TECHNICAL NOTE

AN INTRODUCTION TO LIINE4DU 1.0: A NEW PRIVACY&DATA PROTECTION THREAT MODELLING FRAMEWORK

October 2024

INDEX

I. EXECUTIVE SUMMARY

Risk management is about thinking ahead and handling potential problems (threats) before they become real issues (incidents). It is a proactive process to govern uncertainties that threaten an activity's success: identifying, assessing and prioritising risks, followed by coordinating efforts and decisions to minimise, monitor and control their probability or impact. This process even allows decisions to be made on whether or not to carry out the activity if the risk involved is unacceptable or unmanageable.

Organisations need to manage project risks, financial risks, safety risks, cybersecurity risks, operational risks, market risks, reputational risks, legal risks, etc. When they process personal data, it is essential to carry out another risk management process: the one concerning the rights and freedoms of the data subjects, natural persons potentially affected by such personal data processing (employees, customers, users, providers, etc.). These risks to rights and freedoms may arise from the mere existence of such processing (authorised processing) or due to personal data breaches (unauthorised processing).

This note focuses on privacy threat modelling, the systematic process of identifying, understanding, and communicating threats and their corresponding prevention methods to protect personal data processing purposes. Privacy threat modelling involves systematically understanding what can go wrong using a proactive and structured approach.

Although privacy threat modelling can be used when designing privacy-preserving systems, defining data protection requirements, and facilitating better communication among stakeholders during the design, implementation, and testing phases, risk management is the main application of privacy threat modelling explored in this note. When regularly reviewed and updated as the processing or its context evolves or new threats emerge, privacy threat models support threat-informed risk analysis and impact assessment, threat-informed errors, weaknesses and vulnerabilities analysis and threat-informed mitigation planning.

Therefore, a privacy threat model can be essential for conducting effective Data Protection Impact Assessments (DPIAs). The threat modelling process is not mandatory and does not replace the DPIA or the risk management process, but it can be a very versatile and powerful tool whose output (mainly risk scenarios and potential impacts for data subjects' rights and freedoms) improves the results obtained, enables extended accountability and may save time and effort for the different stakeholders.

While LINDDUN is a robust and mature framework for privacy threat modelling, the AEPD has found some drawbacks when using it specifically to help with GDPR compliance and performing a DPIA. We have proposed the LIINE4DU framework based on LINDDUN but focusing on protecting rights and freedoms. The identified threat categories are different, hence the new acronym. Some categories are consistent with the LINDDUN approach, and others have been modified or added to align them with the primary objective of our framework: data protection, regulatory compliance, and the protection of individual rights and freedoms in the context of DPIAs.

Once the new threat categories have been identified and tested in different projects and initiatives, we are working on analysing what impacts on the rights and freedoms of data subjects each threat entails explicitly and how these threats could be mitigated. Furthermore, new privacy threat trees are being proposed to help practitioners use the proposed framework.

II. TERMS & DEFINITIONS

In the context of this note:

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (from GDPR).

'threat' means any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, the environment or the Nation (from NIST, adapted).

'incident' means an occurrence or materialisation of a threat that results in actual impacts (from NIST, adapted).

'vulnerability' means a condition that enables a threat to materialise and produce an incident (from NIST, adapted).

'risk' means the extent to which an entity is affected by a threat and typically a function of: (i) the adverse impacts that would arise if the threat materialises and produce an incident; and (ii) the likelihood of this occurrence (from NIST, adapted).

'impact' means the magnitude of harm that can be expected to result from the consequences of an incident (from NIST, adapted).

'likelihood' means the chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities (from ENISA).

'risk management' means a structured ongoing development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating and controlling the response to risk (from ENISA).

'scenario' means a pre-defined set of events and conditions that describe an incident or harm related to some aspect(s) of an organisation's operations to support conducting an analysis, developing a strategy or a plan, or conducting exercises (from ENISA, adapted).

'process' means an organised set of tasks which uses resources to transform inputs to outputs (from ENISA).

III. INTRODUCTION

Risk management is, essentially, about thinking ahead and taking action to handle potential problems (threats) before they become real issues (incidents). It is a proactive process to govern uncertainties that threaten an activity's success: identifying, assessing and prioritising risks, followed by coordinating efforts and decisions to minimise, monitor and control their probability or impact. Risk management can be applied to personal activities (for example, in planning a road trip) and business activities (for example, launching a new service). Risk management is a crucial tool for determining which activities can proceed and which should be avoided because they pose an unmanageable and unacceptable risk to people or organisations.

