Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Project „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ (Project Nr. 02-002-P-0001) report

Project name: ***CTI-balanced***

Responsible/Implementation partner (-s): ***MRU***

Action result: ***CTI-balanced Assessment Model***

Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Editor
Evaldas Bružė (MRU)

Contributors
Evaldas Bruze (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)

Reviewers
Evaldas Bružė (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)

1. Introduction & Methodology

This document provides a structured methodology for assessing the data protection, cybersecurity-governance and regulatory implications of the CTI-balanced system. CTI-balanced is a cyber threat intelligence sharing platform that enables the collection, enrichment and sharing of cyber threat intelligence between different entities, including financial institutions and essential or important entities within the meaning of the NIS2 Directive. The system supports the exchange of information about cyber threats in line with the objectives of NIS2 and the Digital Operational Resilience Act. It does not use artificial intelligence; therefore, the assessment focuses on GDPR, NIS2 and DORA rather than AI-specific regulatory obligations.

The deliverable consists of two complementary instruments: a general questionnaire and the Data Protection Impact Assessment template of the Lithuanian State Data Protection Inspectorate. The questionnaire is intended to collect and structure the factual, legal and organisational information needed to assess the planned deployment of the CTI-balanced platform. The DPIA template is included as the formal instrument to be used where the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons.

The inclusion of a DPIA template is justified because CTI sharing may involve information that is technical in nature but still capable of relating to an identified or identifiable natural person. Depending on the concrete deployment, cyber threat intelligence may include IP addresses, user identifiers, email addresses and other personal data within the meaning of the GDPR. The assessment should therefore not assume that CTI is automatically anonymous or outside the scope of the GDPR. Instead, the methodology requires the deploying organisation to determine whether the information processed by the platform constitutes personal data, whether any data has been anonymised or pseudonymised and whether the sharing of such data is necessary and proportionate for the cybersecurity objective pursued.

The questionnaire is broader than a DPIA form. It is intended to support both data protection analysis and cybersecurity-governance assessment. Some questions correspond directly to DPIA requirements, including the description of processing operations, data categories and others. Other questions address the specific governance of CTI sharing, including trusted-community rules, participant vetting and others. This broader structure is important because CTI sharing requires not only legal compliance, but also operational trust, information quality and controlled dissemination.

The DPIA should be completed only on the basis of a concrete deployment. At project level, it is possible to describe the platform architecture, intended data flows and general safeguards, but it is not possible to determine all deployment-specific facts. The final answers depend on the participating entities, the types of CTI exchanged, the sectors involved, the applicable national implementation of NIS2 and other relevant factors. For this reason, the questionnaire and DPIA template should not be pre-filled as if there were one universal deployment scenario. They provide the assessment structure, while the substantive answers must be completed by the organisation or consortium responsible for the actual deployment.

For GDPR purposes, the assessment should focus on whether the CTI-balanced platform processes personal data, the role of each participating entity, the legal basis for collection, enrichment and sharing, and the safeguards applied to avoid unnecessary disclosure of identifiable information. Particular attention should be paid to data minimisation and purpose limitation. The platform should support the sharing of information necessary for cybersecurity purposes but should avoid including personal data where technical indicators or sufficiently anonymised information would be adequate.

For NIS2 purposes, the platform should be assessed as a mechanism supporting cybersecurity risk management and information sharing between relevant entities. NIS2 specifically recognises cybersecurity information-sharing arrangements and refers to the exchange of relevant cybersecurity information, including information relating to cyber threats, near misses, vulnerabilities and other threat-related matters. The methodology should therefore assess whether the CTI-balanced platform provides a structured, secure and accountable environment for such exchanges.

For DORA purposes, the assessment is particularly relevant where financial entities participate in or rely on the CTI-balanced platform. DORA provides that financial entities may exchange cyber threat information and intelligence, where the sharing aims to enhance digital operational resilience, takes place within trusted

communities and is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared. The methodology should therefore assess whether the platform supports trusted-community governance, secure exchange, confidentiality, personal data protection, business secrecy, and clear rules on participation, access and onward dissemination.

