EDPB-EDPS Joint Opinion [4/2026]

on the Proposal for a Cybersecurity Act 2 and the Proposal on amendments to the NIS 2 Directive

Adopted on 18 March 2026

Table of Contents

Executive summary

On 20 January 2026, the European Commission issued a Proposal for a Regulation on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (the Cybersecurity Act 2) and a Proposal for a Directive amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]. On 21 January 2026, the Commission formally consulted the EDPB and the EDPS in accordance with Article 42(2) of Regulation (EU) 2018/1725.

The EDPB and the EDPS recall that the relationship between data protection and cybersecurity is double-sided. On the one hand, cybersecurity serves the protection of personal data by limiting the risks of unwanted access, modification or unavailability of that data. On the other hand, some cybersecurity measures can interfere with individuals' rights and freedoms, in particular the rights to privacy and data protection. Therefore, while effectiveness is an important focus for cybersecurity measures, necessity and proportionality need to be considered.

The EDPB and the EDPS support the Proposals' general objective to strengthen ENISA's role and to facilitate uptake of cybersecurity certification, both subject to the specific recommendations provided in this Joint Opinion. They also welcome the objective to establish mechanisms and conditions in Directive (EU) 2022/2555 to help facilitate compliance with cybersecurity requirements, and in that way make their implementation more coherent and effective, as well as the objective to further address the various risks to ICT supply chains, including the non-technical ones. The EDPB and the EDPS also strongly support the objective of the establishment of a single-entry point for the notification of personal data breaches, as it would reduce the administrative burden for organisations without affecting the level of protection for data subjects.

The EDPB and the EDPS also welcome that the CSA2 Proposal would provide further clarification on the modalities of ENISA providing support to different stakeholders and recommend adding also the EDPS as a possible requestor of advice from ENISA. The EDPB and the EDPS strongly support that such advice would follow a request, ensuring a clear coordination and a clear division of responsibilities.

As concerns the cooperation between ENISA and other Union entities in general, the EDPB and the EDPS welcome the synergies this cooperation can enable, in line with their respective tasks and mandates. They recommend adding an explicit reference also to the EDPS as a Union body, with which ENISA would cooperate.

The EDPB and EDPS consider that if the future tasks of ENISA as information hub would require processing of personal data to a substantial degree, this should be spelled out explicitly in the provisions of the basic act governing the respective tasks, including the essential elements of any large-scale processing and the appropriate safeguards. Conversely, if the aim is to enable ENISA to mainly collect and further process mostly aggregated non-personal data, this should also be clarified.

The EDPB and the EDPS recall that in principle only very technical (practical) details related to the processing of personal data should be left to be decided under the administrative autonomy of the concerned EU body (in this case the Management Board of a decentralised Agency). Additionally, the EDPB and the EDPS recommend providing for in Article 66 of the CSA2 Proposal a prior consultation with the EDPS before adoption of such rules.

With regard to the European Cybersecurity Skills framework ('ECSF'), the EDPB and the EDPS recommend the co-legislators to amend Article 19(2) of the CSA2 Proposal so that the ECSF is not exclusively limited to 'cybersecurity professionals', but also includes profiles for the general workforce.

As concerns the European Cybersecurity Certification Framework, the EDPB and the EDPS recommend further clarifying the scope of Article 80(1)(w) CSA2 and the relationship to GDPR certification. In addition, the EDPB and the EDPS recommend requiring ENISA to consult with the EDPB prior to adopting a certification scheme under Article 80(1)(w) CSA2 to ensure consistency.

The EDPB and the EDPS highlight the need to consider not only the effectiveness of cybersecurity measures, but also their necessity and proportionality. The EDPB and the EDPS recommend clarifying that certification schemes should, to the extent possible, take into account security controls that can help to demonstrate the fulfilment of GDPR requirements, in particular where the schemes apply to ICT products, ICT services, ICT processes and managed security services that are likely to be used in data processing operations.

