DENTONS

# Cyber security information sharing under the new EU regulations

Grow | **Protect** | Operate | Finance

**October 2023**

# Introduction

The following is a summary of eighteen (18) cases in which – according to the provisions of the *NIS 2 Directive** and the *DORA Regulation*** – the exchange of information on incidents and cyber threats, as well as other information related to cyber security, should take place. We have divided the above cases into 5 (five) categories, namely:

1. Sharing of information within the sector;
2. Reporting obligations;
3. Informing customers, internal employees, contractors and the public;
4. Sharing information at the inter-country level and between authorities from different countries.
5. Feedback from authorities.

The above cases apply to all entities covered by (a) national regulations of EU member states that are required to implement NIS 2 Directive by October 17, 2024 (cases marked as "NIS2") or (b) the DORA regulation to be applied as of January 17, 2025 (cases marked as "DORA"). Significantly, both of the above regulations went into effect on January 16 of this year (for more information, **please see our webinar – details on Dentons' website).**

The cases mentioned in the summary below are significant in that **there is growing attention to the fact that affected entities are not sharing information on how to detect, prevent and manage cyber incidents.** This is despite the fact that very often these incidents are massive and come from the same source or were caused by the same malware.

**However, after reviewing the summary below, one can conclude that, with a few exceptions (such as joining intra-sector ISA(s)), the phenomenon of lack of information sharing will continue.** This is due to a number of limitations related to the confidentiality of potentially shared information, for example, because of the damage it can cause if it falls into the wrong hands, or because of its market value or competitive constraints, as well as safeguards against possible claims from customers or other counterparties. For this reason, guidelines in best practices, norms and standards that recommend sharing information on how a threat was handled (e.g. *Computer Security Incident Handling Guide NIST SP 800-61*) for example, will not be fully implemented.

**Since we are dealing with new regulations we encourage sharing all comments with Paweł Gruszecki: pawel.gruszecki@dentons.com.**

* 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) – (Official Journal of the European Union, L333/80, 27.12.2022).

** Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022).

# 1. Sharing of information within the sector

**Article 45(1) – (3) of the DORA regulation**

**Voluntary***

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:<br>• Aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;<br>• Takes places within trusted communities of financial entities;<br>• Is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data in accordance with Regulation (EU) 2016/679 and guidelines on competition policy. | Financial entity regulated by the DORA that has entered into the information-sharing arrangement(s) (ISA(s)) within the trusted communities of financial entities.<br>To some extent public authorities and ICT service providers might be involved in the application of the information-sharing arrangements (ISAs). | Financial entity regulated by the DORA that has entered into the information-sharing arrangement(s) (ISA(s)) within the trusted communities of financial entities.<br>To some extent public authorities and ICT service providers might be involved in the application of the information-sharing arrangements (ISAs). |

***Financial entities should be encouraged to exchange among themselves cyber threat information and intelligence, and to collectively leverage their individual knowledge and practical experience at the strategic, tactical and operational levels with a view to enhancing their capabilities to adequately assess, monitor, defend against, and respond to cyber threats, by participating in information sharing arrangements.**

— Motive 32 of the Preamble to the Dora Regulation.