Because the CTI-balanced system does not use artificial intelligence, the AI Act is not treated as a core assessment framework in this deliverable. However, this conclusion should be revisited if the platform is later modified to include automated functions based on machine learning or other AI techniques.

In conclusion, the methodology used in this document treats CTI-balanced as a cybersecurity information-sharing platform whose compliance profile depends on the data exchanged, the entities involved and the regulatory context of the deployment. The general questionnaire supports structured collection of information and governance evidence, while the SDPI DPIA template supports formal assessment where personal data processing is likely to create high risks. The framework should remain deployment-specific and should be updated whenever the platform's participants, data processing or security or regulatory environment changes.

1. DIGIDEFENSE Assessment Model

Name of the System	
Organisation Details	
Report Details	
Assessment Type	
Document Date	
Document Owner	
Document Authors	

1.1. DISCLAIMER

Thank you for using DIGIDEFENCE Assessment. Please be advised of the following:

- This self-assessment tool is intended to support, in a non-exhaustive and indicative manner, the assessment of cyber threat intelligence (CTI) sharing systems against applicable legal and regulatory requirements, including the GDPR and cybersecurity obligations arising under NIS2, DORA, and any relevant sector-specific or national implementing measures.
- This self-assessment tool offers general guidance to help identify compliance considerations but does not certify compliance, replace the user's responsibility to meet all legal, technical, and organisational requirements, or constitute legal advice; its questions are not exhaustive and may not cover all relevant legal, technical, organisational, operational, or sector-specific issues, so it should be used only as a starting point rather than a complete compliance checklist.
- The legal and regulatory framework governing CTI sharing may evolve, including through legislative amendments, supervisory guidance, case law, and sectoral rules. Compliance must therefore be reassessed on a continuing basis, and the self-assessment should be revisited regularly to reflect changes in law, guidance, organisational practice, technology, threat environment, or the scope of the CTI sharing arrangement.
- Users remain fully responsible for the accuracy, completeness, and reliability of the information they provide in response to the tool's questions, including any information concerning CTI content, sharing practices, technical safeguards, and legal bases for processing or disclosure.

1.2. CTI system & technical / security details

These questions focus on intelligence quality, platform security and operational fit as related to CTI sharing.

1.2.1. Intelligence quality and usefulness

What are the primary purposes of the CTI you intend to share (e.g. detection, prevention, incident response, threat hunting, research)? Please specify.
[*insert your response here*]
For each CTI feed/type, how do you ensure that the information is actionable (i.e. directly usable for concrete defensive measures)?
[*insert your response here*]
Do you systematically tag CTI with any of the following?
☐ sector(s)/vertical(s) affected ☐ geography ☐ TTPs (e.g. via MITRE ATT&CK) ☐ confidence level ☐ other (please specify)
How do you ensure timeliness (e.g. maximum delay between detection and sharing, mechanisms for updating/revoking obsolete indicators)?
[*insert your response here*]
What standard formats or structured systems do you use to share cyber threat intelligence (e.g. STIX/TAXII or your own internal formats), and how do you ensure they are used correctly and not replaced by unclear or excessive free text?
[*insert your response here*]
Do you have a written policy or guide that clearly states what types of cyber threat information (e.g. indicators of compromise, attacker methods, incident details, or vulnerabilities) can be shared with others, and what must stay internal or be cleaned up before sharing?
[*insert your response here*]
Does your CTI policy clearly forbid sharing certain types of sensitive data (e.g. raw emails, full network captures, or unfiltered logs) unless there is a documented and approved exception?

