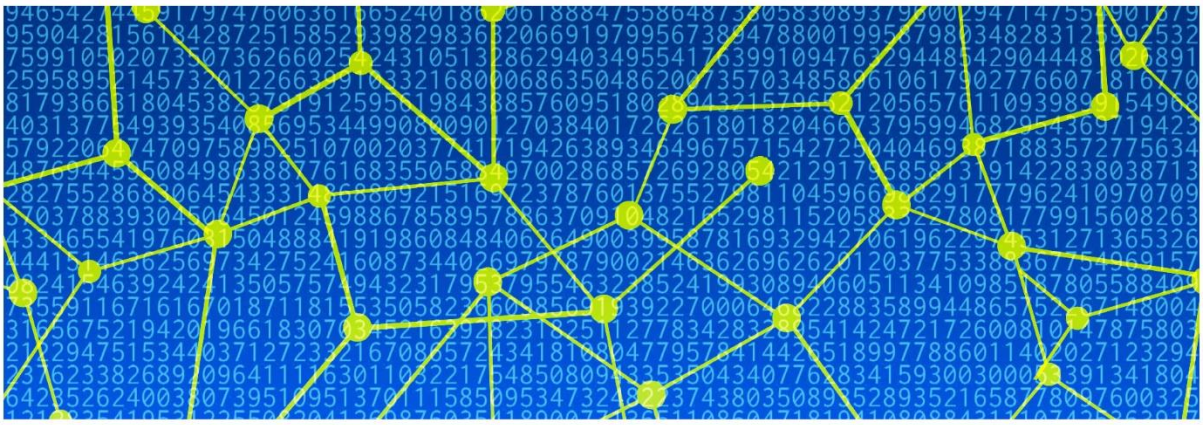

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 5/2021

on the Cybersecurity Strategy and the NIS 2.0 Directive

EDPS

11 March 2021

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Wiewiorówski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under Article 42(1) of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data' and under Article 57(1)(g), the EDPS shall 'advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data'.

This Opinion is issued by the EDPS, within the period of eight weeks from the receipt of the request for consultation laid down under Article 42(3) of Regulation (EU) 2018/1725, having regard to the impact on the protection of individuals' rights and freedoms with regard to the processing of personal data of the Commission Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

Executive Summary

On 16 December 2020, the European Commission has adopted a proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 ('the Proposal'). In parallel, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued a Joint Communication to the European Parliament and the Council, titled 'The EU's Cybersecurity Strategy for the Digital Decade' ('the Strategy').

The EDPS fully supports the overall objective of the Strategy to ensure a global and open internet with strong safeguards for the risks to security and the fundamental rights, recognising the strategic value of the Internet and its governance and reinforcing the Union action therein, in a multi-stakeholders model.

The EDPS therefore equally welcomes the aim of the Proposal to introduce systemic and structural changes to the current NIS Directive in order to cover a wider set of entities across the Union, with stronger security measures, including mandatory risk management, minimum standards and relevant supervision and enforcement provisions. In this regard, the EDPS considers that **it is necessary to fully integrate Union institutions, offices, bodies and agencies in the overall EU-wide cybersecurity framework** for achieving a uniform level of protection, **by including Union institutions, offices, bodies and agencies explicitly in the scope of the Proposal**.

The EDPS further highlights the importance of **integrating the privacy and data protection perspective in the cybersecurity measures** stemming from the Proposal or from other cybersecurity initiatives of the Strategy in order to ensure a holistic approach and enable synergies when managing cybersecurity and protecting the personal information they process. It is equally important that that any potential limitation of the right to the protection of personal data and privacy entailed by such measures fulfil the criteria laid down in Article 52 of EU Charter of Fundamental Rights, and in particular that they be achieved by way of a legislative measure, and be both necessary and proportionate.

It is the expectation of the EDPS that **the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data**, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments. This means that all cybersecurity systems and services involved in the prevention, detection, and response to cyber threats should be compliant with the current privacy and data protection framework. In this regard, the EDPS considers it important and necessary to establish a clear and unambiguous definition for the term "cybersecurity" for the purposes of the Proposal.

The EDPS issues specific recommendations to ensure that the Proposal correctly and effectively **complements the existing Union legislation on personal data protection**, in particular the GDPR and the ePrivacy Directive, also by involving the EDPS and the European Data Protection Board when necessary, and establishing clear mechanisms for the collaboration between competent authorities from the different regulatory areas.

Furthermore, the provisions on managing **internet Top Level Domain registries** should clearly define the relevant scope and conditions in law. The concept of the proactive scans of network and information systems by the CSIRTs equally requires further clarifications on the scope and the types of personal data processed. Attention is drawn to the risks for possible non-

compliant data transfers related to the outsourcing of cybersecurity services or the acquisition of cybersecurity products and their supply chain.

