Formal comments of the EDPS on:

- **the Joint communication by the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament and the Council "Resilience, Deterrence and Defense: Building strong cybersecurity for the EU"** (hereinafter 'the Joint Communication')[i]**;**

- **the Commission 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")[ii];**

- **the Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises** (hereinafter 'the Recommendation')[iii]**;**

- **Communication from the Commission to the European Parliament and the Council "Making the most of NIS - towards effective implementation of the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (**hereinafter 'the NIS Communication'**)[iv].**

The Commission adopted these measures on 13 September 2017 in a common measure, referred to as the 2017 "Cybersecurity Package"[v].

The package also includes a **Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment**[vi], which the EDPS may consider in a different context.

On 18 October, the Commission adopted a package of measures on the Security Union, which elaborates on some of the initiatives announced in the Cybersecurity package. Where relevant, the EDPS takes account of these additional elements in the current formal comments. This concerns in particular the announced policy initiatives relating to encryption.

I. Introduction and background

On 13 September 2017 the European Commission and the High Representative proposed a set of measures for the EU "*... to build a stronger resilience to cyber-attacks and create an effective EU cyber deterrence and criminal law response to better protect Europe's citizens, businesses and public institutions*", called 'Cybersecurity Package'. These measures include the instruments mentioned above.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

On 18 October 2017, the Commission published its report on a Security Union[vii], which further elaborated on some elements of the Joint Communication. In particular, it presented a number of initiatives concerning encryption.

The EDPS has been following the developments on the EU strategy to build cybersecurity capacity since its inception. Among other formal and informal advice, we would like to recall the following deliverables issued by the EDPS:

- Opinion on the proposal for a Regulation on ENISA in December 2010[viii].
- Formal comments on the Commission's public consultation on improving network and information security (NIS) in the EU[ix] in October 2012.
- Opinion on the Joint Communication by the Commission and the High Representative on a Cyber Security Strategy of the EU and on the Proposal for an NIS Directive[x] in June 2013.
- Opinion on Dissemination and use of intrusive surveillance technologies[xi] in December 2015.
- Guidance on Security Measures for Personal Data Processing[xii] in March 2016.

The EDPS observes that the current package has many elements, which are relevant in the context of data protection and privacy. We note that the Commission did not respect its commitment to consult the EDPS ahead of the adoption of such proposals.

II. Scope of EDPS' comments

Applicable data protection law, including the General Data Protection Regulation[xiii], considers information security as an enabler to the protection of individuals through the protection of their personal data. Information security is among the data protection 'principles' laid down by the law (Article 5(1)(f). Article 32 imposes an obligations on all actors ('controllers'[xiv] and 'processors[xv]) processing personal data to *"... implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk ...*". Articles 33 and 34 set the obligation, under certain conditions, to notify personal data breaches[xvi] implying risks for individuals to the competent supervisory authority within 72 hours and to notify to the individuals affected those breaches likely to represent a high risk for them without undue delay.

Analogue provisions are set out in the current Regulation 45/2001 on the processing of personal data by EU institutions and bodies[xvii] as well as in the Proposal for a new personal data protection Regulation for these EU entities.

With particular focus on the privacy of electronic communications, Article 4 of Directive 2002/58/EC contains provisions on cybersecurity. Some of these obligations are maintained in Article 17 of the proposal for an ePrivacy Regulation[xviii] which establishes the obligation to inform end-users in case of a particular risk that may compromise the security of networks and electronic communications services.

While these instruments underline the importance of cybersecurity measures for effective data protection, the implementation of security measures may entail the processing of personal data. Such processing must be compliant with the law and all data protection principles, including purpose limitation and data minimisation, apply.

The present formal comments analyse the instruments mentioned above in the light of the applicable legal framework and the above considerations.

III. EDPS' comments

1. General considerations on the Cybersecurity Package, including the Joint Communication

- *Implementing effective cybersecurity in the EU cannot be postponed.*

Our society relies more and more on the exchange of information via communication networks, most of the times linked to the global Internet, to streamline the delivery and use of essential services such as energy and goods production and distribution, and transport. The processing of information and data, including personal data is considered the foundation of the Digital Economy. One outstanding example of the role that Internet and online services are envisaged to play is the recent Tallinn Declaration on eGovernment, aiming at ensuring high quality, user-centric digital public services for EU citizens and businesses. It considers trustworthiness and security related action as key for success to ensure that *"...information security and privacy needs are taken into consideration when designing public services and public administration information and communication technology (ICT) solutions, following a risk-based approach and using state-of-the-art solutions...*".