1.2.2. Platform security and access control

What security measures control who can access cyber threat information and what they are allowed to do (e.g. multi-factor authentication, role-based access, or API keys)?
[*insert your response here*]
How do you protect cyber threat information when it is being sent and when it is stored (e.g. encryption in transit, encryption at rest, and how encryption keys are managed)?
[*insert your response here*]
How do you define user groups and levels of trust (e.g. different access permissions or reputation scores for contributors)?
[*insert your response here*]
What logging and monitoring is in place to trace CTI access, uploads, downloads, and onward sharing?
[*insert your response here*]
How do you identify and deal with misleading, false, or low-quality information shared in the system?
[*insert your response here*]
Do your governance documents clearly define the minimum security measures that any CTI platform or sharing channel must have (e.g. encryption, strong authentication, and logging), including safeguards required by law such as protecting data confidentiality, integrity, and availability, ensuring systems are resilient, managing access and risks appropriately, and regularly testing and reviewing security measures, as required under GDPR (Article 32) and NIS2?
[*insert your response here*]
Does your platform use the Traffic Light Protocol (TLP) or a similar system to label how sensitive information is, make sure these labels are enforced by the system (e.g. restricting who data can be shared with), and clearly explain the rules for using them in your information-sharing policy?
[*insert your response here*]

1.2.3. Risk of sharing and mitigation

For each dataset, how do you identify, if any, which attributes might expose (1) personal data, (2) sensitive business information, (3) details about the defense posture?
[*insert your response here*]

Do you carry out a structured risk assessment before introducing new types of cyber threat information or new user groups, considering how likely risks are, their potential impact, how much you trust the recipients, and the overall level of risk?
[*insert your response here*]
What technical measures do you apply to reduce sharing risks (e.g. redaction, aggregation, pseudonymisation, delayed sharing, throttling and others)? Please specify.
[*insert your response here*]
Do you keep a list of high-risk types of cyber threat information that need extra approval or additional safeguards before they can be shared?
[*insert your response here*]
Do you have a clear, written process that must be followed before adding new cyber threat information feeds or allowing new groups to receive information, including checks to make sure data protection and security requirements are met?
[*insert your response here*]

1.3. Data protection assessment

These questions assume the CTI may contain personal data or data that can be linked to individuals (e.g. IP addresses, user identifiers).

1.3.1. Roles and allocation of responsibility

For each activity involving cyber threat information, have you clearly identified who is responsible for deciding how and why the data is used (controller), whether this responsibility is shared (joint controller), or whether someone is processing the data on behalf of another (processor)? Is this clearly documented (e.g. in a CTI community agreement, memorandum of understanding, or data processing agreement)?
[*insert your response here*]

1.3.2. Legal basis and necessity

For each way you use cyber threat information (e.g. collecting it, using it internally, sharing it externally, or storing it long term), have you clearly identified and documented the legal basis that allows you to do so (GDPR Article 6(1))?
[*insert your response here*]
If you rely on legitimate interests (Article 6(1)(f)), have you carried out and documented a legitimate interest assessment that: clearly states the specific purpose (e.g. preventing fraud or protecting

networks), explains why using CTI (including any personal data) is necessary for that purpose, and shows how you have balanced this need against the rights and freedoms of individuals?
[*insert your response here*]
If you are sharing cyber threat information because the law requires you to (Article 6(1)(c)) (e.g. under NIS2 or DORA), have you clearly written down which law or rule requires this, and made sure you only share the minimum information needed to meet that requirement? Please specify.
[*insert your response here*]
For each type of data in your CTI (e.g. IP addresses, device IDs, user accounts, or activity logs), have you explained why using that data is needed for your specific purpose?
[*insert your response here*]

1.3.3. Data categories, minimisation and pseudonymization

Have you identified which parts of your cyber threat information could identify a person – either directly (e.g. a name or email address) or indirectly (e.g. an IP address or user ID that can be linked to someone) – and which parts could reveal sensitive personal information (e.g. health, political views) or information about criminal activity? Please specify.
[*insert your response here*]
For each piece of data in your cyber threat information, have you explained why it needs to be included, or considered whether you could achieve the same security goal by using less detailed data (e.g. summarising it, shortening it, or replacing identifying details with pseudonyms so individuals are not directly identifiable)? Please specify.
[*insert your response here*]
Do you have clear, standard methods for removing or masking sensitive details in common types of cyber threat data (e.g. shortening IP addresses or replacing identifiers with hashes), and are these methods applied consistently when data is collected or before it is shared?
[*insert your response here*]
Do you have written rules on how to handle CTI that contains: (1) stolen data sets; (2) data relating to suspected criminals or threat actors; or (3) data that originates from law-enforcement or intelligence sources (e.g. stricter sharing limits, higher classification)? Please speficy.
[*insert your response here*]