The EDPS **welcomes the call for the promotion of the use of encryption**, and in particular end-to-end encryption, and reiterates his position on encryption as a critical and irreplaceable technology for effective data protection and privacy, whose circumvention would deprive the mechanism of any protection capability due to their possible unlawful use and loss of trust in security controls. To this end, it should be clarified **that nothing in the Proposal should be construed as an endorsement of weakening end-to-end encryption** through "backdoors" or similar solutions.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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)[1],

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 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[2], and in particular Article 42(1), 57(1)(g) and 58(3)(c) thereof,

Having regard to 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],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1. On 16 December 2020, the European Commission has adopted a proposal for a Directive of the European Parliament and of the Council, on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148[4] ('the Proposal').

2. On the same date, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued a Joint Communication to the European Parliament and the Council, titled 'The EU's Cybersecurity Strategy for the Digital Decade' ('the Strategy').[5]

3. The Strategy aims to strengthen the Union's strategic autonomy in the fields of cybersecurity and to improve its resilience and collective response as well as to build a global and open Internet with strong guardrails to address the risks to the security and fundamental rights and freedoms of people in Europe.[6]

4. The Strategy contains proposals for regulatory, investment and policy initiatives in three areas of EU action: (1) resilience, technological sovereignty and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing a global and open cyberspace.

5. The Proposal constitutes one of the regulatory initiatives of the Strategy, and in particular in the area of resilience, technological sovereignty and leadership.

6. According to the Explanatory Memorandum, the aim of the Proposal is to modernise the existing legal framework, i.e. Directive (EU) 2016/1148 ('NIS Directive')[7]. The Proposal aims to build on and repeal the current NIS Directive, which was the first EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the Union. The Proposal takes account of the increased digitisation of the internal market in recent years and of an evolving cybersecurity threat landscape, as amplified since the onset of the COVID-19 crisis. The Proposal aims to address several identified shortcomings of the NIS Directive and aims to increase the level of cyber resilience of all those sectors, public and private, that perform an important function for the economy and society.

7. The main elements of the Proposal are:

   (i) the expansion of the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society;
   (ii) stronger security requirements for covered companies and entities, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied;
   (iii) addressing the security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships;
   (iv) enhancement of cooperation between Member State authorities and with Union institutions, offices, bodies and agencies in dealing with cybersecurity related activities, including cyber crisis management.

8. On 14 January 2021, the EDPS received a request for formal consultation from the European Commission, on the "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148".

2. GENERAL COMMENTS

2.1. On the Cybersecurity Strategy

9. The EDPS welcomes the Cybersecurity Strategy and fully supports its objective to ensure a global and open internet with strong safeguards for the risks to security and the fundamental rights, recognising at the same time the strategic value of the Internet and its governance and reinforcing the Union action therein, in a multi-stakeholders model.

10. Article 5(1)(f) of Regulation (EU) 2016/679 (GDPR)[8] has established security as one of the main principles relating to the processing of personal data. Article 32 GDPR further defines this obligation, applicable to both controllers and processors, to ensure an appropriate level of security. Both provisions make clear that security is essential for compliance with EU data protection law. This is why the EDPS agrees that improving cybersecurity is essential for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and strongly supports the proposal for a comprehensive package of relevant effective technical and organisational measures.

11. At the same time the EDPS recalls that the pursuance of the objectives of cybersecurity may lead to deploying measures that interfere with the rights to data protection and privacy

of individuals. This means ensuring that any potential limitation of the right to the protection of personal data and privacy must fulfil the requirements of Article 52(1) of EU Charter of Fundamental Rights, in particular being achieved by way of a legislative measure, being both necessary and proportionate[9], and respecting the essence of the right.

12. Security rules, security policies and security standards form the backbone of a proper cybersecurity and information security management. For this reason, the EDPS welcomes in particular the intention of the Strategy to establish:
    - Security rules for the cybersecurity as well as the information security of the Union's institutions, offices, bodies and agencies;
    - Security rules for the cybersecurity of all connected products (IoT) and associated services;
    - Security standards on the security of 5G and future generation mobile networks, with particular focus on the security of the supply chain.

13. The EDPS fully supports the initiatives of the Strategy regarding 'technological sovereignty and leadership'. In his Strategy for 2020-2024[10], the EDPS expressed his strong support for policy initiatives promoting 'digital sovereignty', where data generated in Europe is converted into value for European companies and individuals, and processed in accordance with European values. The EDPS therefore particularly welcomes the following initiatives:
    - the building of a network of Security Operations Centres across the EU;
    - the initiative to deploy a secure quantum communication infrastructure (QCI) built with European technology;
    - the development of a public European DNS resolver service; and
    - the establishment of the Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN), that will support developing the EU's technological sovereignty, and reduce dependence on other parts of the globe for the most crucial technologies.

14. The EDPS is aware of the potential of artificial intelligence in developing advanced cybersecurity capabilities for the **real-time detection, analysis, containment and response** to cyber threats in a continuously enlarged digital landscape. However, these technologies generally require processing of large amounts of personal data (e.g. user log data) and come with their own risks that need to be identified and mitigated (e.g. lack of transparency or bias). Use of technologies for improving cybersecurity should not unduly interfere with the rights and freedoms of individuals. The first step to avoid or mitigate those risks is to apply the **data protection by design and by default requirements laid down in Article 25 GDPR**, which will assist in integrating the appropriate safeguards such as pseudonymisation, encryption, data accuracy, data minimization, in the design and use of these technologies and systems.

