regard to aligning the security principles contained in the directive with fundamental rights safeguards, particularly the data protection principles enshrined in the GDPR – notably the principles of purpose limitation, data minimisation, data security, storage limitation, and accountability.[61]

For example, various public institutions will be involved in the **Polish** national cybersecurity system. The draft law proposal enables them to process sensitive data within the meaning of Article 9 (1) of the GDPR.[62] However, the opinion that the Polish data protection authority issued on the draft proposal considered the right to process such data excessive and unjustified in the context of the tasks of these institutions.[63] The opinion voices additional concerns about the exemption of data controllers from a series of GDPR duties pertaining to subjects' rights of access, rectification and erasure, notification, and data portability,[64] without any prior impact assessments.[65] It also underlines that the draft proposal should refer more precisely to the safeguarding of personal data, instead of allowing data retention for the "period necessary for the completion of the tasks", which is too general and vague.

In **Germany**, the Act for the implementation of the NIS Directive came into force on 29 June 2017.[66] The IT Security Act had already anticipated many of the provisions of the directive in 2015. The Act makes no explicit reference to the GDPR, but, in principle, the Federal Office for Information Security (BSI) is obliged to delete as soon as possible any data that are processed for IT security purposes. In addition, any use of data by the BSI for other purposes is strictly forbidden, except for national security, counterterrorism and the investigation of serious crimes and cybercrimes. In these cases, it may transfer personal data to public prosecutors, the police and the three federal intelligence agencies.[67]

7.3. Big data: EU and international bodies urge respect for fundamental rights amidst push for innovation

The security of digital data in case of cyberattacks is not the only area where the need to establish data protection safeguards is increasingly important. Nowadays, personal data are collected in areas such as transport, communications, financial services, healthcare and energy consumption. These data can be subject to automatic processing by computer algorithms and advanced data-processing techniques, and may be used to generate correlations, trends or patterns. These techniques provide unprecedented insight into human behaviour and both public and private sectors are willing to use such datasets to bolster competitiveness, innovation, scientific research and policymaking. The development of the Internet of Things (IoT) and of 'big data'[68] analytics, allowing unprecedented availability, sharing and automated use of data, brings opportunities in terms of innovation and economic growth. However, it also poses a number of challenges for individuals' fundamental rights,[69] such as the protection of privacy and personal data, and the rights to equality and non-discrimination. Indeed, intelligence services of Member States have increasingly been relying on processing and analysing such datasets, as FRA highlighted in its report on surveillance activities and fundamental rights.[70]

FRA ACTIVITY

In-depth research on the impact of surveillance on fundamental rights

Terrorism, cyberattacks and sophisticated cross-border criminal networks pose growing threats. The work of intelligence services has become more urgent, complex and international. But intelligence work to counter these threats, particularly large-scale surveillance, can also interfere with fundamental rights, especially privacy and data protection. Following a specific request by the European Parliament, FRA published, in October 2017, its second report on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis on the topic, and supplements that analysis with field-based insights gained from extensive interviews with diverse experts in intelligence and related fields, including overseeing intelligence.

Digital surveillance methods serve as important resources in intelligence efforts, ranging from intercepting communications and metadata to hacking and database mining. Most EU Member States have enacted intelligence laws and have given independent expert bodies the task of overseeing the work of their intelligence services, FRA's 2017 report shows. It also reveals that opinions of these bodies' efficiency are mixed. Similarly, although law provides for diverse remedies, critics contend that actually accessing them is less straightforward. Failing to confront these flaws raises fundamental rights concerns, and carries the risk of undermining the public's trust in their governments' pledges to uphold the rule of law even when confronted with challenges that may make short-cuts look tempting.

For more information, see FRA (2017), Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update, Publications Office, October 2017.

In 2017, authorities at national, EU, and international levels took stock of these realities, and their potential impact on citizens and fundamental rights.