1.3.4. Purpose limitation and re-use

For each CTI dataset, are the primary purposes explicitly defined (e.g. prevention, detection, response) and communicated to participants?
[*insert your response here*]
Do you re-use CTI for secondary purposes (e.g. training AI models, long-term research, product improvement)? If so: (1) how do you assess compatibility with the original purposes, and (2) do you rely on a different legal basis than for the primary data processing, if yes, what is the legal basis?
[*insert your response here*]
Are retention periods defined per CTI category, and are mechanisms in place to delete or anonymise data once it no longer serves the defined purpose? Please specify.
[*insert your response here*]

1.3.5. Transparency and data-subject rights

If and how are data subjects informed that their data may be processed for security logging, incident handling, and CTI sharing (e.g. privacy notices, internal policies)?
[*insert your response here*]
Do privacy notices (external and internal) explicitly: (1) mention CTI and security-logging activities; (2) describe categories of personal data processed for security/CTI; (3) identify typical recipients (e.g. sector ISACs, service providers, authorities); and (4) specify retention periods for CTI-related data in addition to other matters required by the GDPR?
[*insert your response here*]
If you decide not to inform individuals about how their personal data is used in your CTI, do you clearly document: when and why you rely on GDPR exceptions (such as when informing someone would make it impossible or seriously harm security investigations), which legal provision you are using (e.g. Article 14(5), Article 23), why this exception applies in that situation, and what alternative safeguards you have put in place to protect those individuals' rights?
[*insert your response here*]
Through which channels can data subjects exercise their rights (e.g., access, erasure, restriction, objection rights concerning CTI-related processing and others)?
[*insert your response here*]
How do you technically locate and, where appropriate, delete or flag personal data embedded in CTI already distributed across multiple recipients?

[*insert your response here*]

1.3.6. Security of processing, DPIA and accountability

How have you mapped your CTI sharing system's security measures to the requirements of GDPR Article 32, including: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing?
[*insert your response here*]
Have you carried out a Data Protection Impact Assessment (DPIA) for your CTI sharing activities – especially if they involve large-scale monitoring of users or analysing behaviour (profiling) – to assess and manage risks to individuals' privacy?
[*insert your response here*]
Does your DPIA, among other requirements under the GDPR, explicitly: (1) describe CTI data flows and sharing partners; (2) identify specific high-risk scenarios (e.g. large-scale monitoring, cross-border CTI, profiling of users or devices); and (3) analyse risk-reduction measures (pseudonymisation, access controls, minimisation, TLP, logging)?
[*insert your response here*]
Are risks related to CTI and the measures to address them included in your overall risk management and incident response processes, rather than being handled separately?
[*insert your response here*]
Have you included your CTI processing activities and information-sharing arrangements in your records of processing activities (GDPR Article 30), and do these records, among other requirements of the GDPR, clearly: (1) mention when CTI is used to meet NIS2 or DORA requirements; and (2) link to any relevant Data Protection Impact Assessments (DPIAs) and legitimate interest assessments?
[*insert your response here*]

1.3.7. International transfers and onward sharing

Do any CTI flows involve transfer to third countries or international organisations (e.g. global CTI platforms, sector ISACs)?
[*insert your response here*]

For each transfer of CTI to a country outside the EU/EEA, have you identified which GDPR transfer mechanism you rely on – such as an adequacy decision (Article 45 of the GDPR), appropriate safeguards like standard contractual clauses or binding corporate rules (Article 46–47 of the GDPR), or a derogation for specific situations (Article 49 of the GDPR) – and assessed whether the level of protection of personal data in the receiving country is essentially equivalent, including any risks and supplementary measures needed (as explained in Schrems II decision of the CJEU)?
[*insert your response here*]

1.4. NIS2-specific questions – cybersecurity information-sharing arrangements

NIS2 Directive Article 29 requires Member States to ensure that entities can exchange relevant cybersecurity information on a voluntary basis (e.g. threats, vulnerabilities, indicators of compromise) within communities of essential and important entities and, where relevant, their suppliers, through information-sharing arrangements, while preserving confidentiality and protecting security and commercial interests.