15. Whereas the security of the information processed by critical and important organisations and infrastructure, as identified in the Proposal, is of the utmost importance for the EU economy and society, the protection of privacy and personal data is widely supported also by small and medium enterprises (SMEs) providing digital services and needs adequate cybersecurity awareness and skills among individuals. **This is why the EDPS welcomes the plan for a widespread adoption of cybersecurity technologies through dedicated support to SMEs under the Digital Innovation Hubs and other instruments**, as well as

plans for a strengthened cybersecurity awareness among individuals, especially children and young people, and organisations, especially SMEs, through the Revised Digital Education Action Plan.

16. The EDPS submits that the legislator, as well as Member States and EU institutions, should take into account the role of cybersecurity in the protection of privacy and personal data by considering this "dimension" in all the above-mentioned policy actions, and in particular the need to protect individuals and their fundamental rights and have these, too, as assets to protect, further to other kinds of assets under their responsibility. **Integrating the privacy and data protection perspective in the traditional cybersecurity management will ensure a holistic approach and enable synergies to public and private organisations when managing cybersecurity and protecting the information they process without useless multiplication of efforts.**

17. **The EDPS welcomes that the Strategy considers Union institutions, offices, bodies and agencies (EUIs) both as organisations to defend together with Member States entities and actors as part of an EU-wide coordinated cybersecurity approach.** This holds true in particular with a view to the creation of a Joint Cyber Unit (JCU), whose planned purpose is to improve and accelerate coordination among all actors and allow the EU to face up and respond to large-scale cyber incidents and crises. The Strategy notes that as "*part of their contribution to the JCU, the EU actors (Commission and EU agencies and bodies) will therefore be ready to increase significantly their resources and capabilities, so as to level up their preparedness and resilience*". **The EDPS recommends that the co-legislators consider and plan for these resources to be used by EUIs** to strengthen their cybersecurity capacity, including in a way that is fully respecting the EU's values.

18. As mentioned above in the more general context of the Strategy, we recommend that the actions and the relevant increase in resources take into account the privacy and data protection dimensions of cybersecurity by investing in policies, practices and tools where the privacy and data protection perspective is integrated in the traditional cybersecurity management and effective data protection safeguards are integrated when processing personal data in cybersecurity activities.

2.2. On the Proposal

19. The EDPS welcomes the aim of the Proposal to introduce systemic and structural changes to the current NIS Directive in order to cover a wider set of entities across the Union, with stronger security measures, including minimum standards and relevant supervision and enforcement provisions and by promoting the collaboration and shared responsibilities and accountability.

20. The EDPS expects that the proposed changes will have a positive impact on the security of personal data and electronic communications, both by improving the cybersecurity practices the entities that are directly covered by the Proposal, as well as by improving the security of the internet more generally.

21. The EDPS welcomes the numerous references to the protection of fundamental rights, including the right to data protection and privacy in various parts of the text of the Proposal.

2.3. On the scope of the Strategy and of the Proposal to the Union institutions, offices, bodies and agencies

22. The Strategy proposes specific actions aimed to boost the information security posture of EUIs and harmonise it among the various EUIs. These actions include:

    a) two legislative proposals for common binding rules on information security and for common binding rules on cybersecurity for all EUI's in 2021;

    b) increased investments to reach a high level of cyber maturity;

    c) a reinforced CERT-EU with an improved funding mechanism.

23. The EDPS shares the Commission's conclusion in the Strategy that the level of cyber resilience and ability to detect and respond to malicious cyber activities varies significantly across EUI's in terms of maturity. We also take note of the involvement of EUIs such as ENISA and the Commission in the ensuring a high level of cybersecurity in the Member States.

24. The EDPS takes note however that the provisions of the Proposals are addressed only to the Union's Member States. Given the recognised need to improve the overall level of cybersecurity through **consistent and homogeneous rules**, the EDPS **recommends that the co-legislators take into account EUIs needs and roles so that EUIs can be integrated in this overall EU-wide cybersecurity framework** as entities enjoying the same high level of protection as those in the Member States.

25. To this aim, **the EDPS suggests including Union institutions, offices, bodies and agencies explicitly in the scope of the Proposal**. Alternatively, the EDPS recommends that co-legislators include in the text of the Proposal an explicit obligation for the Commission to propose separate legislative proposals for EUIs still within the year 2021, so as to create an actionable link between the Proposal itself and the future legislative action at EUIs level in order to achieve consistent and homogeneous rules for Member States and EUIs.

3. SPECIFIC RECOMMENDATIONS

26. The remainder of this Opinion contains specific recommendations to ensure that the Proposal complements the existing Union legislation on personal data protection, in particular the GDPR and the ePrivacy Directive[11] effectively and increases the protection for the fundamental rights and freedoms of the individuals concerned.

3.1. Relationship to existing Union legislation on personal data protection

27. The EDPS observes that the Proposal in different parts[12] clarifies that it is "without prejudice" to the GDPR and the ePrivacy Directive but only with reference to specific contexts, and sometimes only the one of the two instruments is mentioned.

28. The EDPS notes that, in order to comply with the Proposal, entities covered by it will have to deploy certain cybersecurity controls which will most likely involve the processing of personal data and of electronic communications data, including traffic data.