# 2. Reporting obligations

**Article 23(1) and (4) of the NIS2 Directive**

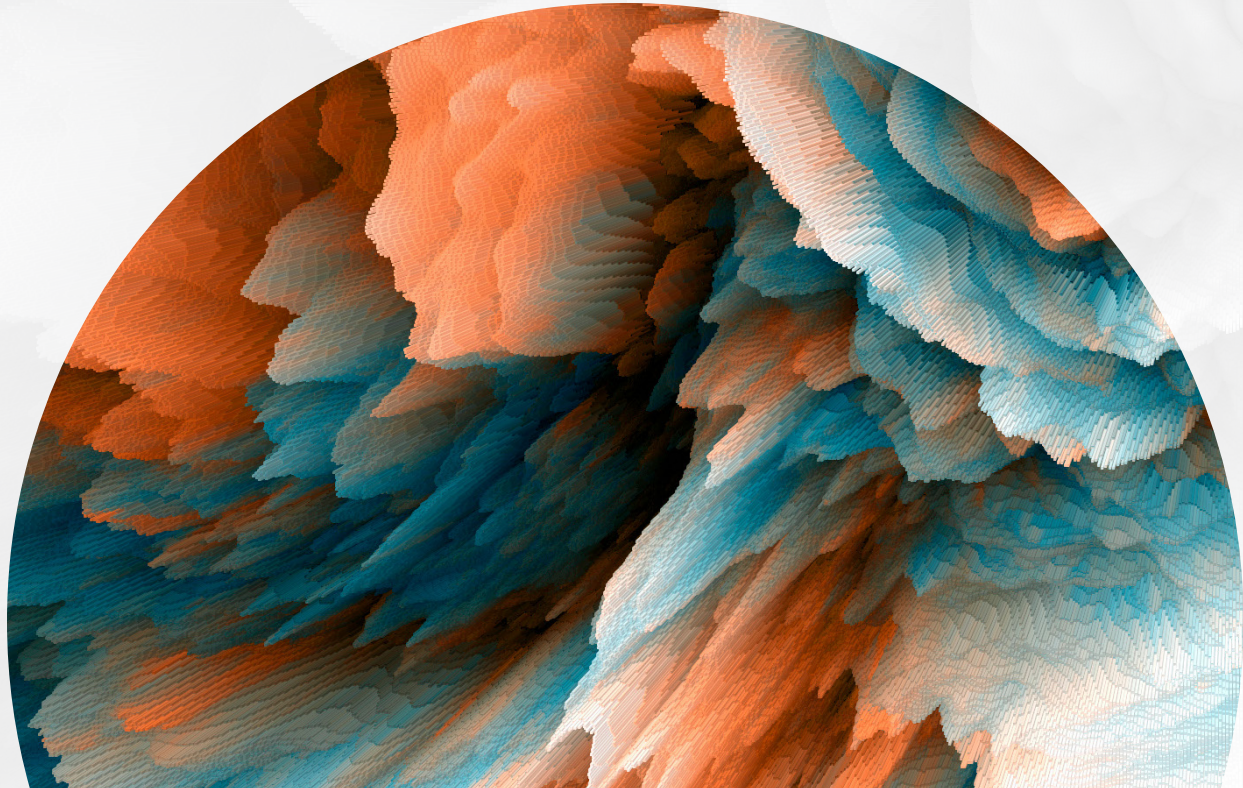
**Mandatory**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| **1.** Without undue delay and in any event within 24 hours of becoming aware of the significant incident*, an **early warning**, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact.<br><br>**2.** Without undue delay and in any event within 72 hours of becoming aware of the significant incident, an **incident notification**, which, where applicable, shall update the information referred to in point 1 above and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;<br><br>A trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify, without undue delay and in any event within 24 hours of becoming aware of the significant incident.<br><br>**3.** Upon the request of a CSIRT or, where applicable, the competent authority, **an intermediate report** on relevant status updates;<br><br>**4.** A **final report** not later than one month after the submission of the incident notification under point (b), including the following: (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; (iv) where applicable, the cross-border impact of the incident.<br><br>**5.** In the event of an **ongoing incident** at the time of the submission of the final report referred to in point 4 above, a progress report and a final report within one month of handling of the incident. | Essential and important entities within the meaning of the NIS 2 Directive which are affected by the significant incident | CSIRT or, where applicable, the competent authority (competent authority forwards the notification to the CSIRT upon receipt)<br><br>In the case of a cross-border or cross-sectoral significant incident, single points of contact are provided in due time with relevant information notified. |

**Article 30 of the NIS2 Directive**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Essential and important entities with regard to incidents, cyber threats and near misses. Entities other than those referred to above, regardless of whether they fall within the scope of the NIS2 Directive, with regard to significant incidents, cyber threats and near misses | Essential and important entities with regard to incidents, cyber threats and near misses. Entities other than those referred to above, regardless of whether they fall within the scope of the NIS2 Directive, with regard to significant incidents, cyber threats and near misses | CSIRTs or, where applicable, the competent authorities (where necessary, the CSIRTs and, where applicable, the competent authorities shall provide the single points of contact with the information about notifications received pursuant to this point) |