1.4.1. Purpose and scope of sharing

Does your CTI sharing clearly aim to: (1) prevent, detect, respond to or recover from incidents, and/or (2) enhance overall cybersecurity (awareness, limiting spread of threats, supporting defensive capabilities, mitigation, collaborative research)? Please specify.
[*insert your response here*]
Are there categories of information you explicitly exclude from sharing because of sensitivity, proportionality or data-protection concerns as mentioned above? If yes, please specify.
[*insert your response here*]
Does the written information-sharing arrangement explicitly map each category of shared information (threats, near misses, vulnerabilities, IOCs, alerts, configuration recommendations) to the purposes listed in NIS2 Article 29(1)?
[*insert your response here*]

1.4.2. Community definition and governance

Are participating entities clearly identified as essential, important, or other entities, and are suppliers/service providers explicitly covered where relevant?
[*insert your response here*]
Do you have formal cybersecurity information-sharing arrangements (charter, terms of reference) that define: (1) membership criteria, (2) rights and obligations, and (3) revocation/exclusion conditions?

[*insert your response here*]
Are national CSIRTs (Computer Security Incident Response Teams) or other public authorities involved in your information-sharing arrangement? If yes, have you clearly defined their role and any conditions or restrictions on how the information they provide can be used or shared?
[*insert your response here*]
Is there a documented process for: (1) onboarding (e.g. vetting, security baseline checks); (2) suspending or excluding members who repeatedly fail to contribute, breach TLP, or misuse CTI; and (3) periodically reviewing membership lists and roles?
[*insert your response here*]

1.4.3. Operational elements and tools

Are dedicated ICT platforms and automation tools used for NIS2-related CTI sharing, and are their operational elements (format, access, logging) documented as part of the arrangement?
[*insert your response here*]
How do you ensure that the arrangement respects the "potentially sensitive nature" of shared information (e.g. tiered access, clearance levels, content vetting)?
[*insert your response here*]
Do you have procedures for incident-driven CTI sharing that align with NIS2 incident reporting timelines and content requirements?
[*insert your response here*]
Does your arrangement clearly document how CTI sharing works in practice, including which platforms and channels are used, who can access what information, logging and audit requirements, and the expected timelines for sharing information about incidents (e.g. early warning within 24 hours, more detailed information within 72 hours, and a final report within one month)?
[*insert your response here*]

1.4.4. Interaction with national implementation

Have you reviewed your Member State's NIS2 transposition to identify any additional conditions on information-sharing arrangements (e.g. notification obligations, sector-specific rules)? If yes, please specify what are these additional conditions.
[*insert your response here*]

For your information, in case there is a need to review the system from the Lithuanian Cyber Security Compliance perspective, there is a tool available here: https://forms.office.com/e/06a8P8cbAp.

This questionnaire is constructed according to the Lithuanian Description of the Cyber Security requirements as available here: https://www.e-tar.lt/portal/lt/legalAct/c8e268a0a00011efa605b9842742bf37. The relevant piece of legislation also include the Lithuanian Cyber Security Law: https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr. This questionnaire does not validate in full the cyber security compliance of the organization, however, provides significant guidance as to the further actions to be taken to ensure cyber security compliance following the NIS2 framework in Lithuania.

1.5. DORA-specific questions – financial sector CTI sharing

Digital Operational Resilience Act Article 45 allows financial entities to exchange cyber threat information and intelligence (e.g. indicators of compromise, tactics, techniques and procedures, alerts) within trusted communities, provided that the exchange enhances digital operational resilience and is carried out under arrangements that protect the confidentiality of the information, personal data, and comply with competition law.