7.3.1. EU and international guidelines: catching up with big data challenges

The latest contributions of EU and international bodies or agencies on the use of big data analytics offer important clarifications to policymakers and legislators. The common idea reflected in the work of the EU, the Council of Europe and the United Nations is that technological innovation must go hand-in-hand with human rights compliance. Strong and effective supervisory mechanisms and a consistent legal framework at an international level can address security risks and issues of privacy, data protection and discrimination that emerge from big data analytics.

The European Parliament adopted a resolution on fundamental rights implications of big data in March 2017.[71] The resolution stresses that fundamental rights should be at the centre of attention when big data analytics are used for commercial, scientific and law enforcement purposes. Big data analytics could result in infringements of individuals' fundamental rights, and in differential treatment of or discrimination against some groups of people. Therefore, EU institutions and bodies, such as the European Commission and the European Data Protection Board, as well as the national data protection authorities, have the job of promoting and ensuring concrete safeguards for fundamental rights.

Similarly, the Council of Europe adopted *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* in 2017,[72] drawing attention to the fact that data subjects' control over their personal data is at risk. Indeed, while they may choose what data they provide for processing, it is almost impossible to control data that have been observed or inferred about them, such as data derived from closed-circuit television cameras, or created through big data analytics.

This capacity to create profiles and make automated decisions has not gone unnoticed. The WP29 in its *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*[73] underlines its opacity and its potential to significantly affect individuals' rights and freedoms. In addition, ENISA, in its latest report on *Baseline Security Recommendations for IoT*,[74] insists on the right of individuals not to be subject to a decision based solely on automated processing, as enshrined in the GDPR.[75]

Furthermore, attention has been brought to big data analytics related to artificial intelligence appliances and robotics. The Council of the EU in its conclusions on the Tallinn Digital Summit on September 2017[76] invites the European Commission to put forward a European approach on emerging trends, such as artificial intelligence and blockchain technology, while ensuring a high level of fundamental rights protection and ethical standards. In addition, the European Parliament stresses in its *Resolution with recommendations on Civil Law Rules on Robotics*[77] that robotics research should respect fundamental rights. In addition, it calls for the designation of a European Agency for Robotics and Artificial Intelligence, which would provide the technical, ethical and regulatory expertise needed. Furthermore, the Parliamentary Assembly of the Council of Europe (PACE), in its Recommendation 2102,[78] recognises that it is

increasingly difficult for law to adapt to the speed at which technology evolves. It concludes that the only way forward is close cooperation of the Council of Europe, the EU and the United Nations on this matter.

However, big data analytics can be also used as a tool to support fundamental rights compliance. The Office of the United Nations High Commissioner for Human Rights (OHCHR), in its latest Report of the Special Rapporteur on the Right to Privacy,[79] underlines that big data has the potential to help states respect, protect and fulfil their human rights obligations. More precisely, it offers the means to develop new insights into intractable public policy issues such as climate change, the threat of terrorism and public health.

7.3.2. National initiatives assessing big data challenges slowly emerge

In some Member States, data protection authorities offered clarifications in 2017 on what the concept of big data analytics encompasses, what laws apply in this area and what risks to the individual's rights and freedoms arise.

At national level, Article 22 of the GDPR and its provisions on automated decision making are a matter of discussion and debate. In **Belgium**, for example, the Privacy Commission[80] stresses the need to define practically the meaning of the right of access and rectification in the context of big data analytics, and to clarify the relation between these rights and the operational part of algorithms. In **Germany**, the Federal Commissioner for Data Protection and Freedom of Information has noted that Article 22 is not sufficient, as it lacks effective limitations.[81] Automated decision making, including profiling, in the era of big data analytics can lead to social exclusion and discrimination, and algorithmic bias is a major societal issue that constitutes a risk to fundamental rights and freedoms.

