LINDDUN GO

A lean team approach to privacy threat modeling

Organizations that are looking for a lean approach to privacy threat modeling will benefit from LINDDUN GO. This trimmed-down variant of LINDDUN helps teams look at their software design from a privacy perspective to identify potential threats. It aligns with the **Privacy by Design principle, and helps build privacy protections at the software system's core.** Clearly, LINDDUN GO is best performed early in the development lifecycle when potential issues can be caught and resolved.

What's great about LINDDUN GO is that it requires little expertise and effort, though ensures a thorough analysis.

LINDDUN GO cards represent common threats

LINDDUN GO takes on a collaborative approach and is best performed in a workshop with a cross-functional team. It comes in the form of a **card deck** and can be played offline or online.

The cards represent the **34 most common privacy threats** and are designed to guide you through the threat analysis process. They come in six suits, matching the main LINDDUN privacy threat categories. These privacy categories are at the core of the methodology and represent realistic, yet sophisticated privacy risks to software systems.

PRIVACY THREAT CATEGORIES

LIND(D)UN is a mnenomic for the privacy threat categories it supports:

LINKABILITY: You can distinguish whether two items of interest (IOI) are linked, even without knowing the identity of the subject of the linkable IOI.

IDENTIFIABILITY: You can identify the subject within a set of subjects (i.e. anonimity set).

NON-REPUDIATION: A data subject cannot deny they know, did, said something.

DETECTABILITY: You can distinguish whether an item of interest exists or not.

UNAWARENESS: A data subject is unaware of, or unable to intervene in, the collection and processing of their personal data.

NON-COMPLIANCE: The system does not comply with data protection principles.

PRIVACY BY DESIGN

In our technology-driven world, there is a growing understanding that privacy is best protected when its built into the core of our systems, services and business processes.

Privacy by design ensures that privacy features are directly embedded into the design at an early stage, and not bolted on afterwards. Privacy laws such as the GDPR mandate privacy by design and by default.

Technology companies that succeed in developing and operating privacy-proof applications, where personal data is protected and privacy breaches prevented, can use this as a market differentiator. Those who lag behind may cause considerable damage to their reputation and harm the rights of their customers, employees and users.

WHY LINDDUN GO?

- **Threat-based**: you need to know what can go wrong in order to fix it.
- **Lean but structured approach**: you systematically iterate over every system hotspot, using privacy threat cards.
- **Knowledge support**: privacy is a complex matter; GO offers expert privacy knowledge on common threats.

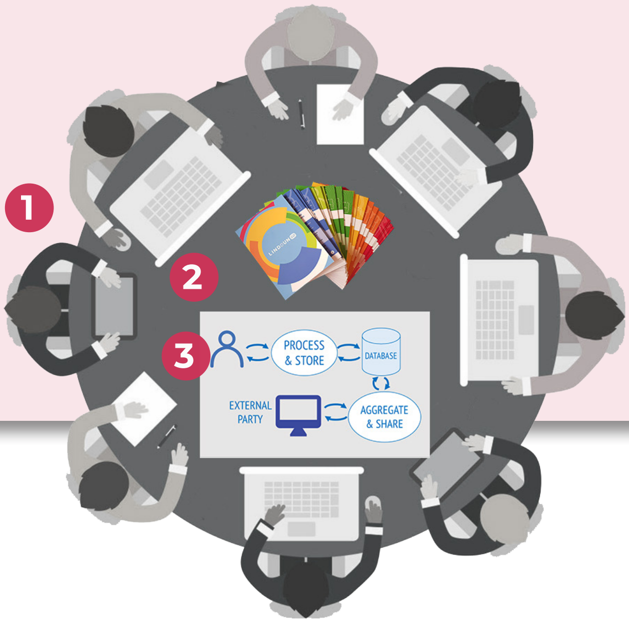
LINDDUN GO was developed at DistriNet Research Group, KU Leuven.
For more info: www.linddun.org and www.linddun.org/go

LINDDUN GO in practice

LINDDUN GO follows the general **Threat Modeling** approach, where a team analyzes a system to highlight concerns.

What you need

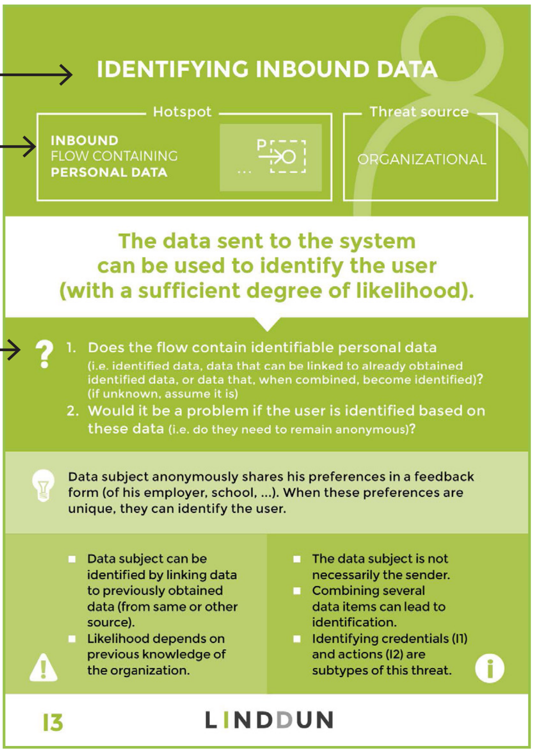
1. A team, including a domain expert, system architect, developer, DPO, legal expert, CISO, privacy champion.
2. The LINDDUN GO card deck.
3. A system description.



LINDDUN GO dynamics

- All participants take turns to discuss potential threats for each card.
- Each card represents a common privacy threat.
- The card guides you through the threat elicitation.
- You systematically iterate over each system hotspot (where threats are likely to occur) in your system description.
- You answer the questions on the card to check if the threat applies.
  - Could it be done?
  - Would it be a problem?
- If both are affirmative for a specific hotspot in your system, you have identified a threat.
- Make sure to document it.
- Proceed with the remaining hotspots until no one can find new threats.
- The exercise is finished when all threat cards have been discussed for all applicable hotspots in the system description.

Schedule 2 to 3 hours to complete the threat modeling process using LINDDUN GO. The more elaborate and complex your system is, the more time you will need.



IDENTIFYING INBOUND DATA

Hotspot: INBOUND FLOW CONTAINING PERSONAL DATA

Threat source: ORGANIZATIONAL

The data sent to the system can be used to identify the user (with a sufficient degree of likelihood).

? 1. Does the flow contain identifiable personal data (i.e. identified data, data that can be linked to already obtained identified data, or data that, when combined, become identified)? (if unknown, assume it is)
2. Would it be a problem if the user is identified based on these data (i.e. do they need to remain anonymous)?

Data subject anonymously shares his preferences in a feedback form (of his employer, school, ...). When these preferences are unique, they can identify the user.

- Data subject can be identified by linking data to previously obtained data (from same or other source).
- Likelihood depends on previous knowledge of the organization.

- The data subject is not necessarily the sender.
- Combining several data items can lead to identification.
- Identifying credentials (I1) and actions (I2) are subtypes of this threat.

I3 LINDDUN

Next steps

After you have identified potential privacy threats to your system design, you are now ready to prioritize these threats and develop mitigating strategies.

www.linddun.org/go