In many contexts, access to the Internet has become essential for full participation in economic and societal activities.

Cybersecurity is no longer exclusively a concern for experts, but a large majority of EU citizens recognizes its importance, as demonstrated by a recent Eurobarometer survey[xix]: 87% of respondents consider cybercrime an important challenge to the internal security of the EU and the misuse of personal data continues to be the most significant concern of internet users.

We thus welcome and deem as essential and not any longer deferrable the effort to improve "*... the security of the Internet and private networks and information systems underpinning the functioning of our society and economy ...*" which is the rationale of the Package.

We observe that the Joint Communication emphasizes a number of measures, which aim at improving the reaction after cyber security incidents have occurred. We recognize that a well-prepared reaction, which is based on good planning, training of staff and establishment of appropriate processes and procedures in advance can considerably reduce the damage caused by an incident and help to avoid further spread of damage.

We recall, however, that adequate measures for prevention of incidents e.g. by appropriate maintenance of IT systems, can be even more effective as they stop attacks before any damage occurs. In this context, it is notable to observe that the Wannacry attacks in May 2017 did not affect systems which had either disabled the vulnerable functionality (which was not used in many systems) or had installed an update which had been available about a month before the attacks and removed the vulnerability used by the attacker[xx]. We therefore underline the importance of establishing state of the art information security risk management systems, developing and applying appropriate policies for all systems and allocate responsibilities in all organisations. These measures correspond to the security approach provided by the relevant data protection legislation and other instruments on information security.

Wannacry and other recent cybersecurity incidents demonstrate that the objectives of the 2013 cybersecurity strategy, to improve resilience and preparedness in the public and the private sector, are still valid and continue to require considerable efforts. Investing in education and appropriate preventative measures should lay the basis on which effective and rapid reaction to unfolding incidents can limit the damage caused. The cybersecurity strategy should follow both threads, and may benefit from a thorough analysis of past incidents in order to identify those factors, which led to the lack of appropriate preparation and prevention measures in the most affected organisations. Measures improving cybersecurity skills as well as cyber hygiene and awareness find our full support.

The elimination or reduction of inherent weaknesses of products and services can be particularly effective to prevent cybersecurity incidents. The Joint Communication refers to several approaches, which can contribute to addressing inherent weaknesses of the current market for products and services:

- The use of the "security by design" approach,
- Establishing the principle of "duty of care",
- Allocating liability for security failures to market actors.

We encourage the Commission to develop and implement policies and propose legal measures to promote these objectives. This would mirror and complement similar approaches already integrated in Union law for the protection of personal data, such as the obligation to observe the principle of data protection by design and by default and the corresponding sanctions and liabilities.

Independent security researchers can play an important role in the detection, assessment and mitigation of cybersecurity vulnerabilities. This research should not face restrictions due to inappropriately designed legislation, which creates risks of prosecution for legitimate activities. We welcome the recognition of this necessity in the Joint Communication.

- *On the planned cybersecurity competence network with a European Cybersecurity Research and Competence Centre*

We take note of the plan to create "*a network of cybersecurity competence centres with a European Cybersecurity Research and Competence Centre at its heart*", to "*stimulate development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level*". We also take note that the Commission will launch an impact assessment in 2018.

We will assess this proposal at a later stage when relevant policy instruments, including legal ones, are developed and we keep at disposal of the Commission for any possible co-operation in our advisory role.

We take the opportunity to welcome the emphasis on the need to develop and assess encryption capabilities in products and services as essential features to protect information and people's fundamental rights by protecting their personal data.

- *On creating effective cybersecurity deterrence*

While we share the understanding that there is a need for an effective law enforcement response focusing on detection, traceability and prosecution of cyber criminals, we stress the need to carry it out in full respect of the EU Charter of Fundamental Rights, including the rights to privacy and data protection. We take the opportunity to recall our advice contained in

the EDPS "Necessity Toolkit" to assess the impact of new provisions and measures on individuals' fundamental rights when processing their persponal data, identify the cases in which the limitation of this right is truly necessary and set adequate safeguards to counterbalance the intrusiveness of the planned measures.

The Joint Communication announces measures on electronic evidence. We shall issue a separate Opinion on the legislative instrument on cross-borders access to e-evidence that the Commission intends to adopt in January 2018.