1.5.1. Purpose and benefits

For each CTI-sharing arrangement involving financial entities, how does the entity document that the sharing: (1) enhances digital operational resilience, (2) raises awareness of cyber threats, and (3) supports detection, mitigation and recovery?
[*insert your response here*]
How do you regularly check and document that your information-sharing arrangement actually improves digital operational resilience (e.g. using metrics, lessons learned from incidents, or testing results)?
[*insert your response here*]
For each CTI information-sharing arrangement, do you keep a clear and simple document or table that: (1) explains how it improves digital operational resilience (e.g. awareness, detection, response, recovery); (2) lists the main types of CTI shared; and (3) shows how this information is actually used in internal processes (e.g. playbooks or incident response procedures)?

[*insert your response here*]
Are there defined KPIs or qualitative criteria for periodically reviewing whether the arrangement continues to provide sufficient resilience benefits to justify the associated risks and costs?
[*insert your response here*]

1.5.2. Trusted communities and rules of conduct

How are "trusted communities of financial entities" defined (e.g. membership criteria, vetting, sector coverage, etc.)?
[*insert your response here*]
Do information-sharing arrangements contain rules of conduct addressing: (1) business confidentiality, (2) protection of personal data in line with GDPR, and (3) competition-law / antitrust considerations? If yes, please specify.
[*insert your response here*]
Are there specific measures to prevent CTI sharing from being misused for anti-competitive behaviour (e.g. no discussion of pricing, market strategies)?
[*insert your response here*]
Do your rules or guidelines clearly explain: (1) how sensitivity labels like TLP should be used and followed; (2) what happens if someone misuses shared information; and (3) how disagreements or suspected breaches of the rules are handled?
[*insert your response here*]

1.5.3. Operational details and participation

What are the formal conditions for joining, remaining in, and exiting each DORA-relevant CTI-sharing arrangement?
[*insert your response here*]
Are public authorities involved; if so, in what capacity, and are their roles clearly limited and documented?
[*insert your response here*]

Are ICT third-party service providers involved in CTI processing or dissemination, and how are their roles governed contractually and technically?
[*insert your response here*]
Do arrangement documents clearly specify: (1) the conditions for participation, including minimum security controls and CTI-handling capability; (2) whether and how public authorities and ICT third-party providers may be involved; and (3) any restrictions on what third parties may do with CTI received through the arrangement?
[*insert your response here*]
Have you designated an internal "DORA Article 45 contact point" responsible for: (1) managing memberships; (2) coordinating CTI sharing; (3) liaising with CTI communities and competent authorities; and (4) maintaining evidence of compliance (e.g. membership validation, notifications, minutes)?
[*insert your response here*]

1.5.4. Notification and supervisory interaction

How do you notify competent authorities of the participation in CTI information-sharing arrangements, and of the cessation of membership?
[*insert your response here*]
Is CTI sharing covered in your broader DORA compliance documentation (e.g. ICT risk-management policies, resilience testing plans, incident reporting)?
[*insert your response here*]

1.6. Cross-cutting issues

Do you ensure that your CTI sharing system is described consistently across all your documentation – meaning that the purpose of sharing, the legal basis used, and the security measures in place are the same in your GDPR records (e.g. records of processing, DPIAs) and in your NIS2/DORA risk management and security documents?
[*insert your response here*]

Where the same CTI flow serves multiple regimes (e.g. NIS2 incident handling and DORA operational resilience), have you mapped how one set of controls and records satisfies all applicable requirements?
[*insert your response here*]
Do your governance documents for information-sharing arrangements (e.g. ISAC charters, MoUs, rules of conduct) clearly reference the relevant requirements from NIS2, DORA, and GDPR, so that responsibilities, rules, and safeguards are aligned and there are no gaps or contradictions between them?
[*insert your response here*]
Have you mapped each CTI flow to all applicable regimes (GDPR, NIS2, DORA, sector-specific rules) and verified that: (1) the same technical and organisational measures are sufficient to satisfy each regime's requirements; and (2) there are no contradictions (e.g. retention obligations vs. minimisation expectations)?
[*insert your response here*]
Is there a designated owner (e.g. CTI governance officer, DPO in consultation with CISO) responsible for regularly reviewing CTI practices in light of new laws, supervisory guidance, and sector best practices, and for triggering updates to LIAs, DPIAs, and information-sharing arrangements?
[*insert your response here*]

DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

1. Reasons for carrying out a data protection impact assessment

Description of the planned activities, their objectives and the planned personal data processing operations. Explanation of why a data protection impact assessment is necessary. If necessary, relevant documents shall be attached to the form.