Consider the example of the road trip. Before making any decisions, you start considering what could go wrong and all the threats (think). For instance, the car might break down, you could get lost, you might run out of fuel or the weather could be bad for travel. Once these threats are identified, you try to evaluate your specific risks, how likely these threats will happen and how severe their impacts could be. With this information, for your particular trip, driving abilities, car and route, you can try to mitigate the most significant assessed risks (act). For example, you may get your old vehicle serviced just before the trip to reduce the chance of a breakdown. Or take out an insurance policy. You can use a GPS or map to plan the route and even have a backup in case you lose signal because you need a better sense of direction on roads you do not know. You may ensure your fuel tank is full, and plan stops at gas stations along the way, etc. The weather forecast might suggest that it is best not to undertake the trip at all. Or you can consider that a non-electric car is not a sustainable way of transportation and that you should not use your car.

In the business example concerning the launch of a new service, at least four types of risk should be managed. In this case, you need to consider project risks, such as timeline delays because the software development takes longer than expected or technical issues because bugs or glitches affect user experience. You also need to manage financial risks, such as budget overruns due to unforeseen expenses or revenue shortfalls, because the service might not initially attract enough customers. In addition, you need to manage safety risks that impact human lives or the environment. For example, if your service delivers food or involves dangerous staff operations. Finally, you must manage cybersecurity risks that could affect business continuity, allow fraudulent activities or compromise business data. Although these four types of risk arise from different threats, they have different impacts and may be managed with very different strategies, all of them are interrelated and should be integrated into a single risk management process. There could also be the need to assess other kind of risks such as operational risks, market risks, reputational risks, legal risks, etc. By considering these additional risks and taking appropriate action, the company can improve the chances of a successful service launch. In some cases, on the other hand, it may be decided to cancel the project because it involves an unacceptable risk.

In cases involving the processing of personal data, it is essential to carry out another risk management process: the one concerning the rights and freedoms of the data subjects, natural persons potentially affected by such personal data processing (employees, customers, users, providers, etc.). These risks to rights and freedoms may arise from the existence of such processing (authorised processing) or due to personal data breaches (unauthorised processing). Again, managing such risks should be integrated with the overall risk management of the processing (data protection by design).

Data protection risks come from threats related to any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration,

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. They depend on the processing's nature, scope, context and purposes.

This note focuses on threat modelling, the systematic process of identifying, understanding, and communicating threats and their corresponding prevention methods to protect the processing purposes. Privacy threat modelling involves systematically understanding what can go wrong using a proactive and structured approach. It is like pessimistic brainstorming that follows a specific method or framework and relies on a collection of reusable knowledge, such as threat libraries and catalogues or attack trees. This is crucial for ensuring that processing activities respect privacy and comply with data protection regulations, but it is definitely a complex task.

IV. PRIVACY THREAT MODELLING

A. THREATS TO THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

The most extended and mature threat modelling methods are focused on safety and cybersecurity, but not on privacy or data protection[1]. In fact, a common mistake in privacy threat modelling is not considering aspects of privacy beyond data breaches and those incidents that strictly impact data confidentiality.

Unlike cybersecurity threat modelling, privacy threat modelling requires considering the potential harm to individuals' rights and freedoms regarding processing their personal data, not to assets or organisations (financial or reputational harm, etc.). It also needs to consider a strong context dependency (social, legal, geopolitical, etc.) and personal data lifecycle, understanding how personal data flows through organisations, systems and services and identifying potential incidents at each stage (threats are different during collection than during retention, for example).

Furthermore, threats can materialise just for the existence of the processing itself, or through neutral or even benign actions (harm may be completely unintended), not only through malicious activities performed by adversaries, as in the case of cybersecurity. It has to be considered that cybersecurity threat modelling is often focused on identifying potential attack vectors and vulnerabilities that malicious actors could exploit. Finally, compliance with regulations is an essential point to be examined when performing privacy threat modelling, not the traditional adherence to security standards or frameworks such as ISO/IEC 27001 or those from the NIST, usually considered when performing security threat modelling.