The "11th progress report towards an effective and genuine Security Union" addresses the issue of law enforcement and judicial authorities encountering encryption used by alleged criminals in criminal investigations. We note that the Commission plans to propose "*legal measures to facilitate access to encrypted evidence*" and "*technical measures to enhance decryption capabilities*". These plans include strengthening Europol decryption capabilities and specific attention to EU-funded research and development in relevant technologies. We note, too, that the Commission further proposes a "*network of points of expertise*" on the subject matter to share national capabilities and expertise. This network should, in the Commission proposal, develop and exchange "*a toolbox of alternative investigation techniques*", whose repository should be kept at the European Cybercrime Centre at Europol. Among other measures, the Commission acknowledges the "*need for continuous assessment of technical and legal aspects of the role of encryption in criminal investigations given the constant development of encryption techniques, their increased use by criminals and the effect on criminal investigations*". The Commission will support "*the development of an observatory function in collaboration with the European Cybercrime Centre (EC3) at Europol, the European Judicial Cybercrime Centre (EJCN) and Eurojust*".

We welcome the fact that the Commissions plans to propose a range of measures to support Member State authorities in tackling encryption in criminal investigations, "*without prohibiting, limiting or weakening encryption*". **We welcome and support the Commission statement not to consider "*measures that could weaken encryption or could have an impact on a larger or indiscriminate number of people*"**. We consider that the measures considered by the Commission may be implemented in full respect of fundamental rights, observing the principles of necessity and proportionality.

We take the opportunity to set out once again our view that weakening encryption to combat cybercrime is not a viable option, and that alternative measures should be explored[xxi]. We note that this view is shared as a rationale in the Commission proposals and largely supported by experts[xxii]. We welcome further research and we are ready to exercise our advisory role and to assess relevant proposals. **In particular, we consider that the planned "observatory" can play an important role to protect individuals' fundamental rights and we expect to be consulted in its preparation**. Furthermore, in our role as supervisor of Europol for the processing of personal data, we will ensure that the measures, once applied in practice, respect individuals' fundamental rights.

The Joint Communication proposes that the future European Cybersecurity Research and Competence Centre and its network, further to supporting the security of "*products and services used by citizens, businesses and governments within the Digital Single Market*", could support the EU cyber defence dimension. We recommend considering that the deliverables of the Centre, intended for the defence of EU citizens, could be used against them if they fall in the wrong hands or are misused.

In our Opinion on intrusive surveillance technologies [xxiii] we already drew attention to EU policies regarding potentially harmful products and services, notably in the cybersecurity domain, and we stated that cyber-surveillance technology should be adequately covered by considerations as those applied to dual use goods. We warned against the risks associated with developing, using and marketing hacking tools, which are highly intrusive in people's lives and represent a high risk for individuals' fundamental rights and freedoms. We said that "*the use of surveillance tools should be addressed by specific legislation framing the acceptable limits of the dissemination and use of such technologies and laying down the necessary safeguards for such use*". We also added that "*In the context of dual-use, standards should be developed in order to assess how the ICT or the information at stake might be used and the potential impact on fundamental rights in the EU*". We take note that the European Parliament is considering a report on the Commission recast proposal on the exports control of dual-use items[xxiv] which would include certain categories of cyber-surveillance tools in the scheme[xxv].

In addition to the external dimension, advanced tools for exploitation of security weaknesses or vulnerabilities may also create risks for those producing them. Recent reports[xxvi] of hacking tools prepared by a state security agency being leaked and used to support malicious cyber-attacks that hit tens of thousands of computers and critical infrastructures, affecting the operations of hospitals and blocking e-government facilities, demonstrate the risks very clearly.

The Joint Communication does not clarify how the risks linked to the planned EU support to Member States "*in the development of dual-use cybersecurity capabilities*" will be managed. We strongly recommend a thorough assessment of the risks of such a strategy, and we invite the Commission to perform a thorough impact assessment before launching any measures.

- *On the application of security and notification obligations and the relationship with security and data breach notifications in the GDPR.*

Organisations which are subject to the security and information related obligations of the NIS Directive have to ensure compliance with the provisions on security of personal data and the notification of personal data breaches at the same time. While the two instruments have different objectives, and their implementation will require consideration of different risks, organisations which are subject to both instruments will have to implement measures that are appropriate to address all requirements. Companies and public authorities processing personal data should take an integrated approach in considering security and personal data protection requirements in the prevention and treatment of network and information incidents. We recommend that the Commission and the Member States take the need for this operational synergy into account when designing measures for the effective implementation of the cybersecurity provisions such as notifications mechanisms and cooperation between data protection supervisory authorities and member states competent authorities as identified in the NIS directive.

