JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

ANNEX IV

Data glossary and instructions for notification of significant cyber threats

Data field	Description	Instructions	Mandatory field	Field type
1. Name of the entity submitting the notification	Full legal name of the entity submitting the notification		Yes	Alphanumeric
2. LEI of the entity submitting the notification	Legal Entity Identifier (LEI) of the entity submitting the notification assigned in accordance with the International Organisation for Standardisation. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.		Yes	Alphanumeric
3. Type of the entity submitting the report	Type of the entity under Article 2.1(a)-(t) of DORA submitting the report	To be provided only where the report is not provided by the affected financial entity directly.	Yes, if appliable	Choice (multiselect) from the pre-defined list of DORA financial entities. 'Other' for entities not listed in Article 2.1 of DORA
4. Name of the financial entity	Full legal name of the financial entity notifying the significant cyber threat.	Field mandatory if the financial entity is different from the entity submitting the notification.	Yes, if appliable	Alphanumeric
5. Type of financial entity	Type of the financial entity under Article 2.1(a)-(t) of DORA notifying the significant cyber threat.	Field mandatory if the financial entity affected by the incident is different from the entity submitting the notification.	Yes, if appliable	Choice (multiselect): Article 2.1 points (a) to (t) of DORA Regulation

Data field	Description	Instructions	Mandatory field	Field type
6. LEI code of the financial entity	Legal Entity Identifier (LEI) of the financial entity notifying the significant cyber threat, assigned in accordance with the International Organisation for Standardisation. This is a unique 20 alphanumeric character code, based on ISO 17442-1:2020.	Field mandatory if the financial entity notifying the significant cyber threat is different from the entity submitting the report.	Yes, if appliable	Alphanumeric
7. Primary contact person name	Name and surname of the primary contact person of the financial entity		Yes	Alphanumeric
8. Primary contact person email	Email address of the primary contact person that can be used by the competent authority for follow-up communication		Yes	Alphanumeric (email format)
9. Primary contact person telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication		Yes	Number (telephone format)
10. Second contact person name	Name and surname of the second contact person of the financial entity or an entity submitting the notification on behalf of the financial entity		Yes	Alphanumeric
11. Secondary contact person email	Email address of the second contact person or a functional email address of the team that can be used by the competent authority for follow-up communication		Yes	Alphanumeric (email format)
12. Second contact person telephone	Telephone number of the second contact person that can be used by the competent authority for follow-up communication		Yes	Number (telephone format)

Data field	Description	Instructions	Mandatory field	Field type
13. Date and time of detection of the cyber threat	Date and time at which the significant cyber threat was detected.		Yes	dd/mm/yyyy hh:mm
14. Description of the significant cyber threat	Description of the most relevant aspects of the significant cyber threat.	Financial entities shall provide: - a high-level overview of the most relevant aspects of the significant cyber threat; - the related risks arising from it, including potential vulnerabilities of the systems of the financial entity that can be exploited; - information about the probability of materialisation of the significant cyber threat; and - information about the probability of materialisation of the significant cyber threat.	Yes	Alphanumeric
15. Information about potential impact	Information about the potential impact of the cyber threat on the financial entity, its clients and/or financial counterparts if the cyber threat has materialised		Yes	Alphanumeric
16. Potential incident classification criteria	The classification criteria that could have triggered a major incident report if the cyber threat had materisalised.		Yes	Choice (multiple): (to be aligned with the RTS on classification of major incidents

Data field	Description	Instructions	Mandatory field	Field type
17. Status of the cyber threat	Information about the status of the cyber threat and whether there has been any changes in the threat activity.		Yes	Choice: a) active b) inactive
18. Actions taken to prevent materialisation	Information about the actions taken by the financial entity to prevent the materialisation of the significant cyber threats, if applicable.		Yes	Alphanumeric
19. Notification to other stakeholders	Information about notification of the cyber threat to other financial entities or authorities		Yes, if applicable	Alphanumeric
20. Indicators of compromise	Information related to the significant threat that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable.	The IoC provided by the financial entity may include, but not be limited to, the following categories of data: • IP addresses; • URL addresses; • Domains; • File hashes; • Malware data (malware name, file names and their locations, specific registry keys associated with malware activity); • Network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); • E-mail message data (sender, recipient, subject, header, content); • DNS requests and registry configurations;	Yes, if applicable	Alphanumeric

Data field	Description	Instructions	Mandatory field	Field type
		• User account activities (logins, privileged user account activity, privilege escalation); • Database traffic (read/write), requests to the same file. In practice, this type of information may include data relating to, for example, indicators describing patterns in network traffic corresponding to known attacks/botnet communications, IP addresses of machines infected with malware (bots), data relating to "command and control" servers used by malware (usually domains or IP addresses), URLs relating to phishing sites or websites observed hosting malware or exploit kits, etc.		
21. Other relevant information	Any other relevant information about the significant cyber threat		Yes, if applicable	Alphanumeric