29. The EDPS therefore considers that the extension of the scope of the Proposal to a wider set of activities will entail an increase in the processing of personal data for cybersecurity purposes. Furthermore, the EDPS notes that in line with Article 2(2), the Proposal also applies to 'public electronic communications networks or publicly available electronic communications services', which are also covered by the ePrivacy Directive. This means that the requirements of both the GDPR and the ePrivacy Directive will need to be taken into account.

30. The EDPS notes that organisations acting as controllers and processors do not always realise that the data processed in cybersecurity systems and services may constitute personal data (e.g. IP addresses, device identifiers, network log files, access control log files, etc.). This leads to non-compliance with the GDPR especially as to principles such as purpose limitation, storage limitation, data protection by design and by default, and obligations for compliant data transfers. The EDPS considers that it must be made evident that all cybersecurity systems and services involved in the prevention, detection, and response to cyber threats should be compliant with the current data protection framework and should take relevant technical and organisational safeguards to ensure this compliance in an accountable way.

31. The EDPS therefore considers it necessary to clarify in Article 2 that the **Union's legislation for the protection of personal data**, in particular the GDPR and the ePrivacy Directive, **shall apply to any processing of personal data falling within the scope of the Proposal** (instead just within specific contexts). A corresponding recital should equally clarify that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments.

3.2. The definition of cybersecurity

32. The EDPS observes that the main term of the Proposal is "cybersecurity" (also in the title of the Proposal), while in the current NIS Directive the main term is "security of network and information systems". However, the term "security of network and information systems" continues to be used in the Proposal alongside the term 'cybersecurity'. Moreover, these terms are not used in a coherent manner throughout the text.

33. In the Proposal, "cybersecurity" is defined in the Article 4(3), which refers to Article 2(1) of Regulation (EU) 2019/881[13] as: "*the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*". The term 'cyber threat' as defined in Article 2(8) of Regulation (EU) 2019/881 means "*any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons*".

34. According to Article 4(2) of the Proposal[14] , the term "security of network and information systems" is defined as: "*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*".

35. The EDPs submits that the term "cybersecurity", as defined in Regulation (EU) 2019/881 and equally used in the Proposal, takes into account adverse impacts also on "*...users of such systems and other persons*". This definition allows to take into account the management of the risks to fundamental rights and freedoms of individuals when their personal data are processed via network and information systems and implies an integrated approach.

36. At the same time we note that the term "security of network and information systems" does not include this perspective, since *it does not explicitly refer to the protection of individuals*. This is not an issue insofar as the term is used only to emphasize the focus on the network and information systems infrastructure as such, and the primary need for protection of these assets, which is then functional to the protection of other assets including individuals. Nevertheless, the EDPS observes as these two terms are used almost in an interchangeable way in the Proposal [15] with possible unintended operational consequences as to the need to take into account the protection of individuals.

37. The EDPS thus invites the co-legislators to clarify this issue. The EDPS suggests that given the broader scope, the term "cybersecurity" should be used in general and that the term of "security of network and information systems" be used only when the context (e.g. a purely technical one, without having regard to impacts also on users of systems and other persons) allows it.

3.3. Domain names and registration data ('WHOIS data')

38. The EDPS welcomes Recital 59 of the Proposal, which states that where processing of 'WHOIS data' includes personal data, such processing shall comply with Union data protection law. Additionally, Recital 60 also confirms that access to these data by competent authorities should comply with Union data protection law insofar as it is related to personal data. As indicated above (see section 3.1), the EDPS strongly recommends adding (in Article 2) a general substantive provision on the application of Union data protection law, instead of several instances.

39. Article 23(2) of the Proposal refers to the "*relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs*". The EDPS recommends **clearly spelling out what constitutes "relevant information"** for purposes of this provision, including personal data, taking into account the principles of necessity and proportionality. Doing so would promote legal certainty, as well as a ensuring a consistent approach across the EU's 27 Member States.

40. Article 23(4) of the Proposal furthermore requires Member States to ensure that the registries and the entities providing domain name registration services publish, without undue delay, domain registration data which are not personal data. The EDPS equally recommends clarifying in greater detail **which categories of data domain registration data** (which do not constitute personal data) **should be the subject of publication**.

41. Recital 14 of the GDPR states that it '*does not cover processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person*'. The EDPS recalls that while the contact details of a legal person are outside the

scope of GDPR provided they do not identify a natural person, the contact details concerning natural persons are within the scope of GDPR[16].

42. Moreover, Article 4(1) GDPR defines personal data as 'any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Even the data concerning legal persons may therefore in some cases be considered as personal data, as the clarified by the CJEU[17]. In these cases, the determining factor is whether the information 'relates to' an 'identifiable' natural person.

43. Article 23(5) of the Proposal requires Member States to ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. The Proposal neither defines what is to be understood by "lawful and duly justified requests", nor defines "legitimate access seekers", nor specifies any purposes for such access. The Proposal also does not lay down any objective criterion by which to determine the limits of the access of "legitimate access seekers" to the data and their subsequent use.