More in detail, we consider that **the relationship between the NIS Directive and the GDPR regarding information security and notifications of personal data breaches should be further clarified**[xxvii]. Under Article 1(7) of the NIS Directive, the provision on security and/or notification requirements for digital services providers ("DSP") or operators of essential services ("OES") under the Directive are not applicable if an EU-sector specific legislation provides for security and/or notification requirement, provided that such requirements are at least equivalent in effect to the obligations laid down in the NIS Directive. This principle is recalled in the Communication of the Commission, stating that a "*lex*

specialis" would prevail on the security and notification requirements conditions of the NIS Directive[xxviii].

However, the obligations from the GDPR are not affected by the NIS Directive or any sector-specific legislation. The NIS Communication recognizes that the notification obligations of the NIS Directive are "*without prejudice to the notification of a personal data breach to the supervisory authority covered by Article 33 of the GDPR*".

We believe that this language is equivocal and would like to clarify how we assess the relationship between the two legal instruments on these obligations.

In our view, the GDPR cannot be considered as a sector specific legislation in the sense of Article 1 (7) of the NIS Directive. The GDPR is, as its title makes it clear, of general application and applies to any entity processing personal data, without the limitations of scope of the NIS Directive and of certain of its specific provisions[xxix].

As a result, all obligations of the GDPR, including those on security of personal data and personal data breaches, apply in addition to all possible obligations under the NIS Directive.
Furthermore, the parallel application of the GDPR and NIS Directive may lead to practical difficulties for organisations subject to both legal acts:

- Article 32 of the GDPR refers to the conditions under which controllers and processors are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks for the individuals whose data are processed. The NIS Directive[xxx] takes a risk based approach to prevent and minimise the impact of incidents affecting the security of the network and information systems on the services provided. While the outcome of the two different assessments might to some extent overlap, the two types of assets to protect are different (fundamental rights of individuals for the GDPR, service continuity for the NIS Directive) and the organisation needs to take into account this difference when carrying out their security risk assessment.

- The incident notification obligations under the NIS Directive and the personal data breach notification obligations under the GDPR[xxxi] are triggered by different circumstances, they have some partially overlapping yet different purpose and the recipient of the notification is a different authority[xxxii].

  While the GDPR mandates notification to the competent data protection authority when there is a risk to personal data, the NIS Directive requires EOS and DSP to notify competent authorities under the Directive whenever there is respectively a significant impact on the continuity of the essential service or a substantial impact on the provision of the service offered by the DSP. The criteria to assess the different notification obligations are also different. The NIS directive focuses on the security of information systems and service recovery while the GDPR focus on the protection of individuals and their personal data. Furthermore the GDPR requires to also notify individuals possibly affected, under specific circumstances and conditions[xxxiii].

In any event, we advise to give more clarity to the targeted organisations (OES and DSP) and Member States on the fact that the security and notification requirements under the NIS Directive do not override or replace those under the GDPR, but rather that both legal texts apply and need effective integrated implementation.

In this context, we join the Commission in inviting the Coordination Group provided for by the NIS Directive to support Member States in taking a consistent approach in the process of identification of the OES, when acting in accordance with Article 5(6) of the NIS Directive.

We note that the Commission also launched a consultation on an Implementing Regulation aimed at providing further specification on the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact[xxxiv]. We invite the Commission to ensure that the future Implementing Regulation supports an approach that is not only compatible but effectively benefits from and complements the legal provisions on data breach obligations, as well as the practical guidance on this matter provided by data protection authorities in the Article 29 Working Party and the future European Data Protection Board (EDPB).

In order to achieve a consistent approach in implementing the NIS Directive and the GDPR, we recommend an enhanced co-operation among the data protection supervisory authorities and the NIS national competent authorities, ENISA and the CSIRTs to address the fragmentation of the different frameworks regarding the security and notification obligations of the organisations and support them in the development methodologies and tools for an integrated approach to information security risk and data breach management that could be effective in complying with the requirements of the NIS, the GDPR and any other applicable legislation.

IV. On the proposed Cybersecurity Act *(hereinafter 'the Proposal")*.

1. On the ENISA reform

We welcome the permanent mandate and new tasks and resources allocated to ENISA. We take note that its increased role of assisting and advising on the development and review of Union policy and law in the area of cybersecurity can be key to a more effective protection of the EU digital assets and the policies they support. We consider that a strong mandate in policy development requires an appropriate governance model for the Agency, which ensures coordination with other organisations with tasks in related domains, as well as the full control by the Institutions of the Union, in particular with respect to preparation and implementation of legislation.

