CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

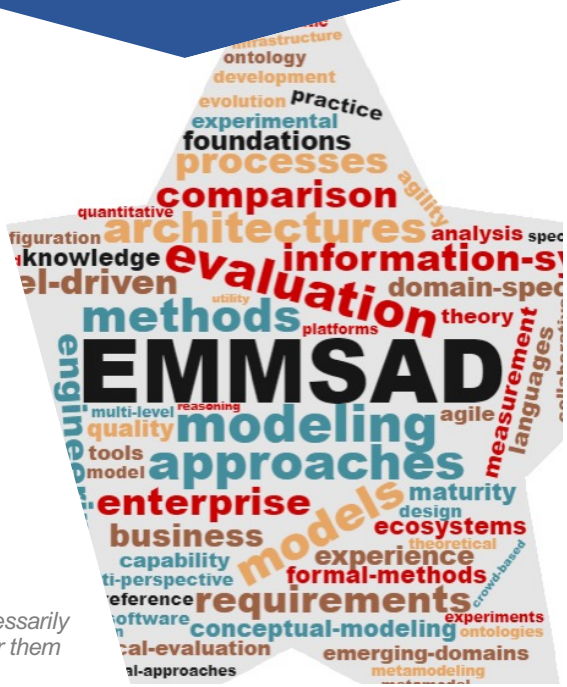
Forensic Readiness and Privacy: Towards Resolving Software Goal Conflict