Some of the main applications of privacy threat models are designing privacy-preserving systems, including data protection requirements from the beginning, thanks to their capacity for anticipating potential issues for the data subjects' rights and freedoms. Threat models support data protection by design because the appropriate technical and organisational measures should be selected to manage specific threats. In addition, they facilitate better stakeholder communication during the design, implementation, and testing phases.

Privacy threat modelling can be a powerful tool for data protection risk management too, specifically in three different areas (figure 1):

1. Threat-informed risk analysis and impact assessment: A risk analysis can be thought of as the combination of a threat model (what can go wrong), an adverse consequences model (what happens when things go wrong, related to impact) and a vulnerability model (the opportunity to make things go wrong, related to probability). The first is often forgotten, making practitioners waste their time assessing impossible scenarios when these scenarios could come directly from a threat modelling process. The threat modelling process can be of great help in this regard, as well as in modelling the impacts on the rights and freedoms of data subjects (adverse consequences and their severity).

2. Threat-informed errors, weaknesses and vulnerabilities analysis: Again, these kinds of analysis are very often scenario-based and can be guided by the results of a threat modelling process, looking for actual issues because specific scenarios may be of particular concern. A privacy threat model provides a detailed understanding of potential privacy threats, helping teams create more realistic and relevant scenarios. It can also support red-teaming or preparedness exercises in different contexts.

3. Threat-informed mitigation planning: The extensive catalogue of privacy safeguards and controls available makes it challenging to make informed decisions about which option

[1] Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). Threat modeling: a summary of available methods. Software Engineering Institute, Carnegie Mellon University.

is best for each case when designing and deploying appropriate technical and organisational measures. A threat model offers guidance to help practitioners address specific privacy concerns with scenario-targeted remedies rather than generic solutions. This approach allows for proposing a mitigation strategy tailored to the actual needs.

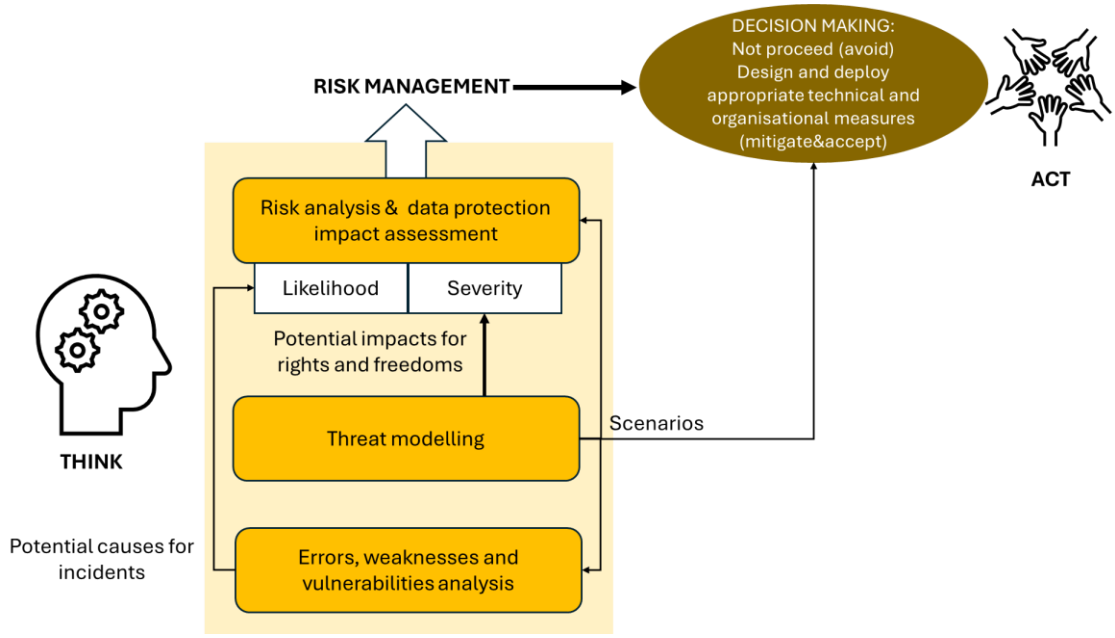

Figure 1. Privacy threat modelling supporting data protection risk management

The decision-making in Figure 1 may involve not proceeding with the personal data processing that was being designed (risk management based on avoiding the risk) or doing so by appropriately mitigating the assessed risks. And to do so by designing and deploying appropriate technical and organisational measures (risk management based in mitigating the risk and on proactive acceptance).