The EDPB and the EDPS further welcome the proposed measure aimed at ensuring a trusted ICT supply chain framework and addressing non-technical risks in sectors of high criticality.

With regard to the Proposal amending the NIS2 Directive, the EDPB and the EDPS welcome the designation of European Digital Identity Wallets and European Business Wallets providers as 'essential entities', and fully support the important objective of preventing future ransomware attacks and disrupting and dismantling the criminal organisations behind them.

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC,

Have adopted the following Joint Opinion (the 'Opinion')

1 BACKGROUND

1. On 20 January 2026, the European Commission ('the Commission') issued a Proposal for a Regulation on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (the Cybersecurity Act 2)[1] and a Proposal for a Directive amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2][2] (hereafter, 'the CSA2 Proposal', 'the NIS2 amendments Proposal', and jointly 'the Proposals'). On 21 January 2026, the Commission formally consulted the EDPB and the EDPS in accordance with Article 42(2) of Regulation (EU) 2018/1725 ('EUDPR')[3].
2. The CSA2 Proposal aims to replace the current Cybersecurity Act[4] in order to (1) strengthen ENISA's role with a focus on stakeholders' needs in an increasingly hostile threat landscape, (2) to revive the implementation of the European cybersecurity certification framework (ECCF), (3) to reduce complexity and diversity of the cybersecurity-related policies, and (4) to further address ICT supply chain security risks[5].
3. The NIS2 amendments Proposal focuses in particular on the third objective, by introducing clarifications and making compliance for regulated entities easier[6].
4. The aim of this Joint Opinion is to address the relevant aspects of the Proposals which are of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data.

2 GENERAL REMARKS

[1] COM(2026) 11 final.
[2] COM(2026) 13 final.
[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.
[4] 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, pp. 15–69, ELI: http://data.europa.eu/eli/reg/2019/881/oj, as amended by Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services, OJ L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj.
[5] Explanatory memorandum, COM(2026) 11 final, p.1.
[6] COM(2026) 13 final.

5. The CSA2-Proposal aims to expand the mandate for ENISA and make it more operational. The EDPB and the EDPS support the strengthening of ENISA's role and the objective to facilitate the uptake of cybersecurity certification, both subject to the specific recommendations provided below.

6. The EDPB and the EDPS also welcome the objective to establish mechanisms and conditions in Directive (EU) 2022/2555[7] (herinafter 'NIS 2 Directive') to help facilitate compliance with cybersecurity requirements, and in that way make their implementation more coherent and effective, as well as the objective to further address the various risks to ICT supply chains, including non-technical ones.

7. As already stated in their joint opinion on the Digital Omnibus proposal[8], the EDPB and the EDPS strongly support the objective of the establishment of a single-entry point for the notification of personal data breaches, as it would reduce the administrative burden for organisations without affecting the level of protection for data subjects.

8. Article 5(1)(f) of Regulation (EU) 2016/679 (GDPR) establishes 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 of personal data processing is essential for compliance with EU data protection law.

9. The relationship between data protection and cybersecurity is double-sided. On the one hand, cybersecurity serves the protection of personal data by limiting the risks of unwanted access, modification or unavailability of that data. On the other hand, some cybersecurity measures can interfere with individuals' rights and freedoms, in particular the rights to privacy and data protection[9].

10. The EDPB and the EDPS recall that Recital 49 of the GDPR recognises that cybersecurity measures involving the processing of personal data constitute a legitimate interest of the data controller concerned, while underlining at the same time that the measures should be strictly necessary and proportionate for the purposes of ensuring network and information security. As a result, cybersecurity measures should not only be guided by considerations of effectiveness, but also consider whether their impact on fundamental rights remains limited to what is necessary and proportionate.

3 SUPPORT BY ENISA FOR IMPLEMENTATION OF UNION POLICY AND LAW AND COOPERATION WITH OTHER UNION ENTITIES

11. Pursuant to Article 5(1) CSA2 Proposal, ENISA shall contribute to the implementation of Union policy and law in a variety of areas, by providing support to different stakeholders, as listed in that Article.