**Voluntary**



**Articles 19(1), (4), 20, and 46 of the DORA regulation.**

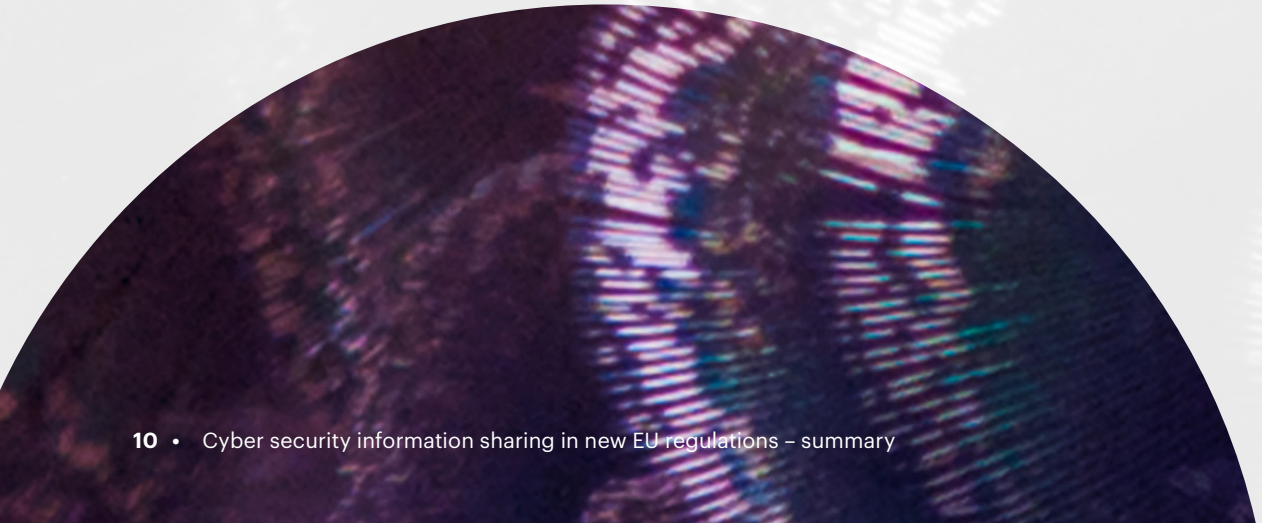
**Mandatory**

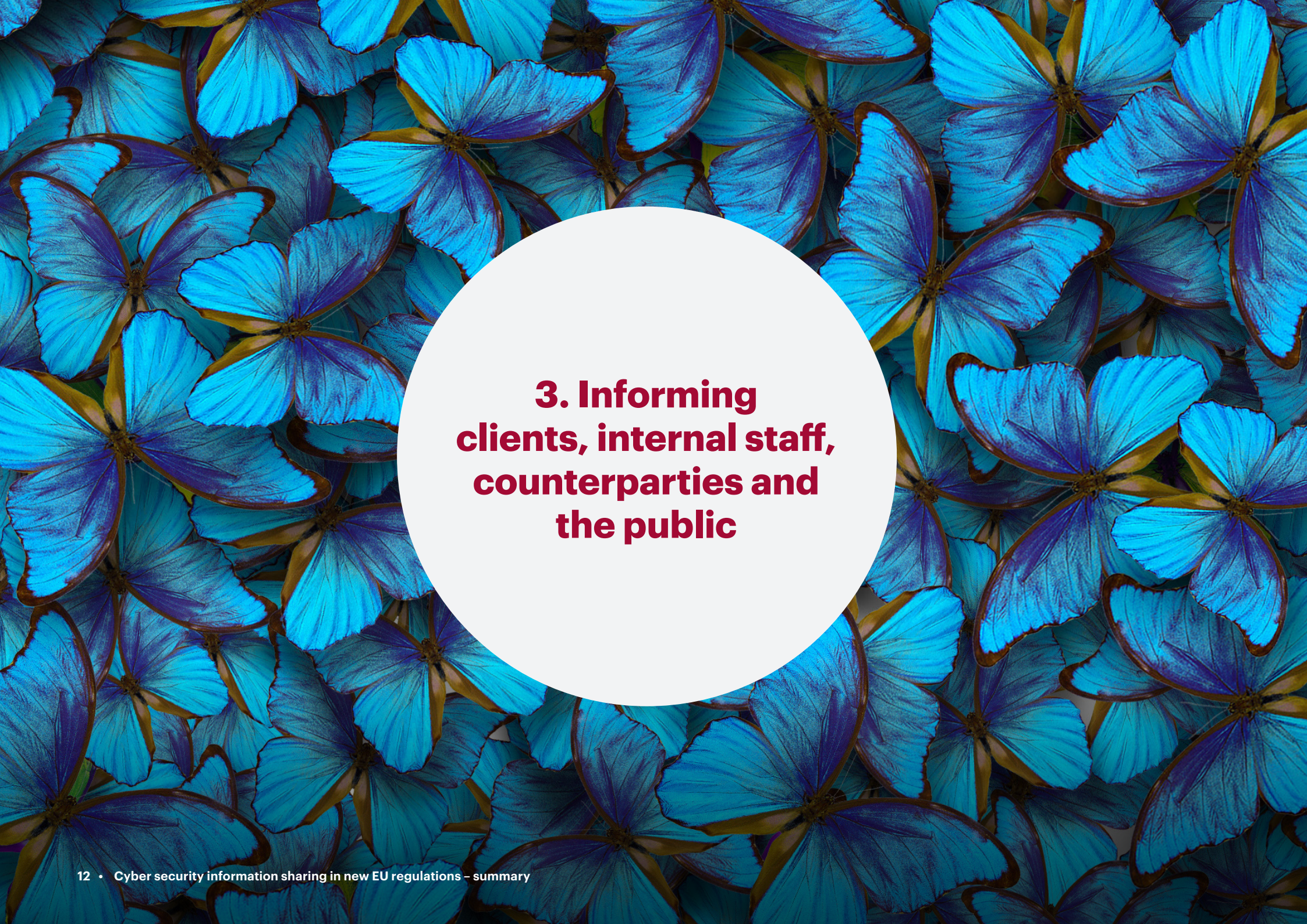
| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| The initial notification and reports referred to in paragraph 4 of the Article 19 of the DORA using the templates referred to in Article 20 of the DORA i.e.<br>• An initial notification;<br>• An intermediate report after the initial notification referred to in point above, as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;<br>• A final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.<br>The initial notification and reports referred to in paragraph 4 of the Article 19 of the DORA shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts. | Financial entity regulated by the DORA | The relevant competent authority as referred to in Article 46 of the DORA in accordance with paragraph 4 of Article 19 of the DORA**/***<br>Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall report major ICT-related incidents to the relevant national competent authority designated in accordance with Article 4 of Directive 2013/36/EU, which shall immediately transmit that report to the ECB. |

**Articles 19 (2) of the DORA regulation.**

**Voluntary**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Significant cyber threats (when the threat will be deemed to be of relevance to the financial system, service users or clients). | Financial entity regulated by the DORA | The relevant competent authority (as referred to in Article 46 of the DORA in accordance with paragraph 4 of Article 19 of the DORA) which may provide such information to other relevant authorities referred to in paragraph 6 of Article 19 of the DORA.**** |
| | | Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, may, on a voluntary basis, notify significant cyber threats to the relevant national competent authority, designated in accordance with Article 4 of Directive 2013/36/EU, which shall immediately transmit the notification to the ECB. |





# 3. Informing clients, internal staff, counterparties and the public

**Article 23(1) and (2) of the NIS2 Directive**

**Mandatory**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Without undue delay information about any measures or remedies that recipients of the services are able to take in response to the threat.<br><br>Where appropriate, information about a significant cyber threat itself | Essential and important entities within the meaning of the NIS 2 Directive which are affected by the significant incident | Recipients of services provided by the essential and important entities (within the meaning of the NIS 2 Directive) that are potentially affected by a significant cyber threat |

**Article 23(7) of the NIS2 Directive**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Information that the significant incident took place | A Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, after consulting the entity concerned (i.e. the entity regulated by the local law implementing the NIS 2 Directive) | The public |