It is essential to understand that threat models are only helpful if they are regularly reviewed and updated as the processing or its context evolves, or new threats emerge. Obsolete or incomplete threat models can only lead to wrong decisions. Anyway, the threat modelling process should be conducted considering the characteristics, nuances and specificities of the particular data processing, taking into account its technical, social, legal, and organisational context.

B. PRIVACY THREAT MODELLING AND THE GDPR

The GDPR establishes principles and requirements for protecting personal data, including data minimisation, purpose limitation, and data security, to mention only some examples. By systematically identifying and mitigating privacy threats, privacy threat modelling may help organisations ensure compliance with these GDPR principles and requirements.

Furthermore, as mentioned before, the GDPR emphasises the concept of data protection by design, which requires integrating data protection measures and guarantees, taking into account the nature, scope, context, purpose, and risks for the rights of natural persons when designing personal data processing activities. Privacy threat models may help embed privacy considerations into the processing design, proactively addressing privacy threats.

The GDPR focuses on protecting personal data from various threats, including authorised processing, unauthorised access, data breaches, or misuse. Privacy threat modelling may help identify specific threats, such as linking, identifying, or data disclosure, and develop targeted mitigations to address these threats.

In addition, the GDPR requires organisations to demonstrate compliance through proper documentation and accountability measures. A privacy threat model may provide clear and structured documentation of identified threats, their impacts and mitigation measures, which can be used to demonstrate the required compliance. Compliance is an ongoing process that requires continuous monitoring and updating of data protection measures. Continuous improvement can be achieved by regularly updating the threat model.

Finally, the GDPR mandates organisations to conduct Data Protection Impact Assessments (DPIAs) for processing activities likely to result in high risks to individuals' rights and freedoms. Privacy threat modelling frameworks provide a structured approach to identifying and assessing privacy threats, which may be essential for effective DPIAs (see Figure 1).

First, it allows the systematic identification and analysis of things that could go wrong. It helps break down high-level threats into specific, actionable items, and as it has been introduced before, it ensures no aspect is overlooked, assisting with prioritisation.

Second, the threat model helps identify appropriate countermeasures for each threat, ensuring that the DPIA includes tailored and practical strategies to manage privacy risks.

Third, a threat model's structured approach ensures that all identified threats, their impact on fundamental rights and freedoms, and mitigation measures are well documented. This documentation may be crucial for demonstrating compliance with data protection regulations, such as GDPR.

Fourth, as already mentioned, the privacy threat model supports continuous monitoring and updating of the DPIA as the processing, or its context, evolves or new threats emerge. It encourages a proactive approach to privacy, helping to anticipate and address potential issues before they become significant problems.

Finally, threat models' visual and structured nature makes communicating privacy risks and mitigation strategies easier for stakeholders, including management, regulatory bodies or control authorities. It facilitates collaboration among different teams, ensuring a comprehensive understanding and approach to data protection.

In conclusion, it should be noted that the threat modelling process is not mandatory and does not replace the DPIA or the risk management process. It can be an additional accountability mechanism and a very powerful tool whose output improves the quality of the obtained results concerning specific tasks.

For example, when conducting a DPIA, once a systematic description of the envisaged processing operations and the purposes of the processing have been produced and an assessment of the necessity and proportionality of the processing operations in relation to the purposes has been performed, the threat model can help with the assessment of the risks to the rights and freedoms of data subjects and with the selection of the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. Furthermore, it may save time and effort for the different stakeholders.

Example 1

According to the AEPD guide "Risk Management and Impact Assessment in the Processing of Personal Data", the identification and analysis of risk factors for the rights and freedoms of natural persons is the previous step to the evaluation of the level of risk inherent in the processing of personal data. In this guide, different risk factors are listed based on the purposes of the processing, the types of data use, etc. Data breach scenarios are mentioned explicitly, but no other types of risk scenarios are mentioned.

The Data breach as a risk scenario and all the risk factors listed in that guide are not exhaustive, but a minimum set laid out in the current regulation[2], and the data controller should identify those risk scenarios and factors that are specific to the processing and include them in its assessment.

Privacy threat modelling allows to extend the minimum set of risk scenarios identified in the already mentioned guide, taking into account all the threats that can materialise. That is, all the things that could go wrong and the severity of the specific impacts that they could have on the rights and freedoms of data subjects (threat-informed risk analysis and impact assessment).