2. Description of personal data processing

The actions of collecting, using, storing and destroying personal data are described, the sources from which the data will be collected and to whom it will be provided are indicated (a scheme of actions for processing personal data can be provided). The actions of processing personal data that may pose a risk to the rights and freedoms of natural persons are described.

The scope of processing is described: what categories of personal data will be processed; whether special categories of personal data or data on criminal convictions and criminal offences will be processed; how much data, how often it will be collected and used; how long the personal data will be stored; the approximate number of data subjects and the geographical scope of data processing are indicated.

The nature of the data processing is described: what kind of relationship your company has with the data subjects; whether the data subjects will have the opportunity to control the data processing; whether the data subjects can foresee that their personal data will be processed in this way; whether the data of children and other vulnerable persons will be processed; an assessment is made of whether such data processing is secure; whether the data processing technologies are new or whether existing technologies will be used in a different way; what is the level of technological development in this area; whether there are any societal or similar problems or issues that need to be taken into account; whether there is an obligation to comply with an approved code of conduct or an approved certification mechanism.

Description of the purposes of personal data processing: what result is sought to be obtained; what impact will it have on natural persons; what is the benefit of such data processing for your company and other persons.

3. Consultations

Describe how you plan to obtain the opinions of interested parties or justify why it is not necessary to do so: what kind of opinions you plan to obtain; what kind of people will be involved in your company, whether data processors will be involved; whether you plan to consult with data security experts or experts in other fields.

4. Assessment of necessity and proportionality

The lawfulness and proportionality of the processing of personal data are described: the basis for lawful processing is indicated; an assessment is made of whether your purpose will be achieved by processing personal data; whether the same result can be achieved in another way; how disruptions to operations will be avoided; how data quality will be ensured and the principle of data minimization implemented; what information will be provided to data subjects; how your company plans to implement the rights of data subjects; how it will be ensured that the data processor complies with the requirements; how the security of personal data transferred to foreign countries will be ensured.

5. Threat identification and assessment

The nature of the threat and the impact on the individual is described. If necessary, the associated business risk is described.	***Probability of harm***	***Severity of damage***	***Overall danger level***
	Unlikely, likely, very likely	Minimal, significant, severe	Low, moderate, high

6. Determination of mitigation measures

Additional measures that can be taken to reduce or eliminate high or medium level risks are indicated.

Threat	*Measures to reduce or eliminate the risk*	*Result of applying the measure*	*Residual danger*	*Measure approved*
		Eliminated, reduced, acceptable risk	Low, medium, high	Yes, no

7. Conclusions and decisions

Measures are indicated and the residual risk is identified.	*Name, surname, date, signature*

Opinion of the Data Protection Officer

The opinion of the Data Protection Officer must be provided on the lawfulness of the processing of personal data, the planned measures to mitigate or eliminate the risks, and the possibility of further processing of personal data.

The opinion of the data protection officer is indicated:	
	Name, surname, date, signature

Indication of whether the opinion of the data protection officer has been taken into account

If rejected, the reasons are justified.	
	Name, surname, date, signature

Opinions received from others

The opinions of other persons are briefly described and whether they have been taken into account. If the decision differs from the opinions of the persons concerned, the reasons are given.

	Name, surname, date, signature

A responsible person has been appointed to oversee this data protection impact assessment.

Note: The Data Protection Officer must monitor the compliance of the processing of personal data with the conclusions and decisions set out in the Data Protection Impact Assessment.