---

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[8] EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted on 10 February 2026.

[9] Cf. EDPS Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive, 11 March 2021, paragraphs 10-11, EDPS Opinion 7/2022 on the Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union, 17 May 2022, paras. 9-10, and EDPS Opinion 2/2024 on the Proposal for a Regulation amending the Cybersecurity Act as regards managed security services, 10 January 2024, para.5.

12. Amongst them, in line with Article 5(1)(h) CSA2 Proposal, ENISA would provide, at the request of the European Data Protection Board, advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy. The EDPB and the EDPS note that Article 5(1)(h) CSA2 Proposal is not an entirely new provision. Article 5(5)(c) of the current Cybersecurity Act already provides that ENISA may support "Member States in the implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy, including by providing advice to the European Data Protection Board upon request".

13. The EDPB and the EDPS welcome that the CSA2 Proposal would provide further clarification on the modalities of cooperation while maintaining the core elements of Article 5(5)(c) of the Cybersecurity Act. The new Article 5(1)(h) would clarify that the EDPB, as a Union body, is entitled to directly request the advice by ENISA (without being linked to Member States' implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy).

14. At the same time, the EDPB and the EDPS recommend adding also the EDPS as a possible requestor in Article 5(1)(h) CSA2, in view of the latter's role of supervisory authority for personal data processing by European Union institutions, bodies and agencies. Allowing both the EDPB and the EDPS to draw on ENISA's technical competence in the area of cybersecurity may contribute to ensure that their guidance and decisions in the area of data protection field are informed by state-of-the-art cybersecurity knowledge. There could be several subjects for which advice and cooperation may be beneficial, including cybersecurity standards and operational practices, as well the use of PETs in the context of cybersecurity.

15. The EDPB and the EDPS strongly support that the advice mentioned in Article 5(1)(h) CSA2 is only provided after a prior request by the EDPB, or, as here proposed, the EDPS. By providing that ENISA only acts upon request from the EDPB or EDPS, Article 5(1)(h) would ensure a clear coordination and a clear division of responsibilities[10].

16. The EDPB and the EDPS note that Article 5(1)(h) of the CSA2 Proposal appears to be a specific manifestation of a more general cooperation obligation enshrined in Article 68 of the CSA2 Proposal, regulating the cooperation of ENISA with other Union entities. According to Article 68, ENISA shall cooperate on matters related to cybersecurity with other EU bodies, including the European Data Protection Board, to ensure consistency, create synergies and address issues of common concern. Such cooperation may be ensured by means of exchange of know-how and best practices; provision of advice and issuance of guidance on matters related to cybersecurity; and establishment of practical arrangements for the execution of specific tasks, after consulting the Commission.

17. The EDPB and the EDPS welcome the cooperation and the synergies between ENISA and other Union entities, in line with their respective tasks and mandates. In this context, for the sake of legal clarity, the EDPB and the EDPS recommend amending Article 68 of the CSA2 Proposal by adding an explicit reference also to the EDPS as a Union body, with which ENISA would cooperate[11].

[10] By predicating ENISA's involvement upon a request made by supervisory authorities, a structured consultative process is maintained, where ENISA provides technical expertise while the SAs retain full control over decisions related to data protection. It also ensures that any intervention by ENISA is coordinated, with the EDPB or EDPS taking the lead and determining the appropriate course of action. This respect for the established roles promotes consistency, prevents regulatory fragmentation, and reinforces the accountability of data protection bodies in their supervisory role.

[11] The EDPB and EDPS consider that Article 7(2) of the current Cybersecurity Act, which obliges ENISA to cooperate at the operational level and establish synergies with Union institutions, bodies, offices and agencies, inter alia with supervisory authorities dealing with the protection of privacy and personal data, with a view of addressing issues of common concern, already extends to the EDPS.