Example 2

According to the AEPD guide "Risk Management and Impact Assessment in the Processing of Personal Data", the impact and likelihood of harm to individuals, as a result of the processing of personal data, must be assessed.

Privacy threat modelling allows a more exhaustive assessment, by risk scenario, of the impact and likelihood of harm to individuals the above the mentioned guide taking into account the specific threats that can materialise and how could they be materialised (threat-informed errors, weaknesses and vulnerabilities analysis).

Example 3

According to the AEPD guide "Risk Management and Impact Assessment in the Processing of Personal Data", the controller or processor has to manage the risk by addressing the specific peculiarities of its data processing. In this regard, the controller or processor must select or define the most appropriate measures and safeguards to address the specific risks that have been identified.

Privacy threat modelling allows a more well-founded and specific selection, by risk scenario, of measures and safeguards from the listed in the mentioned guide taking into account the specific threats that can materialise and how could they be avoided or mitigated (threat-informed mitigation planning).

[2] Mainly the data protection regulation, EDPB opinions and binding decisions, and applicable sectoral regulation.

V. BACKGROUND

While much research and documentation describe threats to privacy and data protection, very few provide a method for actually identifying these threats within specific applications, services, processes, or projects. Clear and practical guidance on determining whether particular threats exist is required.

Specific extensions to traditional cybersecurity threat modelling methods have been proposed unofficially such as Elevation of Privacy[3] (an extension for Elevation of Privilege). But this note is focused on methods and frameworks devoted specifically to privacy and data protection.

The only published and widely used privacy-specific threat modelling method is LINDDUN[4]. LINDDUN is a privacy threat modelling framework designed to help identify and mitigate privacy threats in software systems. LINDDUN is an acronym that stands for the seven types of privacy threats it addresses[5]:

- Linking: Associating data items or an individual's actions to learn more about an individual or group.
- Identifying: Learning the identity of an individual, through leaks, deduction, or inference.
- Non-repudiation: Being able to attribute a claim to an individual.
- Detecting: Deducing the involvement of an individual through observation.
- Data disclosure: Excessively collecting, storing, processing or sharing personal data.
- Unawareness: Insufficiently informing, involving or empowering individuals in the processing of their personal data.
- Non-compliance: Deviating from security and data protection best practices, standards and legislation.

LINDDUN follows the same principles that the well-known cybersecurity threat modelling method STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)[6]. Their approach tries to answer the same four questions:

1. What are we building? The starting point for understanding the modelled system is a Data Flow Diagram (DFD) drawn using the same conventions and vocabulary. This diagram represents the system's data flows, data stores, processes, and external entities and allows for highlighting elements relevant to privacy and data protection.

2. What can go wrong? The privacy threat types mentioned drive this analysis, iterating in a structured way over each system component. LINDDUN threat types are used to systematically identify potential privacy threats for each element in the DFD. Threat trees may help break down complex threats into more manageable sub-threats.

3. What are we going to do about it? This step is guided by a catalogue of mitigation strategies and safeguards, allowing the determination of appropriate countermeasures to mitigate the risk associated with each identified threat.

4. Did we do a decent job? The produced model and the followed method should be evaluated to reflect on lessons learned and improve future results.

[3] Elevation of Privacy, https://github.com/WithSecureOpenSource/elevation-of-privacy
[4] Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering, 16(1), 3-32.
[5] LINDDUN Privacy Threat Modelling, https://linddun.org/
[6] Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.

LINDDUN has been used in the past because it provides a systematic approach to identifying and addressing privacy threats early in the software development lifecycle. It covers a wide range of privacy threats and ensures thorough analysis. Furthermore, it can be tailored to different project needs and complexities.

While LINDDUN is a robust and mature framework for privacy threat modelling, we have found some drawbacks when using it specifically for helping with GDPR compliance and perform a Data Protection Impact Assessment. LINDDUN does not always directly map to specific GDPR principles and requirements. While it helps identify privacy threats, translating these into GDPR compliance measures can be challenging. In addition, LINDDUN primarily focuses on technical threats and may not fully address organizational and procedural aspects of GDPR compliance or aspects concerning data subjects' rights and freedoms. Therefore, integrating LINDDUN findings into a DPIA can be complex and may require additional effort to ensure all essential GDPR aspects are covered.