Lukas Daubner and **Raimundas Matulevičius**

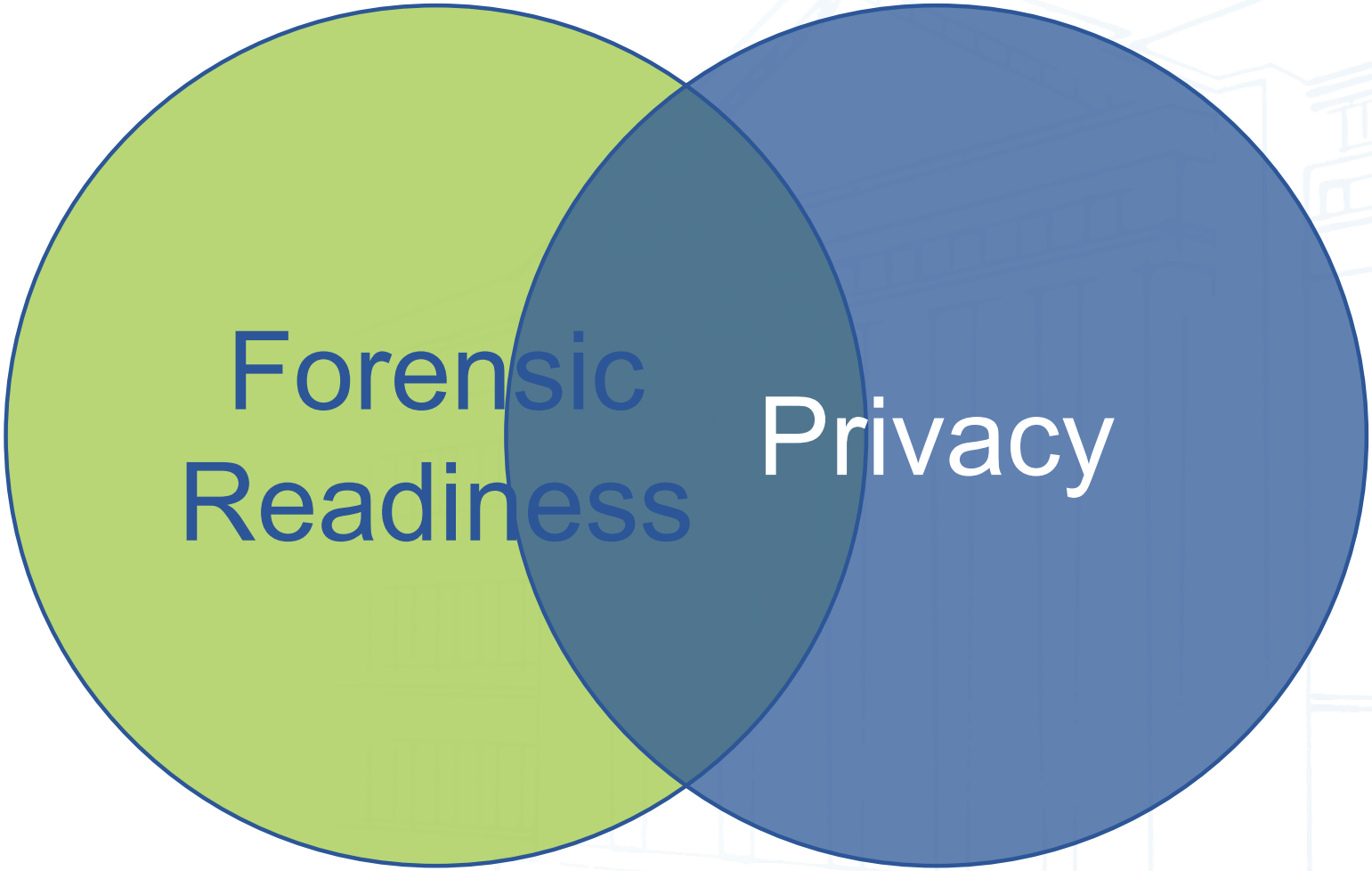
University of Tartu, Tartu Estonia

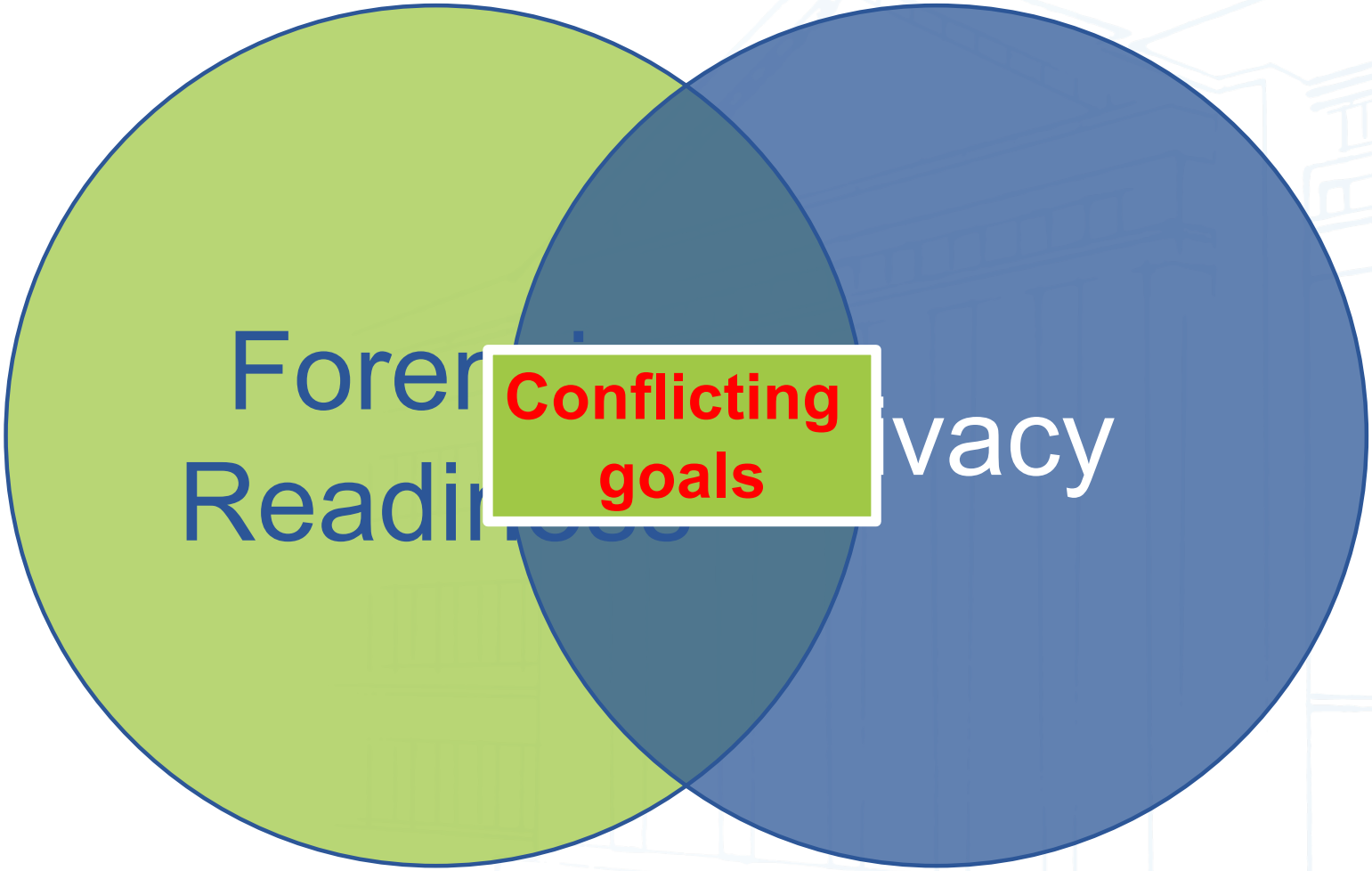
Jakub Harašta

Masaryk University, Brno, Czechia



Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them


Forensic
Readiness
Privacy


Conflicting goals

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Proactive steps towards incident investigation

- *What to do after an attack/accident/dispute*
- *Ensure useful data for the investigation*
- *Minimise the investigation costs*

Forensic Readiness

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Proactive steps towards incident investigation
  - *What to do after an attack/accident/dispute*
  - *Ensure useful data for the investigation*
  - *Minimise the investigation costs*

- Forensic-ready software (forensic-by-design)
  - *Prepare software during its development*
  - *Produce rich and forensically sound evidence for future use*

What to implement? → **Risk assessment**

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Article 5.1: Personal data shall be:

- *processed lawfully, fairly and in a transparent manner*
- *collected for a specified, explicit and legitimate purposes*