**Voluntary***

***Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of a significant incident is otherwise in the public interest.**

**Article 23(7) of the NIS2 Directive**

**Mandatory**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Information that the significant incident took place | The entity concerned (i.e. essential and important entities within the meaning of the NIS 2 Directive which are affected by the significant incident.) which was required to do so by a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned | The public |

**Article 14(1) – (3) of the DORA regulation**

**Having plans and policies is mandatory**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| The following plans and policies should be implemented (as part of the ICT risk management framework referred to in Article 6(1) of the DORA):<br>• A crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities as well as<br>• Communication policies for internal staff and for external stakeholders.<br>Communication policies for staff shall take into account the need to differentiate between staff involved in ICT risk management, in particular the staff responsible for response and recovery, and staff that needs to be informed. | Financial entity regulated by the DORA | Clients, internal staff and counterparts as well as to the public, as appropriate |

**Article 19(3) of the DORA regulation**

**Mandatory**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Information about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such an incident (where a major ICT-related incident occurs and has an impact on the financial interests of clients, without undue delay as soon as they become aware of it) | Financial entity regulated by the DORA | Clients |

**Article 19(3) of the DORA regulation**

**Mandatory (where applicable)**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| In the case of a significant cyber threat – information that clients are potentially affected on any appropriate protection measures which the latter may consider taking | Financial entity regulated by the DORA | Clients |

# 4. Sharing of information at inter-country level and between authorities from different countries

**Article 23(6) of the NIS2 Directive**

**Mandatory***

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| The type of information received by the CSIRT, the competent authority or the single point of contact in accordance with **Article 23(4) of the NIS2 Directive**.<br><br>In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with EU or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided. | The CSIRT, the competent authority or the single point of contact | The other affected Member States and ENISA |

***Where appropriate, and in particular where the significant incident concerns two or more Member States.**

**Article 23 (9) of the NIS2 Directive**

**Mandatory**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| A summary report **(every 3 months)**, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified pursuant to with Article 23 (1) and Article 30 of the NIS2 Directive | The single point of contact | ENISA (in order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report). ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications received **every 6 months** |

**Article 23 (10) of the NIS2 Directive**

**Mandatory**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Information about significant incidents, incidents, cyber threats and near misses notified pursuant to Article 23 (1) and with Article 30 of the NIS2 Directive by entities identified as critical entities under Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance - OJ L 333, 27.12.2022, p. 164–198) | The CSIRTs or, where applicable, the competent authorities | The competent authorities under Directive (EU) 2022/2557 |

**Article 19 (6) of the DORA regulation**

**Mandatory (where applicable)**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Details of the major ICT-related incident (upon receipt of the initial notification and of each report referred to in Article 19 paragraph 4 of the DORA and in a timely manner) | The competent authority | Based, as applicable, on their respective competences<br>• EBA, ESMA or EIOPA;<br>• The ECB, in the case of financial entities referred to in Article 2(1), points (a), (b) and (d) of the DORA<br>• The competent authorities, single points of contact or CSIRTs designated or established in accordance with Directive (EU) 2022/2555;<br>• The resolution authorities, as referred to in Article 3 of Directive 2014/59/EU, and the Single Resolution Board (SRB) with respect to entities referred to in Article 7(2) of Regulation (EU) No 806/2014 of the European Parliament and of the Council (37), and with respect to entities and groups referred to in Article 7(4)(b) and (5) of Regulation (EU) No 806/2014 if such details concern incidents that pose a risk to ensuring critical functions within the meaning of Article 2(1), point (35), of Directive 2014/59/EU; and<br>• Other relevant public authorities under national law |