4 OPERATIONAL COOPERATION, SHARED CYBERSECURITY SITUATIONAL AWARENESS AND PROTECTION OF PERSONAL DATA

18. Under Articles 10 and 11 CSA2 Proposal, which would be a further development of the current Article 7 of the Cybersecurity Act, ENISA would expand its role as a central hub for operational cooperation, including the processing of substantial amounts of threat intelligence information[12]. As a result, one could infer that the information processed by ENISA as part of its role may include personal data, such as IP addresses, user credentials, user logs, financial exchanges or details of compromised accounts.

19. Following the clarifications provided by the European Commission[13], the EDPB and the EDPS understand that no large-scale processing of personal data by ENISA is intended to be mandated and authorised by the CSA2[14].

    While taking note of the fact that ENISA would collect and further process mainly aggregated non-personal data, the EDPB and EDPS nevertheless recall that if the future tasks of ENISA as information hub would require processing of personal data to a substantial degree, this should be spelled out explicitly in the provisions of the basic act governing the respective tasks, including the essential elements of any large-scale processing and the appropriate safeguards. Conversely, if the aim is to enable ENISA to collect and further process mainly aggregated non-personal data, this should also be clarified, at least by way of a recital.

20. The EDPB and the EDPS note that ENISA would continue to process personal data for administrative purposes[15]. Article 66(1) CSA2 Proposal, similarly to the current CSA Regulation[16], contains a general reference to the applicable data protection legislation, i.e. EUDPR, without providing any further specific rules.

[12] Cf. COM(2026) 11 final, Legislative Financial and Digital Statement, p. 19: "The new elements/tasks in the proposal will bring the added value for the European stakeholders that would benefit from ENISA being an information hub, contributing to information sharing and providing alert notification to their constituents", and p. 95: "In the recent years ENISA has become an information hub, holding information from different sources. In this sense, many of the tasks for ENISA are associated with reusing and recycling of information for the purposes of various analyses.".
[13] As provided during an ad-hoc meeting of the Technology Expert Subgroup of the EDPB on 27 February 2026.
[14] The Commission has clarified that ENISA has no mandate to perform operational analysis of incidents, and it has no access to data from the incidents themselves. Instead, the data processed will be aggravated. Alerts from national CSIRTs will typically not include operational personal data, but rather administrative data such as contact information. In the same vein, companies subscribing to receive early alerts might also provide their contact information. According to the European Commission, in the rare event that aggregated threat or incident information provided to ENISA does contain IP addresses, ENISA would have no operational need and consequently no legal and factual possibility to investigate the subscriber behind the IP address. The European Commission further clarified that the help desk envisaged by Art. 13 is of an advisory nature, providing, for example, information about which competent Member State authority to contact.
[15] For example, in the process of examining applications to be authorised as attestation provider under the European individual cybersecurity skills attestation scheme (Article 22), during the appeals process against decisions taken (Articles 36 and following), when handling complaints by natural or legal persons in relation to certification or EU statements of conformity (Article 88(6)(h)) or related to cybersecurity certifications (Article 96).
[16] See Article 41 (1) Regulation (EU) 2019/881.

21. In the same vein, Article 66(2) CSA2 Proposal reproduces the current Article 41(2) CSA, which lays down the possibility for the Management Board of ENISA to adopt 'additional measures necessary for the application of Regulation (EU) 2018/1725' by the Agency[17], without an obligation for the Management Board to take any specific action. The provision of Article 66(2) CSA2 Proposal does not specify the scope and type of such additional data protection measures, nor the applicable procedure for adoption. It also does not clarify the role of the EDPS in the process[18] .

22. It is the understanding of the EDPB and the EDPS that if the Management Board of ENISA does proceed with applying Article 66(2) CSA2 Proposal, its decision(s) should provide additional detail on how ENISA carries out personal data processing.