- *adequate, relevant and limited to what is necessary*
- *accurate and, where necessary, kept up to date*
- *kept in a form which permits identification of data subjects for no longer than is necessary*

Article 16: Right to rectify personal data

- *Does it mean that the evidence can be changed?*

Article 17: Right to be forgotten

- *Possible deletion of potential evidence?*

Article 22: Limitation of automated decision-making and profiling

- *How to process the high data volumes?*

GDPR

€1,2 Billion Questions

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Does forensic-ready software infringe on privacy?

- *Monitoring and tracing*
- *Collected to be "handy in future"*
- *Evidence used against the subject (disputes)*

Can the forensic-ready software be justified?

- *Not being an excuse for invasion of privacy*

Can forensic-ready software not infringe on privacy?

- *Respect the privacy, but remain vigilant*

Goal Modelling

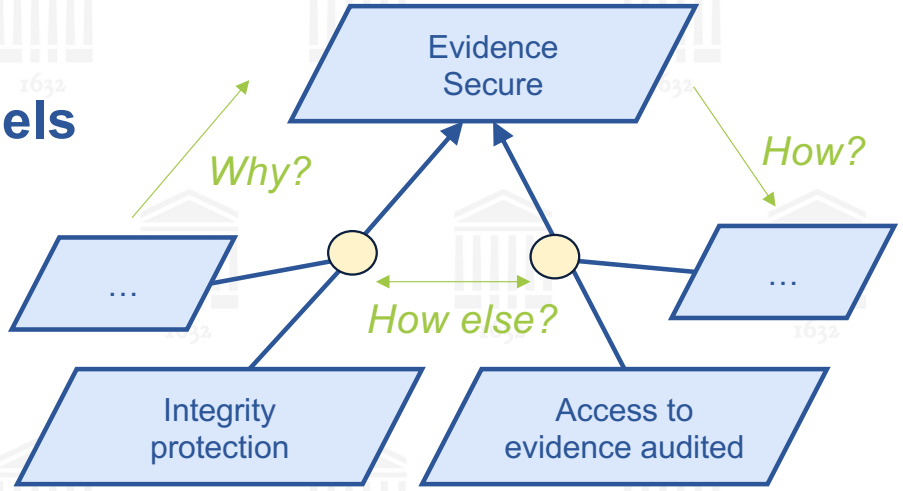
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Represent the two qualities as **goal models**

- *Objectives the system should meet*
- *Refinement towards requirements*
- *Compositions and alternatives*
- *Visual models*