**Article 19 (7) of the DORA regulation**

**Mandatory (where applicable)**

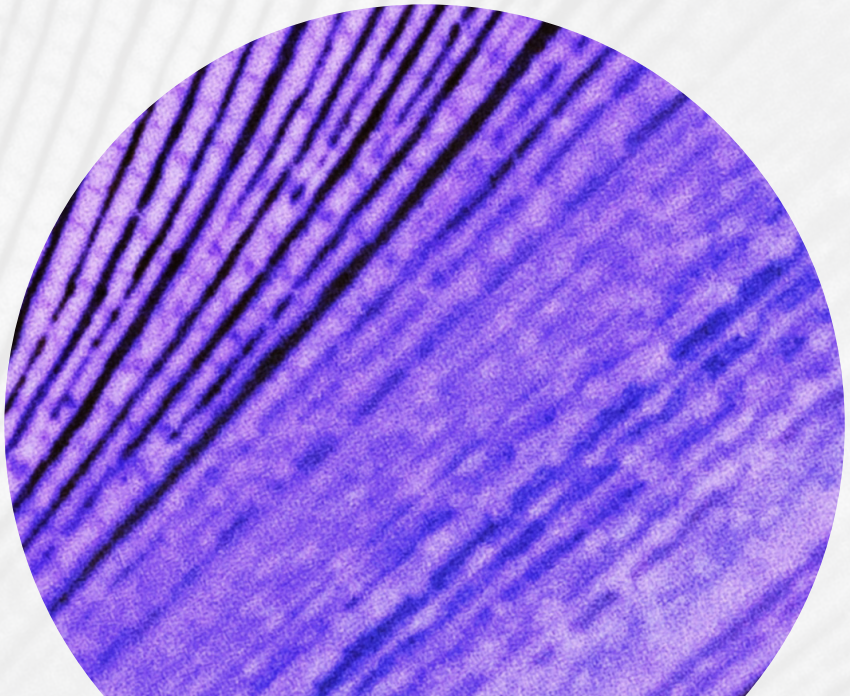
| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Information and reports specified in Article 19(6) of the DORA (as soon as possible following the assessment of whether the major ICT-related incident is relevant for competent authorities in other Member States) | EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority | Relevant competent authorities in other Member States accordingly (informed by EBA, ESMA or EIOPA).<br><br>Members of the European System of Central Banks on issues relevant to the payment system (informed by the ECB) |

# 5. Feedback from authorities

**Article 22 (1) of the DORA regulation**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| Timely manner relevant and proportionate feedback or high-level guidance, in particular by making available any relevant anonymised information and intelligence on similar threats (including discussing remedies applied at the level of the financial entity and ways to minimise and mitigate adverse impact across the financial sector). | Competent authority | Financial entity regulated by the DORA. |

**Voluntary**



**Article 23 (5) of the NIS2 Directive**

**Mandatory**

| Scope and condition of information provision | Who shares information | Who receives information |
|---|---|---|
| A response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. The CSIRT shall provide additional technical support if the entity concerned so requests. Where a significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also provide guidance on reporting that significant incident to the law enforcement authorities. | The CSIRT or the competent authority (without undue delay and where possible within 24 hours of receiving the early warning referred to in Article 23 paragraph 4, point (a) of the NIS2 Directive. Where the CSIRT is not the initial recipient of the notification, the guidance shall be provided by the competent authority in cooperation with the CSIRT. | The notifying entity |

## References contained within the document

* An incident shall be considered to be significant if: (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage .

** Where a financial entity is subject to supervision by more than one national competent authority referred to in Article 46 of the DORA, Member States shall designate a single competent authority as the relevant competent authority responsible for carrying out the functions and duties provided for in Article 19 of the DORA.

*** The EU Member States may additionally determine that some or all financial entities shall also provide the initial notification and each report referred to in paragraph 4 of this Article using the templates referred to in Article 20 to the competent authorities or the computer security incident response teams (CSIRTs) designated or established in accordance with Directive (EU) 2022/2555.

**** The EU Member States may determine that those financial entities, that on a voluntary basis notify in accordance with the first subparagraph, may also transmit that notification to the CSIRTs designated or established in accordance with Directive (EU) 2022/2555.

# Core team members

**Karol Laskowski**
Partner
D +48 22 242 51 27
karol.laskowski@dentons.com

**Paweł Gruszecki**
Counsel
D +48 22 242 56 13
pawel.gruszecki@dentons.com

## ABOUT DENTONS

Across over 80 countries, Dentons helps you grow, protect, operate and finance your organization by providing uniquely global and deeply local legal solutions. Polycentric, purpose-driven and committed to inclusion, diversity, equity and sustainability, we focus on what matters most to you.

**www.dentons.com**



CSBrand-126856-A4-Landscape-Brochure-Cyber-Security-08 — 03/11/2023