23. The EDPB and the EDPS recall that in principle only very technical (practical) details related to the processing of personal data should be left to be decided under the administrative autonomy of the concerned EU body, in this case, by the Management Board of a decentralised Agency. This is because authorising interferences with fundamental rights should be a matter better reserved to the legislator and, at most, to the Commission by way of Implementing or Delegated Acts[19]. Therefore, what is exactly meant with the second sentence of the draft Article 66(2) by 'additional measures necessary for the application of Regulation (EU) 2018/1725 by ENISA', should be explicitly clarified in the enacting provision of the Regulation.

24. If it is nevertheless considered necessary that the Management Board should take measures going beyond technical (practical) details of processing already provided for in legislation or delegated or implementing acts, ~~i~~n addition of their scope being more clearly framed, the measures to be adopted by the Management Board should be clear and precise, and their application should be foreseeable for the persons concerned. This includes said rules being given appropriate publicity. Moreover, they should provide for the necessary safeguards to ensure compliance with key data protection principles and safeguards such as purpose limitation, storage limitation, data protection by design and by default. Furthermore, as an important additional safeguard in such cases, the EDPB and the EDPS recommend that Article 66 CSA2 Proposal provides for a prior consultation with the EDPS before adoption of such rules[20].

5 SINGLE-ENTRY POINT FOR INCIDENT REPORTING (ARTICLE 15 CSA2)

[17] On 21 November 2019, the Management Board of ENISA has adopted Decision on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of ENISA, pursuant to Article 25 EUDPR.

[18] For instance, Article 18a(5) Regulation (EU) 2016/794 (Europol Regulation) provides that the Management Board of Europol, acting on a proposal from the Executive Director and **after consulting the EDPS**, shall specify the conditions relating to the provision and processing of personal data [...] (emphasis added).

[19] See the EDPS 'Guidance for co-legislators on key elements of legislative proposals', available at https://www.edps.europa.eu/system/files/2025-05/EDPS_Publication_Guidance_for_co-legislators_EN.pdf, para. 76.

[20] Similarly to what is foreseen in Article 18a(5) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. (Europol Regulation) OJ L 135, 24.5.2016, p. 53.

25. According to Article 15 of CSA2 Proposal, ENISA must establish, provide, operate, maintain and update as necessary, among others, the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555. These tools aim to simplify the different reporting obligations related to cybersecurity[21].

26. As already stated in their joint opinion on the Digital Omnibus proposal[22], the EDPB and the EDPS strongly support the objective of the establishment of a single-entry point for the notification of personal data breaches, as it would reduce the administrative burden for organisations without affecting the level of protection for data subjects. In its EDPB Helsinki Statement[23], the EDPB already underlined its support for a possible cross-regulatory European notification solution as this would help make GDPR compliance easier. The EDPB and the EDPS also recall the importance of ensuring the security of the notifications submitted to and transmitted through the single-entry point, as data breach notifications often include sensitive information[24].

6 EUROPEAN CYBERSECURITY SKILLS FRAMEWORK ('ECSF') (ARTICLE 19 CSA2)

27. Article 19 CSA2 Proposal would require that ENISA develops and makes publicly available a European Cybersecurity Skills framework ('ECSF'). The ECSF would help ensure that cybersecurity professionals, employers, training providers, and public authorities across Member States use a shared understanding of what specific cybersecurity jobs require. It would support clear job profiles, transparent qualification requirements, and a better alignment between education and labour market needs. ENISA would use the ECSF as a basis for delivering training, particularly to support the implementation of EU cybersecurity legislation, operational cooperation between Member States, and awareness-raising activities. This means the ECSF functions as a foundation for structured cybersecurity training programmes, especially for public authorities and entities covered by EU cybersecurity laws.

28. The EDPB and the EDPS welcome the objective of strengthening the EU Cybersecurity Workforce and underline that making skills more portable and recognisable across borders, is important for the functioning Digital Single Market.

[21] See Article 16(1) of Regulation (EU) 2024/2847 and COM(2025) 837 final, p.8.
[22] EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted on 10 February 2026.
[23] EDPB, The Helsinki Statement on enhanced clarity, support and engagement, A fundamental rights approach to innovation and competitiveness, adopted on 2 July 2025,.
[24] See Chapter 8.3. of the EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted on 10 February 2026.

29. At the same time, they notice that the profiles defined in Article 19(2) of the CSA2 Proposal are currently limited to cybersecurity professionals. The Proposal does not include a profile of necessary skills for citizens, civil servants, or non-specialised members of the workforce. As acknowledged in Recital 21 of the CSA2 Proposal, digital literacy is essential to empower resilient citizens, however, almost half the adult population does not have basic digital skills despite more than 90% of jobs requiring them. Therefore, the ECSF should include a "Cybersecurity for generalists" profile, which would cover the minimum skills that every EU resident of working age should possess to interact safely within the digital single market, protecting not only themselves but also their organisation and others, in particular from AI-assisted phishing, deepfakes, impersonation, and social engineering attacks. Such profile might be used by public or private organisations for the training of their staff to minimise their risks from the human factor, thereby reducing the overall risk of data breaches.

30. The EDPB and the EDPS note that Recital 45 of the Proposal explicitly distinguishes the ECSF from the European Digital Competence Framework (DigComp 3.0), clarifying that the latter is for daily life, participation in society, working and learning, and can be used by both adults and children[25], while the ECSF is for a specialised audience, offering a simple framework identifying cybersecurity roles and associated tasks, knowledge, and skills needed to perform them.

31. The EDPB and the EDPS support all the initiatives mentioned, be they executed by ENISA or, in the case of DigComp, the European Commission's Joint Research Centre (JRC), as they would, provided there is sufficient uptake, reduce the risk of data breaches. Therefore, they encourage all parties involved to explore ways to increase the frameworks' impact.

32. At the same time, the EDPB and the EDPS consider that DigComp does not replace a dedicated cybersecurity scheme for generalists[26] and recommends the co-legislators to amend Article 19(2) of the CSA2 Proposal so that the ECSF is not exclusively limited to 'cybersecurity professionals', but also includes profiles for the general workforce or citizens. This should be accompanied by a corresponding amendment to Recital 45.

33. In addition, the EDPB and the EDPS consider that it is necessary for the professional profiles of the ECSF to integrate a module on the need to ensure compliance of cybersecurity measures with EU data protection law, in particular regarding the practical implementation of the principle of data protection by design and by default (Article 25 GDPR), and invite the co-legislator to add a recital to this aim.

---

[25] The EDPB and the EDPS further recall that between 2022 and 2024, the European Commission explored the development of a European Digital Skills Certificate (EDSC), based on DigComp. The certificate would help people have their digital skills quickly and easily recognised by employers, training providers, and more. This initiative was meant to offer a quality label for digital skills certification across Europe. Following a feasibility study (see CENTENO, C., COSGROVE, J., CACHIA, R., MORA, T., DI LEGGE, A., VIVARELLI, S., BULIAN, G., MOYES PRELLEZO, N., PIÑA DE SANTISTEBAN, P., SCHULZ, C., HÜSING, T., CUARTAS-ACOSTA, A. and TROIA, S., European Digital Skills Certificate (EDSC) Feasibility Study, Publications Office of the European Union, Luxembourg, 2024, doi:10.2760/958195, JRC138344, https://publications.jrc.ec.europa.eu/repository/handle/JRC138344), and a pilot project with several EU countries, the European Commission concluded that such a quality label would not bring enough added value to European citizens. However, DigComp, first published in 2013, still exists (COSGROVE, J. and CACHIA, R., DigComp 3.0: European Digital Competence Framework - Fifth Edition, Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/0001149, JRC144121). It describes what is needed to be digitally competent in today's society, and supports the development of digital competence among individuals of all ages. It covers a wide range of skills levels, from basic to highly advanced. Several competences in DigComp refer explicitly to cybersecurity, such as 4.1 Protecting devices, 4.2 Protecting personal data and privacy and even 4.4 Protecting the environment (preventing data leakage from discarded equipment). Other areas also concern relevant skills, so contains area 1 skills crucial for defending against social engineering, reduces area 2 insider threat risks and prevents accidental information disclosure, and improves area 5 incident detection speed.

