Council of the European Union
General Secretariat

Brussels, 10 February 2025

WK 1722/2025 INIT

LIMITE

DATAPROTECT
JAI
CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Delegations
Subject:	Discussion paper regarding the single entry point for notifications and relation between the GDPR and the NIS2 Directive

In view of the joint discussion between delegates of the Working Party on Data Protection and of the Horizontal Working Party for Cyber Issues on 19 February 2025, delegations will find in the Annex a discussion paper regarding the single entry point for notifications and relation between the GDPR and the NIS2 Directive.

Discussion paper
for the meeting of Working Party on Data Protection and Horizontal Working Party for Cyber Issues on the 19 February 2025 regarding the single entry point for notifications and relation between the GDPR and the NIS2

The EU legislation introduces a complex reporting framework, which poses challenges to both the authorities responsible for oversight and the businesses which have to navigate through a dense web of compliance requirements.

Concerns are being voiced by business associations which indicate mounting compliance costs, burdensome reporting requirements and increasing fragmentation of the Single Market[1]. In a joint statement with Accountancy Europe of 13 February 2024, they highlight the lack of harmonisation in security requirements as a key issue that must be addressed. An **additional challenge**, mentioned in a report of the European Cybersecurity Organisation[2], **is the need to report cybersecurity incidents to multiple authorities**, such as those under NIS2, CRA and GDPR, as well as sectoral ones, such as those under DORA and other related fields, such as CER. It is a challenge for experienced players and even more so for SMEs, who are not sufficiently prepared for the cybersecurity challenges and who have less means to respond to the increasing obligations.

The reporting obligations are essential to ensure transparency, enable swift responses to security and data breaches and to strengthen the resilience of digital infrastructure. Therefore, there is a need to seek solutions to the challenges encountered at implementation, through streamlining these obligations. Digitalisation can play a substantial role in this respect.

Recital 106 of the NIS2 states that "*In order to simplify the reporting of information required under this Directive as well as to decrease the administrative burden for entities, Member States should provide technical means such as a single entry point, automated systems, online forms, user-friendly interfaces, templates, dedicated platforms for the use of entities, regardless of whether they fall within the scope of this Directive, for the submission of the relevant information to be reported. Union funding supporting the implementation of this Directive, in particular within the Digital Europe programme, established by Regulation (EU) 2021/694 of the European Parliament and of the Council, could include support for single entry points. Furthermore, entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional administrative burden and could also lead to uncertainties with regard to the format and procedures of such notifications. Where a single entry point is established, Member States are encouraged also to use that single entry point for notifications of security incidents required under other Union law, such as Regulation (EU) 2016/679 and Directive 2002/58/EC. The use of such single entry point for reporting of security incidents under Regulation (EU) 2016/679 and Directive 2002/58/EC should not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to the independence of the authorities referred to therein. ENISA, in cooperation with the Cooperation Group, should develop common notification templates by means of guidelines to simplify and streamline the information to be reported under Union law and decrease the administrative burden on notifying entities*."

[1] Available at https://accountancyeurope.eu/news/european-business-calls-for-deepening-the-eu-single-market-and-renewing-the-dynamic-of-european-integration/

[2] ECSO Report, "Streamlining Regulatory Obligations of EU Cybersecurity Policies", published on 16 January 2025, published https://ecs-org.eu/?publications=streamlining-regulatory-obligations

A similar idea of establishing a single entry point for vulnerabilities notifications was present in the recitals of the Cyber Resilience Act (recital (72)).

Some Member States link this approach also to the reporting obligation stemming from the GDPR. Providing a single reporting platform for the reporting under the GDPR and cyber legislation could send a clear message that the obligations stemming from the EU legislation can be navigated in a business-friendly way. **The idea of a single entry point for notifications** seems to **have the potential to substantially reduce the administrative burden imposed on enterprises and institutions**.

Article 31(3) NIS2 states that the competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.

Recital 121 clarifies the application of the relevant legal bases of Article 6 GDPR to personal data processing activities for the purpose of ensuring security of network and information systems falling within the scope of NIS2 Directive.

Article 35 NIS2 further provides for the handling of infringements entailing a personal data breach, thereby providing for the cooperation of competent authorities under the NIS2 with the supervisory data protection authorities and for administrative fines.

The Polish Presidency would like to invite the Working Party on Data Protection and the Horizontal Working Party for Cyber Issues to exchange views **on the basis of the following guiding questions:**

1. **Do you consider the notion of a single entry point for notifications as an idea to simplify the application of the related obligations under the GDPR and cyber legislation? Are you implementing or planning to implement a single entry point at national level? What type of reporting obligations are you including or planning to include in the single entry?**
2. **What challenges do you see to make a single entry point for notifications feasible? Please share your national experiences and best practises. Would you see a need for action at EU level? If yes, what kind?**
3. **How is the cooperation between competent authorities under the NIS2 and the GDPR ensured at national level? Please share best practices and challenges.**
4. **Do you consider the existing legal framework sufficient to ensure the necessary exchange of relevant cybersecurity information (e.g. information about incidents and vulnerabilities) between relevant entities (such as CSIRTs, law enforcement, supervisory authorities)? Do you encounter any challenges with personal data protection rules while implementing and enforcing the NIS2?**