44. Article 23(5) of the Proposal creates an obligation for Member States to interfere with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data[18].

45. In accordance with Article 52(1) of the Charter, the CJEU has repeatedly clarified that the legal basis which permits the interference must itself define the scope of the limitation on the exercise of the right concerned[19]. In accordance with the principle of proportionality, any derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary.[20] In order to satisfy that requirement, the legislation in question which entails the interference **must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards**, so that the persons whose data has been accessed have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing.[21]

46. In view of these requirements, **the EDPS underlines that the text of the Proposal must therefore further clarify which (public or private) entities might constitute *"legitimate access seekers"***. For example, it should be clarified whether access shall be limited to those entities identified in recital (60) of the Proposal, or whether any other category of recipients may be given access. The EDPS submits that in practice entities outside the EEA might also request access to specific domain name registration data. For this reason, the EDPS invites the legislators to clarify in this Proposal whether or not the personal data held by the TLD registries and the entities providing domain name registration services for the TLD

should also be accessible by entities outside the EEA. If that is to be the case, the Proposal should clearly lay down the conditions, limitations and procedures for such access, taking into account also the requirements of Article 49(2) GDPR, where applicable.

47. In the same vein, the EDPS also recommends introducing further clarification as to **what constitutes a *"lawful and duly justified"* request** on the basis of which access shall be granted, and under which conditions.

3.4. 'Proactive scanning of network and information systems' by CSIRTs

48. The EDPS observes that Article 10(2)(e) of the Proposal assigns CSIRTs with the task to provide, upon request of an (essential or important) entity, a "*proactive scanning of the network and information systems used for the provision of their services*". The EDPS understands this as referring not only to network scanning but also to scanning of information systems in general (applications, servers, and databases).

49. Recital 25 states that "*[a]s regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council as regards personal data, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services*".

50. The EDPS notes that recital 69 further clarifies the activities of CSIRTs, specifying their purpose in general terms (i.e. 'ensuring network and information security by entities') and scope (i.e. 'measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools') and the types of personal data that might be involved (i.e. 'IP addresses, uniform resources locators (URLs), domain names, and email addresses').

51. The EDPS considers that the Proposal does not sufficiently delineate the nature of the processing of personal data involved in proactive scanning. In light of the wording of Recital (69) ("may require"), the EDPS understands that the aim of Article 10(2)(e) is not to enable systematic collection and analysis of personal data and/or electronic communications data by CSIRTs. In the interest of legal certainty, the EDPS recommends that the co-legislators **more clearly delineate the types of proactive scanning which CSIRTs may be requested to undertake** and to **identify the main categories of personal data involved** in the text of the Proposal.

3.5. Outsourcing and supply chain

52. Recitals 42 and 44 of the Proposal imply that there is a possibility for the essential and important entities to outsource parts or the whole of their cybersecurity activities to external Service Providers, like the 'managed security services providers (MSSPs)'.

53. The EDPS recalls that the outsourcing of such activities by the controller, needs to be in full compliance with the GDPR. In particular, the processing by a processor shall be governed by a contract or other legal act under Union or Member State law in accordance

with Article 28 GDPR. Furthermore, the EDPS recalls that transfers of personal data to third countries or international organisations must comply with Chapter V and the relevant case law of the Court of Justice[22].

54. The EDPS welcomes the measures for mitigation of risks due to technical and, where relevant, non-technical factors of the supply chain through coordinated (sectoral) supply chain risk assessments[23]. The EDPS also welcomes that among the criteria to identify the supply chains that should be subject to a coordinated risk assessment, the Proposal identifies the relevance of specific critical ICT services, systems or products processing, inter alia, personal data.

55. The EDPS stresses that among the specific factors to be considered when assessing supply chains for technology and systems processing personal data, **specific attention should be given to those features enabling the effective implementation of the principle of data protection by design and by default**. Doing so could help promote compliance with Article 25 GDPR, as well as contribute to the effective protection of communications and the terminal equipment in the ePrivacy Directive.

56. Furthermore, the EDPS considers that, in the assessment of the supply chain risks, emphasis should be given to **ICT services, systems or products subject to specific requirements in the country of origin that might represent an obstacle to compliance with EU privacy and data protection law**.

57. The EDPS also recommends that the **European Data Protection Board established by Article 68 GDPR (EDPB) be consulted** when defining these criteria and, as necessary, in the coordinated sectoral risk assessment mentioned in the recital 46.

58. The EDPS takes also the opportunity to recommend to mention in a recital that **open source cybersecurity products** (software and hardware), including open source encryption, might offer the necessary transparency to mitigate specific supply chain risks.

3.6. Encryption

59. The EDPS welcomes the inclusion of encryption and cryptography in the list of minimum safeguards for cybersecurity, in Article 18 of the Proposal. In addition, the EDPS welcomes also the references to the encryption in the Strategy[24].

60. The EDPS fully supports the statement contained in Recital 54 of the Proposal regarding the promotion and even the mandatory use of end-to-end encryption by the providers of electronic communications services.

61. Recital 54 also states, however, that the use of end-to-end encryption should be "reconciled" with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. In particular, it is stated that "*[s]olutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime*".