VI. OUR PROPOSAL

LINDDUN can still be a valuable tool for ensuring comprehensive GDPR compliance or supporting effective DPIAs. However, tailoring LINDDUN to fit specific GDPR compliance needs may require significant customisation and adaptation. We have started by proposing the LIINE4DU framework and performing some initial validations[7].

Some of the essential aspects of LINDDUN that remain in our framework are:

- It is agent-agnostic, focusing on the materialization of privacy threats and their impacts, not threat agents and their motivation.
- A Data Flow Diagram (DFD) is a graphical tool for modelling the processing under analysis and guiding the threat identification and analysis process.
- Some LINDDUN catalogues and body of knowledge have been used as a starting point.
- The followed approach is based on the traditional four questions proposed in STRIDE.

The essential changes of our proposal can be summarised in:

- The focus is on protecting rights and freedoms and regulatory compliance (concerning GDPR).
- The identified threat categories are different, hence the new acronym. Some categories are consistent with the LINDDUN approach, and others have been modified or added to align them with the primary objective of our framework: data protection, regulatory compliance, and the protection of individual's rights and freedoms in the context of DPIAs. Specifically, we have eliminated the Non-compliance category from the regulatory point of view, as data processing that does not comply with regulations cannot be implemented and it is a too generic category to be useful in our context. Additionally, we have added four new categories: Inaccuracy, Exclusion, Data breaches and Deception.

The proposed categories are summarised in Table 1. The last three categories are intrinsically linked to an organisation's risk management processes and the data processing design and entail direct non-compliance with the GDPR. Conversely, the remaining proposed categories may directly impact individual rights and freedoms from a broader perspective and may or may not involve non-compliance with the data protection regulation.

The threat of Data Breach is the frontier between these two groups of threats, as some of them may occur due to non-compliance with the GDPR (by not incorporating adequate security measures, article 32 GDPR) while others may be unavoidable. It has to be considered that most Data Breaches can be avoided by the controller and the processor by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

[7] Beltrán, M., & de Salvador, L. (2024, August). Implications of Age Assurance on Privacy and Data Protection: A Systematic Threat Model. In *Annual Privacy Forum* (pp. 1-22). Cham: Springer Nature Switzerland.

Linking	This threat involves associating different data items or data subject's actions to learn more about a data subject or group.
Identifying	This threat involves learning the identity of a data subject directly (through the processing of identifiable information or leaks, for example) or indirectly (through deduction or inference, for example).
Inaccuracy	This threat involves using obsolete, wrong, incomplete, biased or low-quality data that may lead to incorrect decisions or actions, potentially causing inconvenience or even harm to the data subject.
Non-repudiation	This threat involves the ability to attribute a claim to the data subject (something they know, they are, they do, etc.) when this implies an impact on their fundamental rights and freedoms.
Exclusion	This threat involves unintentionally or deliberately failing to adequately serve a data subject, hindering their participation or involvement in physical or digital life.
Detecting	This threat involves deducing the existence of data items or data subject's actions through observation.
Data Breach	This threat involves destruction, loss, alteration, unauthorised disclosure of, or access to, personal data by mistakes, malicious insiders or cyberattacks.
Deception	This threat involves intentionally attempting to influence, coerce or manipulate the data subject into making unintended, unwilling and potentially harmful decisions, often against their best interests.
Data Disclosure	This threat involves excessively collecting, storing, processing, or sharing/transferring personal data.
Unawareness and Unintervenability	This threat involves insufficiently demonstrating compliance or insufficiently informing, involving, or empowering data subjects in the processing of their personal data.

Table 1. Threat categories in the LIINE4DU framework.