[26] In DigComp, the security content is diffused across 21 competences, it lacks explicit threat models, it does not operationalize organisational security risks, it does not map directly to compliance obligations. While the ECSF in its current form would apply to the skills of cybersecurity professionals, there is a lack of a structured EU-level framework for non-cybersecurity employees. The EDPB and the EDPS recall that most breaches originate from Phishing, social engineering, credential misuse, misconfiguration, and the use of "shadow IT". These are generalist behaviours. A generalist cybersecurity framework could make risks explicit, provide role-sensitive expectations (e.g. for human resources, finance), and support measurable outcomes.

7 EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK (TITLE III)

34. Articles 71 and 80(1)(w) CSA2 Proposal regulate the scope of the cybersecurity certification. Article 80(1)(w) adds, as a security objective for European cybersecurity certification schemes, 'to ensure that the entity is able to ensure the security of processing of personal data.'

35. The EDPB and the EDPS note that the wording of Article 80(1)(w) CSA2 Proposal is very close to the GDPR's requirements of security of processing[27]. In that sense, the scope of the new certification scheme could be interpreted as including requirements under the GDPR. However, the legal and operational scope is not entirely clear, as the provision does not cross-reference GDPR provisions (e.g. Article 5(1)(f), Article 32, Article 25 GDPR) and it is placed inside a list of "security objectives" (Article 80 (1), first sentence).

36. The EDPB and EDPS recall that security under the GDPR relates to risks for the fundamental rights and freedoms of individuals. While the legal definition of cybersecurity under Union law broadly includes the protection of users and other persons[28], the scope of cybersecurity measures typically encompasses risks of all kinds for the organisation concerned. Still there is opportunity to establish synergies so that the risk assessment can integrate the protection of the rights and freedoms of individuals.

37. The EDPB and EDPS further recall that the GDPR has its own certification mechanism (Articles 42-43 GDPR), and they consider that cybersecurity certification is distinct from data protection certification pursuant to Article 42 GDPR.

38. That being said, the EDPB and EDPS consider that there may be synergies between cybersecurity and data protection certification. For example, the CSA2 certification could be used as supporting evidence to demonstrate that some requirements in a GDPR certification are met, as far as cybersecurity is concerned. However, the EDPB and the EDPS note that Article 80(1)(w) CSA2 Proposal does not clearly articulate the relationship with Article 42-43 GDPR certification. In the interest of legal certainty, the EDPB and EDPS recommend further clarifying the scope of Article 80(1)(w) CSA2 and the relationship to GDPR certification. In addition, the EDPB and the EDPS recommend requiring ENISA to consult with the EDPB prior to adopting a certification scheme under Article 80(1)(w) CSA2, to ensure consistency.

39. The EDPB and the EDPS highlight the need to consider not only the effectiveness of cybersecurity measures, but also their necessity and proportionality. Certain cybersecurity controls create specific data protection risks. This can be the case with monitoring and logging, deep packet inspection, or user behaviour analytics. A well-designed certification scheme for security of processing could include controls to ensure that security measures can be implemented in a way that complies with data protection rules (e.g. certain aspects should be configurable; this could be the case, for instance, of the granularity of data that is logged for security purposes -- as this can enable or facilitate the controller's compliance with the security and data minimisation principles in the GDPR; in the same vein, storage periods should be configurable so that the controller can decide, in the context of the processing they are implementing, how long the personal data should be kept before being deleted or anonymised using certified techniques).

---

[27] See Article 5(1)(f) and Article 32 GDPR.

[28] See Article 2(1) of the CSA2 Proposal, which is a legacy provision and reads: 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.