62. The EDPS wishes to reiterate that, in line with the statement of Article 29 Working Party[25] encryption is a critical and irreplaceable technology for effective data protection and privacy. **Strong encryption must be available to be used for the mitigation of high risks for the rights and freedoms of individuals.** As an example of the need to use strong encryption, the EDPS recalls the recent EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[26], which contain certain use cases where strong encryption can be used to mitigate risks related to non-compliant data transfers.

63. Any weakening or circumvention of encryption (e.g. using mandatory backdoors, mandatory key escrow, and hidden communication channels) would completely devoid the mechanism of any effective protection capability due to their possible unlawful use and loss of trust in security controls. It would thus inevitably compromise the protection of the fundamental rights to the protection of personal data and privacy, as it would pose significant risks to the economy and society in general. Even when strong encryption is not used while still available, **unauthorized decryption or reverse engineering of encryption code, or monitoring of electronic communications outside clear legal authority should be prohibited.**

64. While the EDPS understands that law enforcement requires the means to fight crime on the internet, any measure interfering with confidentiality of communications must comply with the requirements of legality, necessity and proportionality, based on substantiated evidence. While encryption makes bulk data collection and mass surveillance difficult, it is not a limiting factor to more targeted and specific measures. **The EDPS therefore recommends clarifying in recital 54 that nothing in the Proposal should be construed as an endorsement of weakening end-to-end encryption through "backdoors" or similar solutions**.

3.7. Cybersecurity risk management measures

65. The EDPS welcomes Article 18 which requires Member States to ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems as well as the minimum set of measures provided in Article 18(2).

66. The EDPS recalls that the management of risks for the rights and freedoms of individuals, when their personal data are processed, is an obligation for all controllers (and not only essential and important entities) under Article 32 of the GDPR. Whereas the Cybersecurity risk management measures of Article 18 of the Proposal aims at protecting network and information systems of the organisation (and the data therein), Article 32 GDPR aims at protecting individuals (not necessarily belonging to the same organisation) and their rights by protecting their data. There is a difference in the assets to protect in the two activities, which might lead to different conclusions in certain circumstances. At the same time, the cybersecurity risk management process can contribute to the assessment of the data protection impact of weaknesses in the security of personal data. As stated above as to the wider measure of the Strategy, the EDPS recommends **integrating the privacy and data protection considerations into cybersecurity risk management** to ensure a holistic approach and enable synergies to public and private organisations when managing cybersecurity and protection the information they process without unnecessary multiplication of efforts.

67. **The EDPS suggests adding these considerations both in recitals and in the substantive part of the Proposal**, in a way that possible future Commission implementing acts, EU level guidance on cybersecurity from ENISA as well as its work on European cybersecurity certification schemes (see Article 21 of the Proposal), and work from EU standardisation bodies (see Article 22), could take them into account and thus integrate the management of the risks for individuals and their fundamental rights stemming from cybersecurity threats.

68. Given the strong links between cybersecurity management and personal data protection the EDPS also suggests **adding an obligation for ENISA to consult the EDPB** when drawing up relevant advice. These acts and guidance can also be useful to those organisations that are not under the scope of the Directive but could still provide similar benefits as well as promote compliance with the GDPR obligations on security of personal data.

3.8. Personal data breaches

69. Pursuant to Article 20(2) of the Proposal, Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident. Article 20(3) defines when an incident shall be considered "significant". One option is that the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.

70. The EDPS welcomes Article 20(3)(b) of the Proposal which considers not only impacts on the organisation but also those on natural persons who may be affected. At the same time, the EDPS also notes that the definition in Article 20(3)(b) would encompass some "personal data breaches", as defined in Article 4(12) of the GDPR. It seems that the corresponding reporting obligations may also overlap in certain cases with the notification of personal data breaches to competent authorities in accordance with Article 33 GDPR. Nevertheless, the definitions of the circumstances leading to the obligation, the set maximum delays as well as the competent authorities to report/notify are different. Analogous notification obligations to competent authorities are set in the ePrivacy Directive, currently under review.

71. The EDPS welcomes Article 28(2), which establishes that the competent authorities under the Proposal shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches, and thus creates synergies between the legal instruments. The EDPS also welcomes the obligations of Article 32(1) for competent authorities to inform data protection competent authorities when they have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach which shall be notified pursuant to Article 33 GDPR.

72. The EDPS notes that this obligation on competent authorities to notify to GDPR competent authorities is "within a reasonable period of time". The EDPS observes that this obligation is without prejudice to the reporting obligation on controllers as defined in Article 33 GDPR, which must be done "without undue delay" and "not later than 72 hours" after becoming aware of the personal data breach. In order to enable data protection authorities to perform effectively their tasks, **the EDPS suggests to change the wording of the Proposal "within a reasonable period of time" to "without undue delay".**

3.9. Cooperation Group

73. Article 12 of the Proposal establishes a Cooperation Group in order to support and to facilitate strategic cooperation and the exchange of information among Member States in the field of application of the Proposal. Taking into account the task of this Group and possible link with the data protection framework, **the EDPS recommends including a representative of the EDPB as a member of the Cooperation Group**.