	Name, surname, date, signature

Bibliography

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
2. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng.
3. Article 29 Working Party Guidelines on Data Protection Impact Assessment, available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.
4. European Data Protection Supervisor – Data Protection Impact Assessment (DPIA), available at: https://www.edps.europa.eu/data-protection-impact-assessment-dpia_en.
5. Lithuanian State Data Protection Inspectorate – Sample DPIA Form, available at: https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzd_PDAV_forma.docx.
6. Lithuanian State Data Protection Inspectorate – DPIA: 10 Most Common Mistakes, available at: https://vdai.lrv.lt/uploads/vdai/documents/files/05_%20PDAV.pdf.
7. Republic of Lithuania Law on Legal Protection of Personal Data Processed for Law-Enforcement, National-Security or Defence Purposes, available at: https://www.e-tar.lt/portal/lt/legalAct/TAR.299D835159BE.
8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, available at: https://data.europa.eu/eli/reg/2024/1689/oj.

Literature used to compile the questionnaire

1. Abraham, C., Bélanger, F., & Daultrey, S. (2025). Promoting research on cyber threat intelligence sharing in ecosystems. Journal of Cybersecurity, 11(1). Available at: https://academic.oup.com/cybersecurity/article/11/1/tyaf016/8244123.
2. Albakri, A., Boiten, E., & Smith, R. (2020). Risk Assessment of Sharing Cyber Threat Intelligence. In: DETIPS 2020 – Workshop on Data Extraction and Threat Intelligence for Physical Security. Available at: https://detips2020.github.io/PreProceedings/DETIPS2020-paper-09.pdf.
3. Allegretta, M. (2025). Data-Driven Assessment of Cyber Threat Intelligence Sharing Practices (Doctoral thesis, Universidad Carlos III de Madrid). Available at: https://hdl.handle.net/10016/48644.
4. Borden, R. M., Mooney, J. A., Taylor, M., & Sharkey, M. (2018). Threat Information Sharing and GDPR: A Lawful Activity that Protects Personal Data. FS-ISAC White Paper (with White and Williams LLP & Osborne Clarke LLP). Available at: https://www.whiteandwilliams.com/assets/htmldocuments/Threat%20Information%20Sharing%20and%20GDPR_FS-ISAC%20Branded_1.2.19_Final_TLP%20WHITE.pdf.
5. 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 (NIS2 Directive).
6. 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) (Text with EEA relevance). OJ L 333, 27.12.2022, p. 80–152.
7. ENISA. (2009). Good Practice Guide on Information Sharing. Available at:https://www.enisa.europa.eu/publications/good-practice-guide.
8. ENISA. (2018–2025). Various reports and toolkits on ISACs, cooperative models and NIS/NIS2 implementation (including Cooperative Models for PPPs and ISACs and NIS2 support material). PPP/ISACs study available at: https://www.enisa.europa.eu/publications/public-private-

partnerships-ppp-cooperative-models. ISACs overview & toolkit available at: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/information-sharing-and-analysis-centers-isacs.

9. ENISA. (2018). Information Sharing and Analysis Center (ISACs): Cooperative Models. Available at: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.
10. ENISA. (2025). NIS2 Technical Implementation Guidance. Available at:: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.
11. Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6). Available at: https://researchportal.vub.be/en/publications/the-new-eu-cybersecurity-framework-the-nis-directive-enisas-role-/.
12. NIST. (2016). Guide to Cyber Threat Information Sharing (NIST Special Publication 800-150). Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf.
13. Nweke, L. O., & Wolthusen, S. (2020). Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection. In: 12th International Conference on Cyber Conflict (CyCon 2020), NATO CCDCOE Publications. Available at: https://www.ccdcoe.org/uploads/2020/05/CyCon_2020_4_Nweke_Wolthusen.pdf.
14. 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 (General Data Protection Regulation) (Text with EEA relevance). OJ L 119, 4.5.2016, p. 1–88.
15. 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 (Text with EEA relevance). OJ L 333, 27.12.2022, p. 1–79.
16. Sullivan, C., & Burger, E. (2017). "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence. Computer Law & Security Review, 33(1), 14–29.
17. The Legal Landscape of Cyber Threat Intelligence Sharing: A Study on International Legal Standards and Best Practices. Legal Studies in Digital Age, 2(1), 13–26. Available at: https://jlsda.com/index.php/lsda/article/view/8.
18. Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber Threat Intelligence Sharing: Survey and Research Directions. Computers & Security (preprint). Available at: https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf.