LINDDUN

GO

www.linddun.org

DistriNet

KU LEUVEN

Introducing LINDDUN GO

Your Privacy Threat Modeling Companion

LINDDUN GO revolutionizes privacy threat modeling with a lean card game approach.

Derived from LINDDUN, GO simplifies the identification of privacy threats using 7 key LINDDUN threat types: Linking, Identifying, Non-Repudiation, Detecting, Data Disclosure, Unawareness and Unintervenability, and Non-Compliance. With 33 threat cards highlighting the most common privacy threats and system hotspots, this game transforms the privacy assessment process into an engaging, collaborative experience.

Designed for structured brainstorming with diverse teams, LINDDUN GO requires only the card deck and a system sketch to kickstart your dynamic journey. Whether you're a seasoned pro or new to threat modeling, it offers an accessible and engaging way to address privacy concerns.

Gather your team, shuffle the cards, and let the adventure in privacy threat modeling begin.

Visit our website to learn more: www.linddun.org

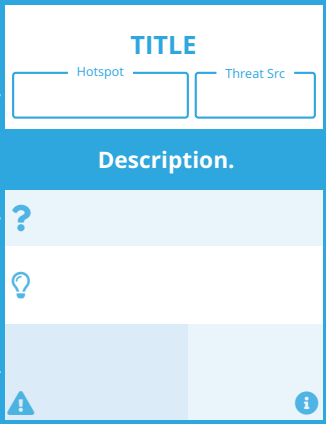
v240118

THREAT CARDS

Title: the name of the threat card

Hotspot: where the threat occurs in the system

Threat source: origin of the threat



Description: brief explanation of the threat

Elicitation questions: to determine if the threat applies

Examples: illustrating the threat

Consequences: why the threat is important

Additional information

Card identifier

INSTRUCTIONS

Gather a diverse group of privacy enthusiasts, and bring a simple sketch or diagram of the software system under analysis. Game dynamics:

1. The first participant picks a random threat card and puts it on the table so that everyone can see it.

2. Assess if the illustrated privacy threat forms a relevant risk in the system. For each hotspot in your system, consider the card's elicitation questions.

3. If the threat is possible, you have identified a threat. Make sure to document the threat.

4. Other participants can join in and report any overlooked threats.

5. When no one can discover any new threats, the next participant draws a card and starts over.

6. The exercise is finished when all threat cards have been discussed.

LINKING

What?

Learning more about an individual or a group by associating data items or user actions. Linking may lead to unwanted privacy implications, even if it does not reveal one's identity.

Tell me more!

Linking refers to the process of associating different data items (incl. metadata) in a manner that results in undesirable privacy implications. Combining related data items may reveal (additional) information about a data subject or groups of data subjects.

So what?

Linking becomes problematic when it can result in inference (learning more about individuals), singling out individuals, aggregating additional data to build profiles, etc. This may subsequently give rise to other threats, such as identifying.

Hotspots

Inbound user with personal data

There is an inbound flow from the user to the system in which personal data is transferred.

Inbound personal data

There is an inbound flow to the system in which personal data is transferred.

Inbound user

There is an inbound flow from the user to the system.

Storing/retrieving

The system stores incoming data or retrieves stored data.

Processing

The system processes incoming data and provides this to another entity.

IDENTIFYING

What?

Identifying threats arise when the identity of individuals can be revealed through leaks, deduction, or inference in cases where this is not desired.

Tell me more!

A key distinction is made between threats in the context of identified data (where there is an explicit link), and identifiable data (where the link can be derived based on a pseudonym, identity-revealing content, or a small set of potential subjects, known as the anonymity set, that allow (re-)identification).

So what?

It can be undesirable to know the identity. Working with identified data records requires additional protective measures and can lead to other threats such as unawareness and non-compliance.

Hotspots

Inbound user with personal data

There is an inbound flow from the user to the system in which personal data is transferred.

Inbound user

There is an inbound flow from the user to the system.

Inbound personal data

There is an inbound flow to the system in which personal data is transferred.

Storage

The system has a data store.

NON-REPUDIATION

What?

Non-repudiation threats pertain to situations where an individual can no longer deny specific claims.

Tell me more!

The system retains evidence related to a particular action or fact, influencing the ability to deny claims. Examples of this evidence include log files, digital signatures, document metadata, and watermarked data, all of which can be attributed to an individual.

So what?

Non-repudiation threats impact the plausible deniability of individuals, rendering them unable to refute specific actions or involvements, such as submitting a whistleblower report or casting a vote for someone.

Hotspots

In/outbound user

There are inbound flows from and outbound flows to a user.

Inbound user

There is an inbound flow from the user to the system.

Outbound user

The system has an outgoing flow to the user.

Storage

The system has a data store.

Processing

The system processes incoming data and provides this to another entity.

DETECTING

What?

Detecting threats pertain to situations where the involvement, participation, or membership of an individual can be deduced through observation.

Tell me more!

Detecting can be done by observing communication flows, including interactions with a system or service, and communication between systems. Detecting can also be achieved by observing application side effects or system responses, where the existence of certain data may be inadvertently revealed by the system.

So what?

Observing or ascertaining the existence can be sufficient to learn sensitive information about individuals. Furthermore, detecting also facilitates linking and identifying, allowing for the inference of additional information about individuals.

Hotspots

Outbound flows

There are outbound flows from the system to external entities (e.g., third parties).

In/outbound user

There are inbound flows from and outbound flows to a user.

In/outbound flows

The system has in- and outbound flows to external entities (e.g., third parties).

Retrieving

The system responds to data requests.

DATA DISCLOSURE

What?

Data disclosure threats represent cases in which disclosures of personal data to, within, and from the system are considered problematic.

Tell me more!

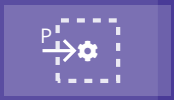
Disclosures should consider the best interests of the involved data subjects, with the minimization principle playing a crucial role. The system should be designed to only collect, process, store, and share the minimum amount of personal data necessary for the required functionality.

So what?

In addition to legal implications (non-compliance), this also raises the likelihood and impact of theft, data leaks, and unwanted or accidental disclosure to unintended parties. The more data is disclosed to and by the system, the more likely it can be abused for detecting, linking, identifying, or non-repudiation threats by any of the threat sources considered.

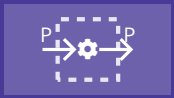
Hotspots

Inbound personal data



There is an inbound flow to the system in which personal data is transferred.

Processing personal data



The system processes incoming personal data and shares this with external entities.

Storage

The system has a data store.

Outbound personal data

There are outbound flows of personal data from the system to external entities (e.g., third parties).

UNAWARENESS AND UNINTERVENABILITY

What?

Unawareness and unintervenability threats occur when individuals are insufficiently informed, involved, or empowered with respect to the processing of their personal data.

Tell me more!

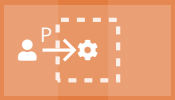
These threats may arise when there is (1) insufficient transparency (individuals are not aware of the collection or processing of their personal data or the personal data of others), (2) insufficient feedback (individuals are insufficiently informed about the privacy impact they may cause to others by using the system), and (3) insufficient intervenability (individuals cannot access or manage their personal data).

So what?

Unawaress and unintervenability are problematic because individuals are not informed about the potential implications of sharing personal data and cannot access or manage, withdraw, correct, or limit the processing.

Hotspots

Inbound user with personal data



There is an inbound flow from the user to the system in which personal data is transferred.

Inbound personal data

There is an inbound flow to the system in which personal data is transferred.

Inbound user

There is an inbound flow from the user to the system.

Storing

The system stores incoming data.

Retrieving

The system responds to data requests.

NON-COMPLIANCE

What?

Non-compliance threats arise when the system deviates from legislation, regulation, or standards and best practices, leading to the incomplete management of risk.

Tell me more!

When addressing potential privacy issues, also consider regulatory compliance, data lifecycle management, and cybersecurity risk. Pay specific attention to cases in which these aspects lead to privacy problems.

So what?

Violation of regulatory compliance obligations can lead to severe fines for the organization.

Hotspots

Processing personal data

The system processes incoming personal data and shares this with external entities.

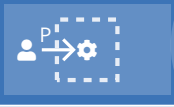
Processing

The system processes incoming data and provides this to another entity.

LINKED USER REQUESTS

Hotspot

INBOUND USER WITH PERSONAL DATA



Threat Source

ORGANIZATIONAL, EXTERNAL

User requests can be linked because they contain a unique identifier.

- ? Is there an identifier (unique in system/session) or dataset?
- ? Is there other data associated with that identifier?
- ? Is there previous data with the same identifier to which new data can be linked?

- Using an email address as an identifier enables the linking of all activities to the same individual, even across multiple services.
- An IP address can be used to link multiple visits to the same individual.
- All product views in a web shop are linked to the same user because they are logged in.

⚠ Unique identifiers facilitate the linking of new data items to a user profile, accumulating growing amounts of personal data associated with this profile. This can later lead to 'Identifying' threats.

ⓘ Linking is especially easy for authenticated users, as all requests in the same session are linked.


LINDDUN
GO

LINKABLE USER REQUESTS

Hotspot

INBOUND PERSONAL DATA

Threat Source

ORGANIZATIONAL, EXTERNAL

User requests can be linked because they contain attributes that can be combined into quasi-identifiers.

- ? Is there a set of attributes that can serve as an identifier?
- ? Is there other data sent together with that quasi-identifier?
- ? Is there existing data to link it to?

- A small set of locations can be used to uniquely link activity to a single user.
- A subset of attributes may be sufficient to uniquely link data to a particular individual.
- A browser fingerprint combines properties (OS, browser, display size, ...) that together are unique to a website visitor.

- ⚠ The use of quasi-identifiers enables the linking of new data items to a user profile to gather increasing amounts of personal data, even without unique identifiers.
- ⓘ Many requests contain a lot of different properties that, when combined, are unique to an individual.


LINDDUN
GO

LINKING THROUGH DISTINGUISHABLE PATTERNS

Hotspot

INBOUND USER

Threat Source

ORGANIZATIONAL, EXTERNAL

Patterns in the (meta)data contained in user requests can be used to link them to each other.

? Is the data from different individuals distinguishable?
? Is it possible to query data using distinguishable attributes?

- Unique timing patterns could be recognized to link the use of a service to the same user.
- Messages can be analyzed for patterns (e.g., writing style, timing) to link them to the same user.

⚠ When users are distinguishable from one another, user profiles can be constructed to collect growing amounts of personal data associated with each profile. This can later lead to 'Identifying' threats.

ⓘ Even data without clear attributes could contain patterns to allow distinguishing between different individuals.


LINDDUN
GO

LINKABLE DATASET

Hotspot

STORING/RETRIEVING

Threat Source

ORGANIZATIONAL, EXTERNAL

Stored personal data can be linked to individuals.

- ? Is there a set of attributes that can serve as an identifier?
- ? Is there other data sent together with that quasi-identifier?
- ? Is there existing data to link it to?

- Fine-grained raw data is stored that enables linking specific entries to individuals.
- Querying the average salary with a strict set of criteria can reveal the salary of an individual employee.
- Patterns in a person's writing style can be used to link multiple texts written by the same person.

- ⚠ The use of quasi-identifiers enables the linking of new data items to a user profile to gather increasing amounts of personal data, even without unique identifiers.
- ℹ Many requests contain a lot of different properties that, when combined, are unique to an individual.


LINDDUN
GO

PROFILING USERS

Hotspot

PROCESSING

Threat Source

ORGANIZATIONAL, EXTERNAL

Users can be profiled by analyzing their data for patterns.

? Are there patterns derivable from the data?
? Can (new) personal data be inferred from the linked data points?

- By applying sentiment analysis to faces in pictures, the emotional state of an individual can be derived.
- The frequency of data exchanges from a health monitoring device allows an adversary to infer a patient's medical condition.

- Deriving patterns from the data can facilitate the linking of data that was not intended to be linked.
- Timing patterns of messages can be used to link requests to construct profiles.

- The more data is collected and the more detailed it is, the easier it can become to discern patterns for linking.


LINDDUN
GO

IDENTIFIED USER REQUESTS

Hotspot

INBOUND USER WITH PERSONAL DATA

Threat Source

ORGANIZATIONAL

The incoming user requests contain data that directly reveals the user identity.

? Does data sent to the system (potentially) contain identity data?

- An online service requests full name and address during the registration process.
- The username for a service contains identity data (e.g., “firstname.lastname”).

- Identified data can severely amplify the impact of a future data breach.
- Depending on the context, the identity may reveal very sensitive attributes (e.g., health records).

- Users often need to provide identified data even when not essential for the functionality.
- Identified data requires stronger security measures.


LINDDUN
GO

IDENTIFIABLE USER REQUESTS

Hotspot

INBOUND USER

Threat Source

ORGANIZATIONAL

The user can be identified because the data in their requests can be used to infer who they are.

? Are requests or records sufficiently unique to differentiate them from those of a specific individual?

- User search queries, such as looking up nearby businesses or info about a rare illness, can be highly specific and may lead to identification.
- A person's consistent access at a particular time each week could link their visits even when they are not logged into their account.

⚠ Even without identity information, user actions or data may be very specific and unintentionally reveal the identity.

ⓘ The likelihood depends on how distinguishable an individual is from others.


LINDDUN
GO

IDENTIFIABLE DATA FLOWS

Hotspot

INBOUND PERSONAL DATA

Threat Source

ORGANIZATIONAL

Data sent to the system is sufficiently revealing to identify the user.

? Is there free-form user provided data that is received or processed by the system?

? Is data collected that may reveal the identifying information?

When an individual shares detailed data (such as location, employer, device type, etc.) in a feedback form, the provided information may be revealing enough to uniquely identify that person.

Inadvertently providing identifiable attributes in user-submitted data can lead to the unintentional identification of the individual.

The data subject is not necessarily the source of the provided data.


LINDDUN
GO

IDENTIFIERS IN DATA REQUESTS

Hotspot

INBOUND USER WITH PERSONAL DATA

Threat Source

ORGANIZATIONAL, EXTERNAL

Communication contains (quasi-)identifiers.

? Is there a distinctive identifier used during interactions or when referring to an individual's data?

? Can multiple attributes be combined to create a unique reference to an individual or their data?

- The (re)use of an email address facilitates easy combination with other data, leading to the identification of the individual.
- IP addresses in communication can be used to uniquely identify an individual.
- Browser fingerprinting entails the combination of various properties to create a unique identifier, serving as a pseudonym for the user.

⚠ Pseudonyms facilitate the aggregation of data on the same individual (see linking). Storing a substantial amount of data increases the possibility of identifying the individual behind it.

ⓘ Identifying individuals through identifiers is easy when these identifiers are reused across multiple services or in publicly available data.


LINDDUN
GO

IDENTIFIABLE DATASET

Hotspot

STORAGE

Threat Source

ORGANIZATIONAL, EXTERNAL

Stored data can be used to identify individuals.

? Can multiple attributes be combined to create a unique reference to an individual or their data?

? Is there a distinctive identifier used during interactions or when referring to an individual's data?

A dataset removes names and reduces addresses to cities. Nevertheless, a combination of various attributes (city, birth date, language preference, etc.) could still be adequate to identify individuals.

Pseudonyms facilitate the aggregation of data on the same individual (see linking). Storing a substantial amount of data increases the possibility of identifying the individual behind it.

Identifying individuals through identifiers is easy when these identifiers are reused across multiple services or in publicly available data.


LINDDUN
GO

NON-REPUDIATION OF SERVICE USAGE

Hotspot

IN/OUTBOUND USER

Threat Source

ORGANIZATIONAL, EXTERNAL

Users cannot deny having used a service because of authentication or logged access.

? Does the system record data affecting deniability?
? Does the data itself impact deniability claims?

- An account with a corporate email address eliminates the employee's deniability of having used that service.
- System administrators can access log files linking an entry in an internal complaint system to the individual employee.

- Identity information can magnify the impact.
- Depending on the context (e.g., medical, whistleblower), this can have a large impact on the data subject.

- If deniability is required, do not store the data at all or remove any attributable data.
- Avoid credentials with identity information.


LINDDUN
GO

NON-REPUDIATION OF SENDING

Hotspot

INBOUND USER

Threat Source

ORGANIZATIONAL

Users cannot deny having sent a message.

? Is the data digitally signed?
? Which keys are used for signing? Who has access to these keys to verify signatures?

- A digitally signed email prevents the user from later denying having written the message.
- A common spam countermeasure (DKIM) involves signing outgoing emails, this prevents users from denying the authenticity of leaked or stolen emails.

- Signatures provide strong non-repudiation, as they can also be verified by third parties.
- Append-only storage systems make it impossible for the data subject to later remove their personal data.

- Signed data applies not only to messages, but also to documents, requests, etc.


LINDDUN
GO

NON-REPUDIATION OF RECEIPT

Hotspot

OUTBOUND USER

Threat Source

ORGANIZATIONAL

Users cannot deny having received a message.

? Do (passive) interactions with the system (e.g., receiving a message) have side-effects (e.g., trigger transmissions, logging)?

? Is deniability of receipt a desired feature for the system?

- Read notifications serve as evidence that the user has opened/read the message.
- An individual's browser history may be used to substantiate claims about their online activities.
- Actions can be logged as evidence.

⚠ Some actions may trigger side-effects that impact deniability claims regarding those actions.

ⓘ These side-effects often happen implicitly or without user intervention.


LINDDUN
GO

NON-REPUDIATION OF STORAGE

Hotspot

STORAGE

Threat Source

ORGANIZATIONAL

Users cannot deny claims about data stored in non-repudiable storage.

? Is the data digitally signed?
? Which keys are used for signing? Who has access to these keys to verify signatures?

Data stored on a blockchain cannot be modified, eliminating the deniability of claims related to this data.

Signatures provide strong non-repudiation, as they can also be verified by third parties.
Append-only storage systems make it impossible for the data subject to later remove their personal data.

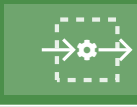
Signed data applies not only to messages, but also to documents, requests, etc.


LINDDUN
GO

NON-REPUDIATION OF HIDDEN DATA OR METADATA

Hotspot

PROCESSING



Threat Source

ORGANIZATIONAL

Hidden or metadata in a document prevent users from denying claims associated with it.

? Does stored or transmitted data have associated metadata?
? Are there embedded data or hidden patterns in the data or transmissions?
? Does this data lead to undesirable deniability issues?

- Author or revision metadata in documents prevents deniability.
- Data watermarked with hidden artifacts (uniquely linked to a person) can be used to track the person revealing or disclosing the data afterwards.
- Remote resources (e.g. image in email) are automatically loaded to track the user opening it.

- The unintentional inclusion of metadata with data or transmissions may impact deniability claims.
- Hidden/embedded data can prevent a user from denying claims about the data.

- This is also used as an explicit countermeasure to prevent people from sharing data.


LINDDUN
GO

DETECTABLE USERS

Hotspot

OUTBOUND FLOWS

Threat Source

EXTERNAL

Inferring the existence of a user from the system's response.

? Does the system show status messages (informational, warnings, errors) when retrieving data?

? Are the status messages distinct when an item (a file, user, …) does not exist compared to not having access rights?

A 'wrong password' error message reveals the existence of the account.

A firewall responding with 'port closed' reveals the existence of a device at the IP address.

Being able to detect the existence of certain items can be a stepping stone to security threats.

Simply knowing the existence of data may be sufficient to infer sensitive information.

Prevent information leakage by not revealing the existence of items in system responses.


LINDDUN
GO

DETECTABLE SERVICE USAGE

Hotspot

IN/OUTBOUND USER

Threat Source

EXTERNAL

Detecting communication between a service and its users.

? Can the communication be observed?
? Can information be inferred from the observed communications?

- Observing communication with a service to infer that a person is a user (e.g., adult website).
- Communication with a telemedicine service implies the user is a patient.
- Participation in the Tor network can be determined by observing traffic.

⚠ In sensitive contexts (medical, whistleblower) detecting service usage may have a severe impact on the user.

ⓘ Services like Tor conceal the destination but the utilization of Tor can still be detected.


LINDDUN
GO

DETECTABLE EVENTS

Hotspot

IN/OUTBOUND FLOWS

Threat Source

EXTERNAL

Detecting side effects or communications triggered by application events.

? Do actions in the system have side effects (e.g., saving a file, writing to a log, triggering other transmissions)?

? Are these side effects observable?

- Log files on a shared system reveal applications used or actions taken by other users.
- Deleted applications may leave behind traces (configuration, temporary files).
- When steganography is used to hide data, the increased file size may still indicate the existence of that hidden data.

⚠ Sensitive information may be deduced from observed side effects, such as communication.

ℹ Dummy traffic can be used to conceal actual events.


LINDDUN
GO

DETECTABLE RECORDS

Hotspot

RETRIEVING

Threat Source

EXTERNAL

Detecting the existence of records in a system.

? Does the system show status messages (informational, warnings, errors) when retrieving data?

? Are the status messages distinct when an item (a file, user, …) does not exist compared to not having access rights?

- An error message stating 'insufficient access rights' may inadvertently leak the existence of a specific record.
- An error message stating 'address already registered' when subscribing to a political newsletter reveals a current member.

- Being able to detect the existence of certain items can be a stepping stone to security threats.
- Simply knowing the existence of data may be sufficient to infer sensitive information.

- Prevent information leakage by not revealing the existence of items in system responses.


LINDDUN
GO

EXCESSIVELY SENSITIVE DATA COLLECTED

Hotspot

INBOUND PERSONAL DATA

Threat Source

ORGANIZATIONAL

The system acquires more sensitive or finegrained data than strictly necessary for its functionality.

- ? Is the data more sensitive than strictly necessary?
- ? Is the data more fine-grained than strictly necessary?
- ? Does the data encoding include additional (meta)data?

- Tracking a patient's weight is pertinent for dieting apps but not for a contact tracing application.
- A smart meter shares realtime measurements rather than the aggregated consumption.
- A camera application on a smartphone does not necessarily need to record the picture's location.

⚠ Processing excessively sensitive data amplifies the impact of a potential data breach, thereby increasing the consequences for the affected individuals.

ⓘ When designing the system, assess whether all the data is genuinely necessary for providing the system's functionality.


LINDDUN
GO

EXCESSIVE AMOUNT OF DATA COLLECTED

Hotspot

INBOUND PERSONAL DATA

Threat Source

ORGANIZATIONAL

The system acquires more data than strictly needed for its functionality.

- ? Is the amount of collected data necessary for the correct functioning of the system?
- ? Is the processing frequency necessary?
- ? Are there more data subjects involved than necessary?

- A generic service that is not age-restricted should not request a user's age.
- Recording patient weight on a weekly or monthly basis may suffice; collecting such information every half hour is unnecessary.
- Posts on social networks frequently include personal data about other individuals.

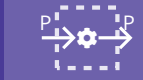
- ⚠ Regular data collection results in an increased dataset, potentially giving rise to additional privacy threats, such as data mining for patterns.
- ⓘ Evaluate whether regular data collection is necessary for the system's functionality.


LINDDUN
GO

UNNECESSARY DATA ANALYSIS

Hotspot

PROCESSING PERSONAL DATA



Threat Source

ORGANIZATIONAL

Data is further processed, analyzed, or enriched in a way that is not strictly necessary for the functionality.

? Is the data enrichment/analysis necessary for the system's functionality?

- A camera application on a smartphone does not need to perform face-based recognition or emotion detection.
- Analyzing a user's blog posts for language proficiency is unnecessary for blogging functionality.
- User profiles accumulate unnecessary details over time, tracking a broad range of actions or service usage that is not essential for the provided functionality.

⚠ Processing the data can be used to learn additional sensitive information.

ⓘ Evaluate which types of personal data processing are necessary for providing the system's functionality.

DD3 LINDDUN


LINDDUN
GO

UNNECESSARY DATA RETENTION

Hotspot

STORAGE

Threat Source

ORGANIZATIONAL

Data is stored for longer than needed.

? Is the data stored for longer time than necessary?

Retaining the email addresses of newsletter subscribers long after they have unsubscribed.

Storing data longer than needed serves no further purpose and increases the impact of a data breach.

Evaluate your storage policies. Consider how long you store personal data and whether you have a process to remove data you no longer need.


LINDDUN
GO

OVEREXPOSURE OF PERSONAL DATA

Hotspot

OUTBOUND PERSONAL DATA

Threat Source

ORGANIZATIONAL, EXTERNAL

Personal data is shared with more services or external parties than necessary.

- ? Is the data necessary for the recipient?
- ? Are there more parties involved than necessary?
- ? How accessible is the data (public/limited/private)?

- Location data from a navigation application is propagated to all the other applications (e.g., calendar, mail).
- Personal data is disclosed to other users of the service.
- In a medical application, while collecting patient weight data is deemed necessary, making such datasets publicly available would be unnecessary and harmful.

- ⚠ Overexposure of personal data may lead to unintended consequences, as others could reuse the data for unforeseen purposes.
- ℹ Carefully assess the necessity of sharing personal data and ensure that the involved parties genuinely require access to that data.


LINDDUN
GO

INSUFFICIENT TRANSPARENCY

Hotspot

INBOUND USER WITH PERSONAL DATA

Threat Source

ORGANIZATIONAL

Data subjects are insufficiently informed about the collection and processing of their personal data.

? Are data subjects insufficiently informed about the processing of personal data, including the purposes and methods of the processing involved?

- Data subjects are not aware of the identities of the third parties with whom their data will be shared.
- The privacy notice provided to the data subject was not presented in clear and plain language.
- Data subjects are unaware that traffic cameras collect not only number plates but also facial images.

⚠ Insufficient transparency may lead to data subjects being unaware that their personal data is utilized for certain purposes, especially if those purposes are different from what was initially indicated.

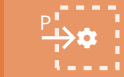
ⓘ Data subjects must also be informed on any 'indirect' data collection, i.e. from third parties.


LINDDUN
GO

INSUFFICIENT INFORMATION WHEN SHARING DATA OF OTHERS

Hotspot

INBOUND PERSONAL DATA



Threat Source

ORGANIZATIONAL

When sharing personal data of others, users are insufficiently informed about the further data processing.

? If a user shares personal data of others, is it clear what, why, and how that data is further processed?

- A user posting a picture on social media may not be aware that others in the picture are automatically tagged with a facial recognition system.
- Using a DNA testing service can entail sharing medical information about family members.
- A service invites a user to share their address book to find contacts on a service.

⚠ Users may not realize that they are unintentionally sharing personal data belonging to other individuals.

ⓘ While users are often informed about the consequences of sharing their own data, systems rarely inform them about the impact of sharing data of others.


LINDDUN
GO

INSUFFICIENT PRIVACY CONTROLS

Hotspot

INBOUND USER

Threat Source

ORGANIZATIONAL

Data subjects have insufficient controls to manage their preferences.

? Does the system enable the data subject to configure which personal data is processed and for what purposes?
? Can the data subject alter their preferences afterwards?

- The data subject is unable to set appropriate preferences on which data is shared and why.
- The data subject is unable to set their consent preferences for the processing of personal data.

⚠ Appropriate control mechanisms are required to record data subject preferences and keep track of how the data may be further processed.

- Privacy-friendly settings should be the default.
- Nudging can raise awareness and induce more privacy-preserving behavior.


LINDDUN
GO

INSUFFICIENT ACCESS

Hotspot

STORING

Threat Source

ORGANIZATIONAL

Data subjects do not have access to their personal data.

? Do data subjects lack the ability to access the personal data being collected, processed, stored, or disclosed about them?

- It is not possible for a data subject to request access, neither directly through the system nor indirectly through a helpdesk.
- The sensor data from a wearable is transmitted to a lifestyle tracking app, but the user cannot access statistics and information derived from their data.

⚠ Lack of access may violate the legal rights of data subjects.

ⓘ The right to access is not always absolute. Limitations may exist depending on applicable laws (e.g., trade secrets, rights of other data subjects).


LINDDUN
GO

INSUFFICIENT RECTIFICATION OR ERASURE

Hotspot

RETRIEVING

Threat Source

ORGANIZATIONAL

Data subjects cannot rectify or erase their personal data.

? Do data subjects have the ability to correct or delete their personal data?

- The data subject is unable to correct their personal data.
- When a data subject deletes their social media account, the account is disabled, but the actual data is not erased.
- A data subject is unable to update their home address after relocating.

⚠ Data subjects have the right to rectify incorrect personal data or request the removal of data that is no longer relevant or needed.

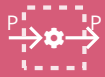
ⓘ Rectification or erasure can also be performed indirectly (e.g., through a customer service ticket).


LINDDUN
GO

NON-COMPLIANCE OF PROCESSING WITH APPLICABLE REGULATIONS

Hotspot

PROCESSING PERSONAL DATA



Threat Source

ORGANIZATIONAL

The processing of personal data by the system is not compliant with applicable privacy regulations.

- ? Will the system be used in jurisdictions with specific rules for personal data processing (e.g., the EU)?
- ? Does the system, or its processing activities, violate one or more rules in these applicable regulation(s)?

- The system processes information of EU citizens without a valid legal ground under GDPR.
- The system shares user information with third parties, violating 'Do Not Sell My Data' rights under the CCPA.

- ⚠ Non-compliance with local regulations may lead to hefty fines or other sanctions.
- ⚠ High-profile complaint cases or lawsuits may lead to negative media exposure and reputational damage.

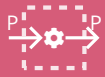
- ℹ Before processing any personal data, perform an assessment on the applicable regulations for your processing activities and system.


LINDDUN
GO

NON-ADHERENCE TO PRIVACY STANDARDS

Hotspot

PROCESSING PERSONAL DATA



Threat Source

ORGANIZATIONAL

The system is not compliant with privacy standards and best practices.

? Are there any (industry) specific privacy standards that are applicable to the system?
? Does the system adequately implement the principles and controls outlined in these standards?

- The system does not adhere to the best practices and principles outlined in the relevant ISO norms on data protection and privacy-by-design.
- Privacy risks are not classified and managed using a standardized methodology such as the NIST Privacy Framework.

⚠ Non-adherence to industry standards and best practices makes it more difficult to demonstrate compliance with applicable laws.

ⓘ Check whether there is industry-specific guidance on data processing for your sector (e.g., healthcare, manufacturing).


LINDDUN
GO

IMPROPER DATA LIFECYCLE MANAGEMENT

Hotspot

PROCESSING

Threat Source

ORGANIZATIONAL

Data is not properly managed throughout its entire lifecycle within the system.

- ? Is there a data lifecycle management policy defined for the data processed within the system?
- ? Does the policy outline clear principles for each phase of the data lifecycle (creation, storage, sharing and usage, archival, and destruction)?

- There is no clear policy or mechanism to enforce deletion of data that is no longer needed.
- The organizational roles and responsibilities surrounding data management in the system are not sufficiently defined.

⚠ Inadequate or nonexistent data lifecycle management can result in a loss of overview of the data within the system and its maintenance, posing concerns not only for privacy and data protection but also security and availability.

ⓘ Data lifecycle management is a continuous process that must be consistently carried out as long as the system is designed, developed, and used.


LINDDUN
GO

INSUFFICIENT SECURITY OF PROCESSING

Hotspot

PROCESSING

Threat Source

ORGANIZATIONAL, EXTERNAL

Data security measures and processes do not adhere to risk and security management best practices and standards.

- ? Is there an established process to manage security risks and identify the required countermeasures?
- ? Does the system incorporate the required countermeasures?
- ? Are the countermeasures aligned with industry standards and best practices?

- No security assessment was performed of the software.
- There are no processes in place to ensure software and services are kept up to date.
- The organization does not use appropriate access control mechanisms to limit access of employees to personal data.

- ⚠ The security of the system plays a crucial role in safeguarding the privacy of individuals whose data is processed. Personal data breaches can result in significant fines and reputational damage.

- ℹ Consider complementary methods like security threat modeling.
- ℹ Consider adhering to standards such as ISO27001 or the CIS Security Controls.


LINDDUN
GO