3.10. Jurisdiction and territoriality

The EDPS observes that the concept of "main establishment" used in Article 24(2) of the Proposal[27], is defined differently than in Article 4(16) of the GDPR.

74. As regards the GDPR, the concept of "main establishment" is particularly important in cases involving cross-border processing of personal data. Article 56(1) GDPR contains an overriding rule and provide that the supervisory authority of the main establishment or of the single establishment of the controller or processor is competent to act as Lead Supervisory Authority for the cross-border processing carried out by that controller or processor[28]. Consequently, the EDPS recommends **providing a clarification** in the legal text **that the Proposal does not affect the competences of data protection supervisory authorities under the GDPR** (see above, section 3.8).

75. The EDPS reiterates his support for Article 28(2) of the Proposal, which provides that competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches (see above, para. 67).

76. At the same time, the EDPS stresses the need to provide in the Proposal **a more comprehensive legal basis for the cooperation and exchange of relevant information** between the competent authorities under the Proposal and other relevant supervisory authorities, each acting within their respective areas of competence. In particular, the EDPS recommends to make explicit that competent authorities under the Proposal should be able to provide to the competent supervisory authorities under Regulation (EU) 2016/679, upon request or on their own initiative, any information obtained in the context of any audits and investigations that relate to the processing of personal data and to include an explicit legal basis to that this effect.

4. CONCLUSIONS

77. In light of the above, the EDPS makes the following recommendations:

Concerning the Cybersecurity Strategy

- to take into account that the first step to mitigate data protection and privacy risks that are associated with new technologies for improving cybersecurity, such as AI, is to apply the data protection by design and by default requirements laid down in Article 25 GDPR, which will assist in integrating the appropriate safeguards such as pseudonymisation, encryption, data accuracy, data minimization, in the design and use of these technologies and systems;

- to take into account the importance of integrating the privacy and data protection perspective in the cybersecurity related policies and standards as well as in the traditional cybersecurity management in order to ensure a holistic approach and enable synergies to public and private organisations when managing cybersecurity and protecting the information they process without useless multiplication of efforts;

- to consider and plan for resources to be used by EUIs to strengthen their cybersecurity capacity, including in a way that is fully respecting the EU's values;

- take into account the privacy and data protection dimensions of cybersecurity by investing in policies, practices and tools where the privacy and data protection perspective is integrated in the traditional cybersecurity management and effective data protection safeguards are integrated when processing personal data in cybersecurity activities;

On the scope of the Strategy and of the Proposal to the Union institutions, offices, bodies and agencies:

- to take into account the EUIs needs and role so that EUIs be integrated in this overall EU-wide cybersecurity framework as entities enjoying the same high level of protection as those in the Member States; and

- to include Union institutions, offices, bodies and agencies explicitly in the scope of the Proposal.

Concerning the relationship to existing Union legislation on personal data protection:

- to clarify in Article 2 of the Proposal that the Union's legislation for the protection of personal data, in particular the GDPR and the ePrivacy Directive apply to any processing of personal data falling within the scope of the Proposal (instead just within specific contexts); and

- to also clarify in a relevant recital that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments;

Concerning the definition of cybersecurity:

- to clarify the different use of the terms "cybersecurity" and "security of network and information systems"; and to use the term "cybersecurity" in general and the term of "security of network and information systems" only when the context (e.g. a purely technical one, without having regard to impacts also on users of systems and other persons) allows it.

Concerning the domain names and registration data ('WHOIS data'):

- to clearly spell out what constitutes "relevant information" for the purposes of identification and contacting the holders of the domain names and the points of contact administering the domain names under the TLDs;

- to clarify in greater detail which categories of data domain registration data (which do not constitute personal data) should be the subject of publication;

- to clarify further which (public or private) entities might constitute *"legitimate access seekers"*;

- to clarify whether the personal data held by the TLD registries and the entities providing domain name registration services for the TLD should also be accessible by entities outside the EEA, and if that would be the case to clearly lay down the conditions, limitations and procedures for such access, taking into account also the requirements of Article 49(2) GDPR, where applicable; and

- to introduce further clarification as to what constitutes a *"lawful and duly justified"* request on the basis of which access shall be granted, and under which conditions.

Concerning the 'proactive scanning of network and information systems' by CSIRTs:

- to clearly delineate the types of proactive scanning which CSIRTs may be requested to undertake and to identify the main categories of personal data involved in the text of the Proposal.

Concerning outsourcing and supply chain:

- to take into account the features enabling the effective implementation of the principle of data protection by design and by default, when assessing supply chains for technology and systems processing personal data;

- to take into account specific requirements in the country of origin that might represent an obstacle to compliance with EU privacy and data protection law, when assessing the supply chain risks of ICT services, systems or products; and

- to include in the legal text the mandatory consultation of the EDPB when defining the aforementioned features and, as necessary, in the coordinated sectoral risk assessment mentioned in the recital 46.