In addition to an extended policy function, the proposed Regulation would allocate to ENISA an operational role of knowledge hub for incidents pursuant to the NIS, eIDAS and the Directive establishing the European Electronic Communications Code (Article 5(5) of the Proposal.

We welcome that Article 7 confirms that ENISA will be tasked with operational cooperation with, among others, Union institutions, bodies, offices and agencies, and supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern.

Article 20 confirms the existence and the role of a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, including representatives of the data protection supervisory authorities. Even though the PSG has only an advisory function, we believe that more substantial representation of supervisory authorities for data protection would strongly benefit the Group and contribute to better quality of its advice.

We notice some changes in references to ENISA competences on privacy and personal data protection in the Proposal.

Even though in the substantive provisions there is no real change in ENISA tasks on privacy and data protection (see Article 3(e) of Reg. 526/2013 and Article 7(2) of the Proposal), many recitals of Regulation 526/2013 directly referred to such tasks (recitals 13, 16). These recitals are no longer in the Proposal and there is no mention of privacy and data protection in Article 10 on ENISA tasks relating to research and innovation.

We regret the disappearance of this task in research and advice is likely to lead to discontinuation of ENISA's work on privacy and data protection enhancing technologies (PET)[xxxv] and more in general on data protection by design and by default[xxxvi], since we strongly believe that there is a need to boost such research and advice activities, in particular with a view to the obligations on data protection by design and by default created by the GDPR. There are currently no EU bodies which could fill the possible gap.

We recommend that the legislator consider how to best continue and improve this policy task, either by explicit confirming ENISA role on it via substantive provisions in the Proposal or by handing over the personal data protection competencies to another EU body. Personal data protection includes security but it is not limited to it and a mandate on this policy aspect should be framed within a specialised context and supported by adequate resources.

The EDPS, which has the duty under Article 46 (e) of Reg.45/2001 to "*monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies*" is ready to continue and increase its contribution, either in tighter collaboration with ENISA or any other way the legislator will provide for, provided adequate resources are made available.

One option to enhance research and advice on data protection enhancing technologies would be to give a stronger mandate to the EDPS, where feasible reflected in the ongoing reform of Regulation 45/2001 and, elaborating on the already existing tasks, to monitor and promote the development of PETs and methods for data protection by design and by default. This task could be performed in coordination with relevant national research carried out by academia, industry and public authorities, including data protection authorities, provided that the necessary resources are allocated by the budgetary authorities.

2. European Cybersecurity Certification Framework

Increasing transparency of cybersecurity assurance, which is one of the driving objectives of the new proposal, increases the ability of users to trust providers of digital services processing personal data and contributes to the ability of controllers to choose processors providing guarantees to comply with the security obligation of data protection law.

According to its Article 43, the Cybersecurity Act proposal aims to establish a cybersecurity certification framework, which aims to issue certificates which "*shall attest that the ICT products and services that have been certified (...) comply with specified requirements as regards their ability to resist at a given level of assurance*" actions aimed at compromising security. The object of certification are products and services, the objectives are related to resilience against actions which are aimed to compromise central security objective and the certification concerns three different levels of assurance. National certification supervisory authorities will, among others, be competent to handle complaints lodged by natural or legal

persons in relation to certificates issued by conformity assessment bodies established in their territories and may impose penalties in accordance with national Member State law[xxxvii].

This framework differs substantially from the approach employed by the GDPR. Certification of one or more processing operations under Article 42 of the GDPR may contribute to demonstrating compliance with the GDPR itself in certain circumstances, in application of the accountability principle. The WP29 is currently developing guidance on the certification and accreditation criteria in the GDPR. Among other elements, the certification schemes recognized under the GDPR may cover the obligations under Article 32 of the GDPR on the security of processing operations. Object of certification under the GDPR are personal data processing operations, security is only one of the areas covered, and the concept of assurance levels is not applicable.

As the same organisations may be pursuing certifications under both instruments, it is of the utmost importance that technical and governance synergies be created so that certifications under the European Cybersecurity Certification Framework and under the GDPR are not perceived as contradictory or unrelated by the organisations striving for compliance with the relevant instruments. While the different scope of the certification schemes prevents their seamless integration, the EU bodies involved in their implementation should ensure that they complement and reinforce each other. The Commission and ENISA are invited to liaise with the WP29 and the future EDPB for possible cooperation. Before the Commission considers an implementing act on a certification scheme under Art. 44 of the proposed Cybersecurity Act, it may consult the EDPB and take account of its view.