40. Therefore, the EDPB and the EDPS recommend explaining in a recital that certification schemes should, to the extent possible, be designed, implemented and maintained in a way that take into account security controls that can help to demonstrate the fulfilment of GDPR requirements, where the schemes apply to ICT products, ICT services, ICT processes and managed security services that are likely to be used in data processing operations. It should also be noted that some controls can be enablers for privacy and data protection by design and by default.

8 TRUSTED ICT SUPPLY CHAIN FRAMEWORK (TITLE IV)

41. The CSA2 Proposal adds measures for the Security of ICT Supply Chains, addressing in particular non-technical risks such as geopolitical, legal, ownership, dependency and strategic interference factors affecting ICT supply chains in sectors of high criticality and other critical sectors. While such supply chain security measures aim primarily to address risks which are not directly related to data protection, they may also have a beneficial impact on the protection of fundamental rights by limiting the foreign interference with the data of EU data subjects through activities such as espionage and surveillance.

42. The EDPB and the EDPS welcome the proposed measure aimed at ensuring a trusted ICT supply chain framework and addressing non-technical risks in sectors of high criticality.

9 ADDITIONAL ESSENTIAL ENTITIES UNDER THE NIS2 PROPOSAL

43. The Proposal amending the NIS2 Directive would include European Digital Identity Wallets and European Business Wallets providers, as 'essential entities', regardless of size. Entities classified as ‘essential’ are subject to full NIS2 cybersecurity risk-management obligations and must implement the security measures required under Article 21 NIS2, including risk analysis and security policies, incident handling, business continuity and crisis management, supply chain security, vulnerability handling, policies on cryptography and encryption, and access control and asset management.

44. The EDPB and the EDPS welcome the designation of European Digital Identity Wallets and European Business Wallets providers as 'essential entities'. The EDPB and the EDPS consider that Digital identity wallets are a core component of the EU digital infrastructure, so that incidents affecting them could have broad cross-border impact. They underpin secure identification, authentication, and electronic attestations. For the digital economy, business wallets are equally critical as European Digital Identity Wallets. Consequently, both types of Wallet providers are treated similarly to trust service providers, which have already been designated as ‘essential entities’ under NIS2, and other highly critical infrastructure operators.

10 COLLECTION OF DATA ON RANSOMWARE ATTACKS

45. According to Article 5 (8) NIS2 amendments Proposal, proposing to add new paragraphs 12 and 13 to Article 23 NIS2, in case of a ransomware attack, the entities concerned may be requested to submit certain information regarding ransomware incidents to Computer Security Incident Response Teams (CSIRTs), including whether an entity has paid a ransom, and if so, what amount and to whom (crypto-assets/service providers) and the identity of the person acting as the point of contact.

46. Pursuant to Article 23(11) NIS2, the Commission is empowered to adopt implementing acts further specifying the type of information, the format and the procedure of the reporting obligations. The scope of this implementing act would be extended to cover also the new reporting obligations in case of ransomware attacks.

47. The EDPB and the EDPS fully support the important objective of preventing future ransomware attacks and disrupting and dismantling the criminal organisations behind them. The EDPB and the EDPS note that the information to be shared regarding ransomware attacks could be of potentially sensitive nature as further explained by the Commission in Recital 10 of the NIS2 amendments Proposal. Moreover, such reporting may entail processing of personal data. The EDPB and the EDPS welcome the tiered approach chosen in paragraphs 12 and 13, where the more sensitive information in paragraph 13 will only be reported upon request.

48. At the same time, in view of the sensitivity of the reported data and in line with the principles of necessity and proportionality, in case the reporting of ransomware attacks would involve processing of personal data, the EDPB and the EDPS recommend specifying in the implementing act pursuant to Article 23(11) NIS2 Directive the applicable data protection safeguards. In this regard, they also recall the requirement for the Commission pursuant to Article 42(1) EUDPR to consult the EDPS on the draft implementing and delegated acts where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.