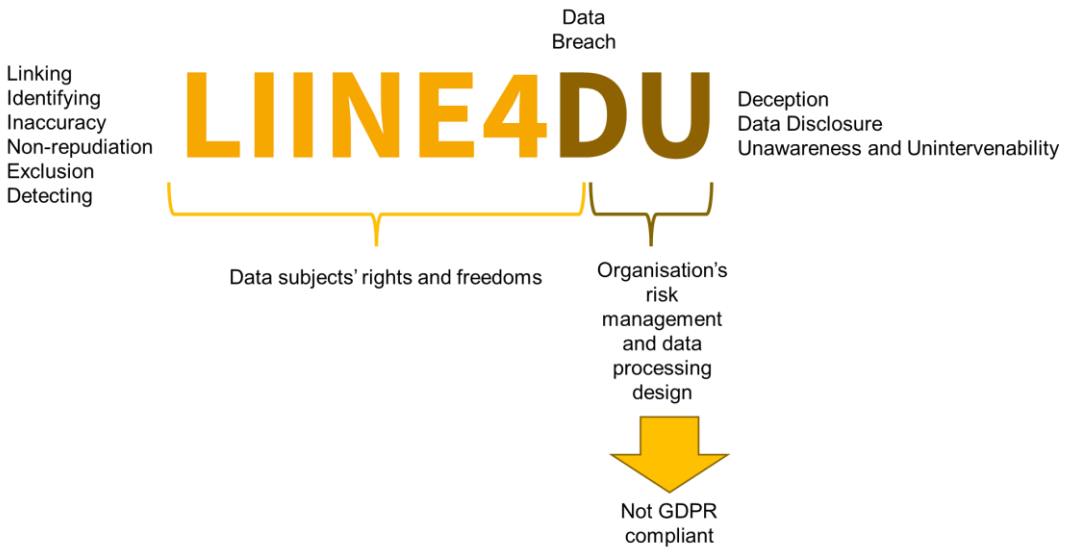

Figure 1. Summary of threat categories in the LIINE4DU framework.

Some additional clarifications may be appropriate at this point:

- A prerequisite for using the LIINE4DU framework is the legitimacy and lawfulness of the modelled personal data processing. The proposed framework does not consider "non-compliance" as a threat. Threats from personal data processing with illegitimate specific purposes determined at the time of the collection of the personal data that do not have a legal basis or which clearly violate data protection regulation in any other aspect (mainly, articles 5 to 50 GDPR) should not be modelled, since a personal data processing that is not compliant cannot be carried out. It would not make sense to model its potential impacts to the data subjects' rights and freedoms.
- In this way, only threats from personal data processing that have already been initially assessed as legitimate, lawful, and compliant should be modelled since the proposed framework focuses especially on how to avoid or mitigate the identified threats and on understanding their potential impacts on the rights and freedoms of data subjects.
- Once the LIINE4DU framework has been used, the existence of threats in the last categories of the acronym (most Data breaches, Deception, Data Disclosure, Unawareness and Unintervenability) implies non-compliance with the GDPR and directly that personal data processing should not be carried out until such threats are avoided. The following table provides a first approximation (not exhaustive) to the most common infringements in relation to these threat categories:

Data Breach	• Article 5: "integrity and confidentiality". • Article 25: Data protection by design and by default. • Article 32: Security of processing.
Deception	• Article 5: "fairness", "transparency", "purpose limitation", "data minimisation". • Article 25: Data protection by design and by default.
Data Disclosure	• Article 5: "fairness", "purpose limitation", "data minimisation", "storage limitation". • Article 25: Data protection by design and by default.
Unawareness and Unintervenability	• Article 5: "transparency", "accuracy", "accountability". • Articles 12 to 21 concerning the Rights of the data subject. • Article 22: Automated individual decision-making, including profiling. • Article 25: Data protection by design and by default.

- Threats in the rest of the framework acronym categories (Others in Figure 2) may or may not involve non-compliance with the data protection regulation. The privacy threat modelling process should help the controller sufficiently identify and avoid or mitigate the risks.
- Once the data processing complies with the regulation (after two checks), the outputs of the threat modeling process can be used for the different threat-informed applications mentioned in section IV of this document.

Figure 2 summarises the context for conducting privacy threat modelling with LIINE4DU. As shown, it can be a very versatile and powerful extension (see examples in Section IV.B) of the already existing guide and tools for risk management and impact assessment in the processing of personal data.