In **Hungary**, the national data protection authority challenged[82] the fundamental rights compliance of a draft Act. The latter would have established a central system for storing image and voice recordings from police, public transportation companies, road management companies, road tax collectors, public safety offices and financial service providers. Such a central system could systemise these recordings by using a computer algorithm to find correlations and connections between these data and analyse patterns. The data protection authority's intervention prompted the Hungarian Parliament to adopt the draft Act without all of the provisions relating to the establishment of the central image and voice recording storing system.[83] This clearly demonstrates the power of data protection authorities to challenge and influence the regulatory powers and the decision-making process.

Promising practice

Raising awareness on legal and ethical concerns arising from use of algorithms

In **France**, the national data protection authority has developed a system intended to help people understand how algorithms structure and influence our digital interactions. The aim is to raise awareness about the functioning of algorithms so that individuals will be able to retain their free will and not allow algorithmic calculations to constrain them. In addition, with its latest survey, the French data protection authority aims to raise public awareness of the role of algorithms and artificial intelligence in everyday life. This work does not touch upon legal matters exclusively, but also assesses the ethical concerns that arise from these new technologies.

For more information, see Commission nationale de l'informatique et des libertés (CNIL), 'The Oracle of the Net' (L'oracle du net), September 2017; and CNIL, 'Report on the ethical matters raised by algorithms and artificial intelligence', December 2017.

FRA opinions

Article 8 (3) of the EU Charter of Fundamental Rights and Article 16 (2) of the TFEU recognise the protection of personal data as a fundamental right. They affirm that compliance with data protection rules must be subject to control by an independent authority. The oversight and enforcement of data protection rights can become reality if such authorities have the necessary human, technical and financial resources, including adequate premises and infrastructure, to ensure effective performance of their tasks and exercise of their powers. Such a requirement is grounded in Article 52 (2) of the General Data Protection Regulation (GDPR).

FRA opinion 7.1

EU Member States should thoroughly assess the human and financial resources, including technical skills, necessary for the operations of data protection authorities in view of their new responsibilities deriving from the enhanced powers and competences set out under the General Data Protection Regulation.

The GDPR requires that data protection authorities ensure awareness and understanding of the rights and risks related to the processing of personal data. However, most of the guidelines and awareness-raising campaigns are mainly accessible online, so access to the internet is crucial for awareness of rights. In a majority of Member States, there is still an important digital divide between generations in terms of the use of the internet.

FRA opinion 7.2

Data protection authorities should ensure that all data controllers give specific attention to children and older EU citizens to guarantee equal awareness of data protection and privacy rights, and to reduce the vulnerability caused by digital illiteracy.

Taking into account the analysis of the CJEU, the scope of data retention carried out pursuant to the Passenger Name Record (PNR) agreement and PNR Directive should be limited to what is strictly necessary. This means excluding the retention of data of passengers who have already departed and who do not present, in principle, a risk of terrorism or serious transnational crime – at least where neither the checks and verifications nor any other circumstances have revealed objective evidence of such a risk.

FRA opinion 7.3

When reviewing the PNR Directive pursuant to Article 19, the EU legislator should pay particular attention to the analysis of the Court of Justice of the European Union (CJEU). Notably, it should consider reviewing the provisions of the PNR Directive to limit the scope of data retention, after air passengers' departure, to those passengers who may objectively present a risk in terms of terrorism and/or serious transnational crime.

Data protection authorities have the task of monitoring and enforcing the application of the GDPR, and promoting the understanding of risks, rules, safeguards and rights in relation to personal data processing. This role becomes even more important in the context of 'big data' analytics, which allows for unprecedented availability, sharing and automated use of personal data. As the European Parliament and the Council of Europe have highlighted, such processing – operated by natural persons, private companies and public authorities – could pose a number of challenges to individuals' fundamental rights, notably their rights to privacy, protection of personal data and non-discrimination. Further research is still necessary to identify such challenges clearly and address them promptly.

FRA opinion 7.4

EU Member States should evaluate the impact of 'big data' analytics and consider how to address related risks to fundamental rights through strong, independent and effective supervisory mechanisms. Given their expertise, data protection authorities should be actively involved in these processes.

The Directive on security of network and information systems (NIS Directive) enhances the overall level of network and information system security by, among other strategies, imposing a variety of obligations on national "operators of an essential service", such as electricity, transport, water, energy, health and digital infrastructure, to ensure that an effective strategy

is implemented across all these vital sectors. In particular, Article 8 of the directive obliges Member States to designate one or more national competent authorities, as well as a national single point of contact on the security of network and information systems, which "shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities". Implementation initiatives in several Member States have highlighted the need to ensure that the data protection principles enshrined in the GDPR are properly taken on board and reflected in national legislation transposing the NIS Directive.

FRA opinion 7.5

EU Member States should ensure that the national provisions transposing the NIS Directive into national law adhere to the protection principles enshrined in the General Data Protection Regulation (GDPR). In particular, national provisions need to adhere to the principles of purpose limitation, data minimisation, data security, storage limitation and accountability, especially as regards the NIS Directive's obligation for national authorities to cooperate with national law enforcement and data protection authorities.

Index of Member State references

Endnotes

1 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.

2 Directive (EU) 2016/680 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 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.

3 Official Journal of the European Union, L 119, 4 May 2016.

4 The opening clauses of the General Data Protection Regulation are in Art. 4 (7), 6 (2), 8, 9 (2) (a) (g), 9 (4), 10, 14 (5) (c) (d), 17 (1) (e) (3) (b), 20 (2) (b), 22 (2) (b), 23, 26 (1), 26 (3) (a) (g), 28 (3) (a) (g) (4), 32 (4), 35 (10) 36 (5), 37 (4), 39 (1) (a) (b), 49 (1) (4) (5), 58 (1) (6) 83 (7), 84, 85, 87, 88, 89 (1), 89 (2), and 90.

5 Austria, *120. Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird, Datenschutz-Anpassungsgesetz 2018*.

6 Germany, Gesetzgebung *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680*.

7 FRA (2017), *Fundamental Rights Report 2017*, Opinion 6.1, p. 142.

8 GPDR, Art. 52 (4).

9 Police Directive Art. 42 (4).

10 The Netherlands, Andersson Elffers Felix, '*Organisatorische vertaling Verordening & Richtlijn gegevensbescherming*', *Eindrraportage*, 2017.

11 Article 29 Working Party, *Guidelines on Data Protection Impact Assessment* (DPIA), wp248, 4 April 2017; Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*, wp243, 13 December 2016; Article 29 Working Party, *Guidelines on Personal Data breach notification*, wp250, 3 October 2017.

12 GDPR, Art. 57 (1) (b).

13 GDPR, Recital (38).

14 See the recent mapping offered by Better Internet for Kids on their webpage.

15 FRA (2017), *Mapping minimum age requirements concerning the rights of the child in the EU*.

16 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.

17 Belgium, Law of 25 December 2016 pertaining to the processing of passengers' data.

18 Germany, Act for the Implementation of Directive (EU) 2016/681 (*Gesetz zur Umsetzung der Richtlinie* (EU) 2016/681), 6 June 2017.

19 Hungary, Act XXXIII of 2017 on the amendment of certain laws related to internal affairs (*2017. évi XXXIII. törvény egyes belügyi tárgyú törvények módosításáról*), 5 May 2017.

20 European Commission, COM(2017) 779 final, *Twelfth progress report towards an effective and genuine Security Union,* 12 December 2017, p. 6.

21 CJEU (2017), Opinion 1/15 on the envisaged agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 26 July 2017.

22 FRA (2011), *Opinion of the European Union Agency for Fundamental Rights 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 (COM(2011) 32 final)*, Vienna, 14 June 2011; FRA (2017), *Fundamental Rights Report 2017*, pp. 159-160, 167.

23 CJEU (2017), Opinion 1/15, para. 232.

24 COM/2017/010 final; Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

25 European Council, 11995/17, Brussels, 8 September 2017.

26 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report, A8-0324/2017, 20 October 2017.

27 European Council, 15333/17, Brussels, 5 December 2017.

28 WP29 Opinion 1/2017, adopted on 4 April 2017 and European Data Protection Supervisor, Opinion 6/2017 adopted on 24 April 2017, followed by recommendations on some aspects of the e-Privacy Regulation on 5 October 2017.

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

30 FRA (2017) *Fundamental Rights Report 2017*, p. 142, Opinion 6.2.

31 EDPS (2017), Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (e-Privacy Regulation), Opinion 6/2017, 24 April 2017.

32 Recital 37 and Art.17 of the Proposal, A8-0324/2017, 23 October 2017.

33 European Commission, Eleventh progress report towards an effective and genuine Security Union, COM(2017) 608 final, 18 October 2017, pp. 8-10.

34 For detailed information on data protection implications in cross-borders situations, please see Chapter 6 of this report on Asylum, visas, migration, borders and integration.

35 European Commission (2017), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy*, Commission staff working document, SWD(2017) 155 final, Brussels, 10 May 2017, p. 36.

36 Tasheva, Iva (2017), *European cybersecurity policy – Trends and prospects*, European Policy Centre (EPC), 8 June 2017.

37 Symnatec, *WannaCry Ransomware: Information from Symantec*, 24 May 2017.

38 ENISA, *WannaCry Ransomware: First ever case of cyber cooperation at EU level*, 15 May 2017.

39 UK, National Audit Office, Department of Health, *Investigation: WannaCry cyber-attack and the NHS*, Report by the Comptroller and Auditor General, 27 October 2017.

40 ENISA, *WannaCry Ransomware: First ever case of cyber cooperation at EU level*, 15 May 2017.

41 UK, National Audit Office (2017), p. 25ff.

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

43 ENISA, *WannaCry Ransomware: First ever case of cyber cooperation at EU level*, 15 May 2017.

44 ENISA, *EU operational cooperation under test for the second time*, 3 July 2017.

45 EIT, *EIT Digital creates Security Operations Centre for detecting and responding cyber-attacks*, 31 May 2017.

46 European Commission (2017), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy*, COM(2017) 228 final, Brussels, 10 May 2017.

47 *Ibid*, pp. 12-13.

48 European Commission (2017), *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, Joint Communication to the European Parliament and the Council, JOIN(2017) 450 final, Brussels, 13 September 2017.

49 European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and*

Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final, Brussels 13 September 2017.

50 European Commission (2017), *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, Joint Communication to the European Parliament and the Council, JOIN(2017) 450 final, Brussels, 13 September 2017.

51 Council of the European Union (2017), *Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, 14435/17, Brussels, 20 November 2017.

52 European Commission (2017), *Special Eurobarometer 464a: Europeans' attitudes towards cyber security*, Brussels, 13 September 2017.

53 NIS Directive (2016), Preamble.

54 *Ibid*, Art. 25 and Art. 5.

55 Czech Republic, Act No. 205/2017, amending the Act on Cyber Security (*zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti*), No. 181/2014, 1 August 2017.

56 Germany, Act on the Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (*Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*), 23 June 2017.

57 Hungary, Act CXXXIV of 2017 on the amendment of laws related to internal matters and other connected topics (*2017. évi CXXXIV. törvény a belügyi feladatokat érintő és más kapcsolódó törvények módosításáról),* 10 November 2017.

58 See, for example, Bulgaria, State e-Government Agency (*Държавна агенция „Електронно управление"*) (2017), Letter No. ДАЕУ-4427/25.09.2017 to the Center for the Study of Democracy (*Писмо № ДАЕУ-4427/25.09.2017 до Центъра за изследване на демокрацията*), 25 September 2017; Croatia, National Security Council Office (*Ured Vijeća za nacionalnu sigurnost*) (2017), *Decision on the establishment of a Council Working Group for the NIS Directive Implementation*, 25 May 2017.

59 See, for example, Slovenia, Proposal of the Act on Information Security (*Predlog Zakona o informacijski varnosti*, ZIV), 8 September 2017; Spain, Ministry of Energy, Tourism and Digital Agenda (*Ministerio de Energía, Turismo y Agenda Digital*), *Public consultation on the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* (*Consulta pública sobre sobre la transposición de la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*), December 2016.

60 NIS Directive (2016), Art. 8.

61 Regulation 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, *OJ L 119*, (General Data Protection Regulation) Art. 5. See, for example, Cyprus, *Draft law on digital security (Setting up of Authority, competences, establishment and functioning of the Authority) of 2018* [*Ο περί της Αρχής Ψηφιακής Ασφάλειας (Σύσταση Αρχής, Αρμοδιότητες, Ίδρυση και Λειτουργία Αρχής) Νόμος του 2018*], Art. 17 (1).

62 Poland, Draft law proposal on Law on national cyber security system (*Opinia dotycząca projektu ustawy o Krajowym Systemie Cyberbezpieczeństwa*).

63 Poland, Inspector General for the Protection of Personal Data (*Generalny Inspektor Ochrony Danych Osobowych*), *Opinion to the draft law proposal on Law on national cyber security system* (*Opinia dotycząca projektu ustawy o Krajowym Systemie Cyberbezpieczeństwa)*, 14 November 2017.

64 Regulation 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, *OJ L 119*, (General Data Protection Regulation) Art. 12-22.

65 Ibid, Art. 35 and Art. 23, para. 2.

66 Germany, Act on the Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (*Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*), 23 June 2017.

67 Germany, Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*), Section 5 and 5a.

68 'Big data' generally refers to considerable technological developments in the past decades related to the production and use of information and data. Big data is characterised by an increased volume, velocity and variety of data being produced ("the three Vs"), mainly on the internet.

69 European Parliamentary Research Service, *Reform of the e-Privacy Directive*, September 2017.

70 European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update*, p. 80, October 2017.

71 European Parliament, *Resolution on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*, February 2017.

72 Council of Europe (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, January 2017.

73 Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, October 2017.

74 ENISA, *Baseline Security Recommendations for IoT*, November 2017.

75 GDRP, Art. 22.

76 European Council (2017), *European Council Meeting (19 October 2017) – Conclusions*, October 2017.

77 European Parliament (2017), *Resolution with recommendations to the Commission on Civil Law Rules on Robotics*, February 2017.

78 The Parliamentary Assembly of the Council of Europe (PACE), *Recommendation 2102 - Technological convergence, artificial intelligence and human rights*, April 2017.

79 United Nations Human Rights Office of the High Commissioner (UNHRC), *Report of the Special Rapporteur on the right to privacy*, October 2017.

80 Belgium, Privacy Commission (*Commission de la protection de la vie privée/Commissie voor de bescherming van de persoonelijke levensfeer*), Big Data Rapport, February 2017.

81 Germany, Federal Commissioner for Data Protection and Freedom of Information (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*), *26. Tätigkeitsbericht für die Jahre 2015 und 2016*, May 2017.

82 Hungary, Hungarian Authority for Data Protection and Information Freedom, *Letter on the Draft Proposal on the amendment of certain laws related to interior matters and other areas in connection with interior affairs*, August 2017.

83 Hungary, Hungarian Parliament, Act CXXXIV of 2017 the amendment of certain laws related to interior matters and other areas in connection with interior affairs (*2017. évi CXXXIV. törvény a belügyi feladatokat érintő és más kapcsolódó törvények módosításáról*), December 2017.