Co-operation with national data protection supervisory authorities, where necessary, would allow more effective supervision for both types of competent authorities. The Cybersecurity Act should explicitly include data protection supervisory authorities among the authorities to co-operate with (Article 50(6)(d)).

Brussels, 15 December 2017

Wojciech Rafał WIEWIÓROWSKI

Notes

[i] Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy, JOIN/2017/0450 final, 13.09.2017, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2017:450:FIN

[ii] 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/2017/0477 final, 13.09.2017, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0477R(01)

[iii] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239, 19.9.2017, p. 36.

[iv] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM/2017/0476 final, 13.9.2017, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:476:FIN

[v] https://ec.europa.eu/digital-single-market/en/cyber-security

[vi] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, COM(2017)489, 13.9.2017, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0489

[vii] Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union, COM(2017) 608 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0608

[viii] EDPS Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), of 10 December 2010 https://edps.europa.eu/sites/edp/files/publication/10-12-20_enisa_en.pdf

[ix] EDPS Comments on DG CONNECT's public consultation on improving network and information security (NIS) in the EU, of 12 October 2012: https://edps.europa.eu/sites/edp/files/publication/12-10-10_comments_nis_en.pdf

[x] EDPS Opinion on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, of June 2013: https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_en.pdf

[xi] EDPS Opinion on Dissemination and use of intrusive surveillance technologies, of 15 December 2015: https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf

[xii] EDPS Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001, of 21 March 2016: https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf

[xiii] 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, 4.5.2016, p. 1.

[xiv] See definition of 'controller' in Article 4(7) of the GDPR.

[xv] See definition of 'processor' in Article 4(8) of the GDPR.

[xvi] See definition of 'personal data breach' in Article 4(12) of the GDPR.

[xvii] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1.

[xviii] 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 (Regulation on Privacy and Electronic Communications), COM/2017/010 final, 10.1.2017, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010

[xix] Special Eurobarometer 464a, Europeans' attitudes towards cyber security, published September 2017,

[xx] CERT-EU Security Advisory 2017-012 of May 22, 2017, WannaCry Ransomware Campaign Exploiting SMB Vulnerability, https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf

[xxi] Speech by Giovanni Buttarelli, EDPS, "Chiffrement, Sécurité et Libertés at Assemblée nationale française, Paris, France": https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/encryption-protects-security-and-privacy_en

[xxii] Scientific Opinion No. 2/2017 of 24 March 2017 of the High Level Group of Scientific Advisors to the Commission on Cybersecurity in the European Digital Single Market, section 4.1.3, https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf-

[xxiii] Cf. endnote xi.

[xxiv] Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast), COM(2016) 616 final, 28.9.2016

[xxv] 2016/0295(COD) Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items. Recast,

[xxvi] See for example: https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html

[xxvii] Cf. endnote x.

[xxviii] Examples of such sector specific legislation are given in the Communication, and in the NIS Directive :

- Obligations under Directive 2002/21/EC applicable to public communications networks and publicly available electronic communications services.
- Obligations under the eIDAS Regulation 910/2014.
- Notifications under Directive 2014/64/EU on markets in financial instruments.
- Obligations under Regulation 648/2012 of the European parliament and of the Council on central counterparties and trade repositories.
- Obligations under Payment Service Directive 2.

[xxix] For example Article 16(11) of the NIS Directive.

[xxx] See Articles 14 and 16 of the NIS Directive.

[xxxi] The Article 29 Working Party has issued draft guidelines on how to interpret the GDPR provisions on personal data breaches: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741 A final version will be issued in the forthcoming months.

[xxxii] See also ENISA, Incident notification for DSPs in the context of the NIS Directive - A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive, February 2017, p. 20, available at www.enisa.eu: "*DSPs might have to report the same incident to both authorities responsible. In theory, GDPR covers the privacy of personal data and the NISD covers the confidentiality of the service offered and the underlying data (which in most cases is personal data). The GDPR has no notion of a 'light touch approach' as used by the NISD*".

[xxxiii] See Article 34 of the GDPR

[xxxiv] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-4460501_et

[xxxv] e.g. Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies of March 2016 and subsequent measures on PETS; Privacy Enhancing Technologies: Evolution and State of the Art, March 2017, https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art

[xxxvi] e.g. Report on Privacy and Data Protection by Design, January 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[xxxvii] cf. Art. 50(7) and Art. 54 of the Cybersecurity Act proposal.