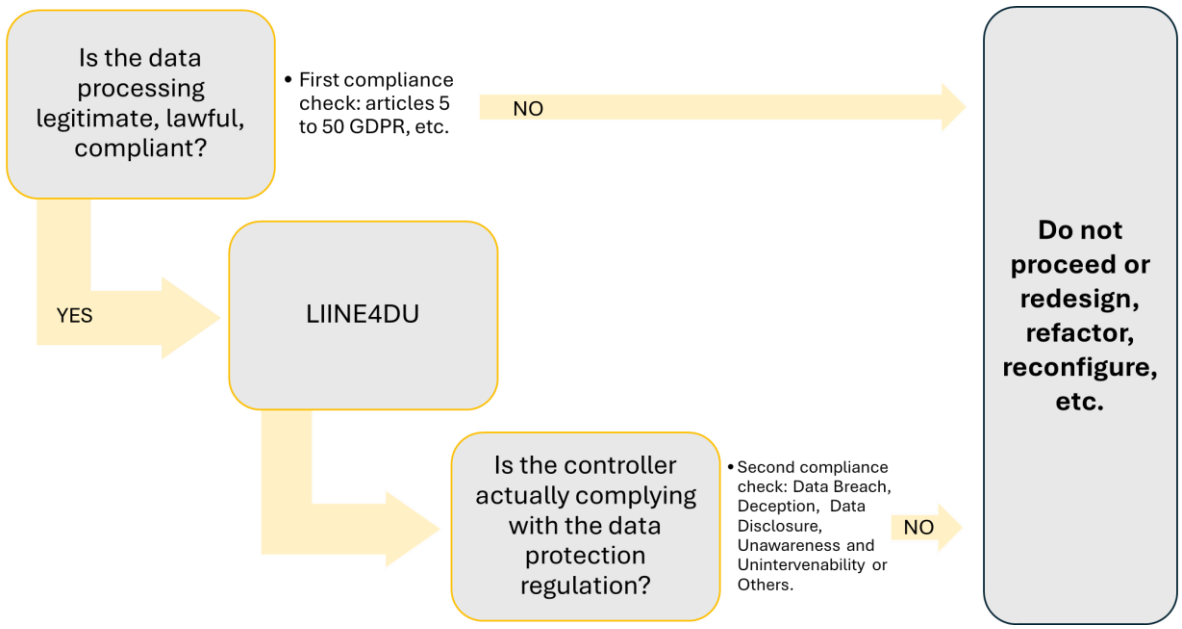

Figure 2. Applying the LIINE4DU framework in the initial stages of designing a personal data processing.

VII. NEXT STEPS

Once the new threat categories have been identified and validated in different projects and initiatives, we are working on analysing the first categories of threats. It means analysing LIINEDD (excluding “Deception”, “Disclosure” and “Unawareness and Unintervenability”, because, as it has been already mentioned, they imply non-compliance with the GDPR), what impacts on the rights and freedoms of data subjects each threat entails explicitly, and how these could be mitigated. It would be essential to adopt a risk-based approach, which is so common in the data protection field, to decide about implementing the appropriate technical and organisational measures to integrate the necessary safeguards into the processing to meet the GDPR principles and requirements.

Furthermore, new threat trees are required. Threat trees are helpful in privacy threat modelling, as demonstrated in LINDDUN over the last few years. They help break down complex threats into more manageable components.

Remember that threat trees are hierarchical diagrams representing potential threats, starting with a root node representing a high-level threat and branching out into sub-threats and contributing factors. A threat tree is composed of a Root Node (the main threat or privacy concern), Branches (sub-threats or specific aspects of the main threat) and Leaves (the most granular level of threats, often representing particular events, actions, vulnerabilities or attack vectors).

Threat trees guarantee clarity, providing a clear, structured way to visualise and understand complex threats. They ensure that all potential sub-threats and aspects are considered. Threat trees can be completed and improved with guiding questions and criteria, examples, and additional information such as impacts or safeguards. We are working on creating a first threat tree for each threat category in our model along with detailed examples of their use. Colleagues from other Data Protection Authorities, experts in conducting DPIAs and researchers will help to review these trees to ensure completeness.

Threat trees will be updated as threats evolve, or new threats are identified (we expect new LIINE4DU versions in the future). We intend to involve different stakeholders to view potential threats comprehensively and leverage existing projects and initiatives to guide our efforts, such as the MITRE Pattern and Action Nomenclature Of Privacy Threats In Context (PANOPTIC)[8], the Solove’s taxonomy of privacy[9], the NIST Problematic Data Actions[10] or the Data Privacy Vocabulary[11].

[8] MITRE PANOPTIC™, https://ptmworkshop.gitlab.io/#/panoptic

[9] Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, 154(3), 477–564. https://doi.org/10.2307/40041279

[10] NIST IR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems (2017), https://csrc.nist.gov/pubs/ir/8062/final

[11] W3C Data Privacy Vocabulary, https://w3c.github.io/dpv/2.0/dpv/