- to recommend to mention in a recital that **open source cybersecurity products** (software and hardware), including open source encryption, might offer the necessary transparency to mitigate specific supply chain risks

Concerning encryption:

- to clarify in recital 54 that nothing in the Proposal should be construed as an endorsement of weakening end-to-end encryption through "backdoors" or similar solutions;

Concerning Cybersecurity risk management measures:

- to include both in recitals and in the substantive part of the Proposal the concept that integrating the privacy and data protection perspective in the traditional cybersecurity risk management will ensure a holistic approach and enable synergies to public and private organisations when managing cybersecurity and protection the information they process without useless multiplication of efforts;

- to add in the legal text an obligation for ENISA to consult the EDPB when drawing up relevant advice;

Concerning personal data breaches:

- to change the text "within a reasonable period of time" of Article 32(1) to "without undue delay";

Concerning the Cooperation Group:

- to include in the legal text the participation of EDPB in the Cooperation Group, taking into account the link between the task of this Group and the data protection framework.

Concerning jurisdiction and territoriality:

- to clarify in the legal text that the Proposal does not affect the competences of data protection supervisory authorities under the GDPR;

- to provide a comprehensive legal basis for the cooperation and exchange of information among competent and supervisory authorities, each acting within their respective areas of competence; and

- to clarify that competent authorities under the Proposal should be able to provide to the competent supervisory authorities under Regulation (EU) 2016/679, upon request or on their own initiative, any information obtained in the context of any audits and investigations that relate to the processing of personal data and to include an explicit legal basis to that this effect.

Brussels, 11 March 2021

[e-signed]
Wojciech Rafał WIEWIÓROWSKI

Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 295, 21.11.2018, p. 39.

[4] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM (2020) 823 final.
[5] The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final.
[6] See chapter I. INTRODUCTION, page 4 of the Strategy.
[7] 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, OJ L 194, 19.7.2016, p. 1–30
[8] 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. 1–88.
[9] See for more details: EDPS guidelines "Assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data", 19/12/2019, (https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en) as well as the EDPS paper "Necessity toolkit on assessing the necessity of measures that limit the fundamental right to the protection of personal data", 11/04/2017(https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en).
[10] EDPS, Shaping a Safer Digital Future: a New Strategy for a New Decade, 30/6/2020 (https://edps.europa.eu/data-protection/our-work/publications/strategy/edps-strategy-2020-2024-shaping-safer-digital-future_en).
[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37 – 47.
[12] Recital 25 of the Proposal refers only to the Regulation (EU) 2016/679 regarding the proactive scanning of the network and information systems; recital 48, refers to both (EU) 2016/679 and the Directive 2002/58/EC regarding the reporting obligations; recital 56 refers to both (EU) 2016/679 and the Directive 2002/58/EC regarding notification obligations from different regulatory instruments; recital 58 refers only to Directive 2002/58/EC regarding the compromise of personal data in the context of security incidents, -while it should also refer to the Regulation (EU) 2016/679-; Article 26 refers to the Regulation (EU) 2016/679 regarding the exchange of cybersecurity information between Member States; and the Article 32 refers to the Regulation (EU) 2016/679 regarding the Infringements entailing a personal data breach.
[13] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)), OJ L 151, 7.6.2019, p. 15–69.
[14] The same definition exists in the current NIS Directive.
[15] For example in Article 4(4) of the Proposal : '*national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State;*'
[16] https://edpb.europa.eu/sites/edpb/files/files/file1/icann_letter_en.pdf (p. 4)
[17] See Court of Justice of European Union in Joint Cases C92/09, Volker und Markus Schecke Gbr v. Land Hessen, and C-93/09, Eifert v. Land Hessen and Bundesanstalt für Landwirtschaft und Ernahrung, at paragraph 53, where the CJEU considered that legal persons can claim the protection of Articles 7 and 8 of the Charter in so far as the official title of the legal person identifies one or more natural persons.
[18] Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
[19] See, to that effect, Court of Justice of European Union, judgment of 17 December 2015, WebMindLicenses, C-419/14, EU:C:2015:832, paragraph 81.

[20] Court of Justice of European Union, judgments of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, paragraph 56; of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 51 and 52; of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 92; and of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 96 and 103.
[21] Cf. Court of Justice of European Union, Opinion 1/15 of the Court of 26 July 2017, paragraphs 140 and 141.
[22] the judgment C-311/18 (Schrems II) of the Court of Justice of the European Union (CJEU) (http://curia.europa.eu/juris/liste.jsf?num=C-311/18#)
[23] Recital (46) and Article 19 of the Proposal.
[24] These references are: (i) the inclusion of encryption in the set of important technologies for the Strategy, for which the EU needs to ensure control of their supply chain (page 1) and on the other hand the inclusion of encryption in the technologies in which the EU should further develop (page 18); (ii) the statement in section 2.4 of the Strategy, that encryption is regarded as one of the 3 key technologies with which cybersecurity must be integrated; and the intention to develop "new and more secure forms of encryption to shield against cyberattack" in the context of deploying a secure quantum communication infrastructure (QCI) for Europe which will offer high level of confidentiality.
[25] Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, Brussels, April 11 2018: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.
[26] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.
[27] In line with Article 24(2) of the Proposal entities referred to in paragraph 1of Proposal shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken.
[28] See the EDPB Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment adopted on 12 July 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201908_changeofmainorsingleestablishment_en.pdf.