Analyse relationships

- *Conflicting goals*
- *Resolution strategies*



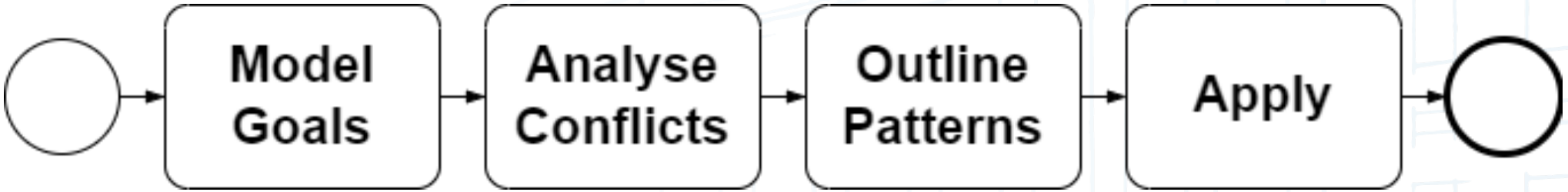
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Research question

*How to resolve the conflicts between the goals of **forensic readiness** and the **goals of privacy**?*

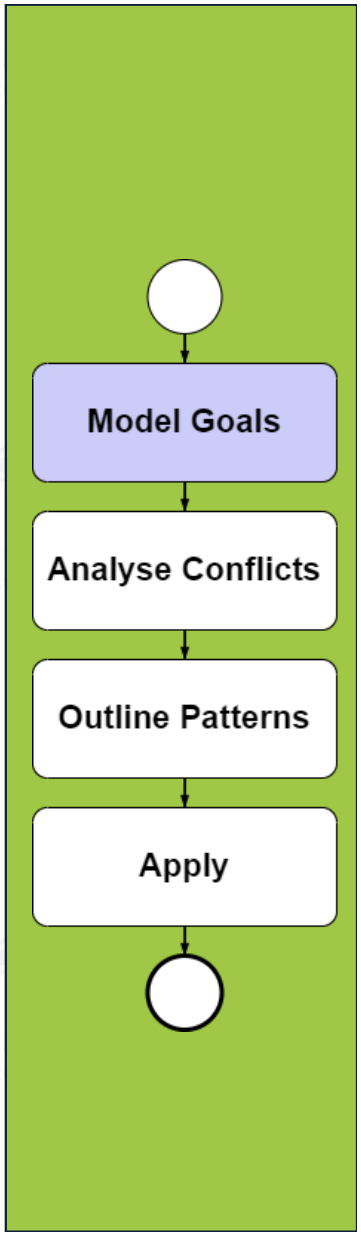
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Research method



GDPR Goal Model

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia



Representative of privacy legislation

- *Only articles 5-23 in scope*

Goals derived from articles

- *Top-down on „how“ to satisfy them*
- *Bottom-up on a common „why“*
- *Limited to sub-paragraph level*

Forensic Readiness Goal Model

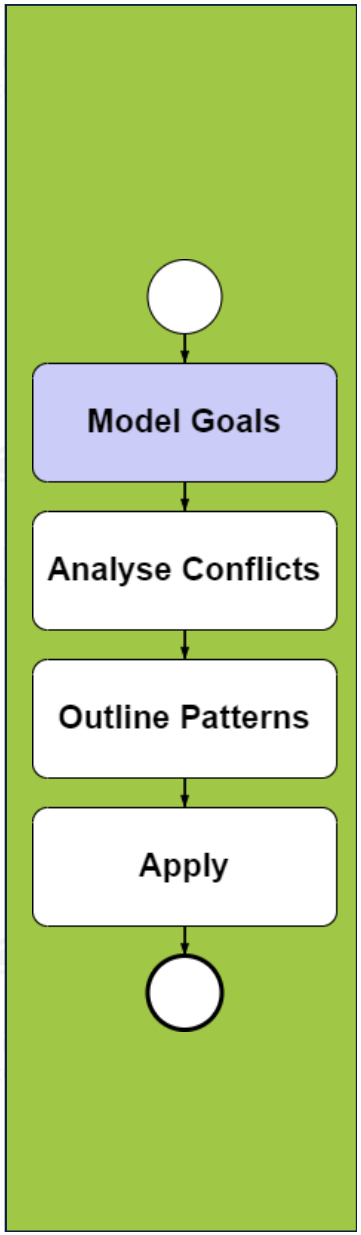
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Rowlingsons's Ten-step guide

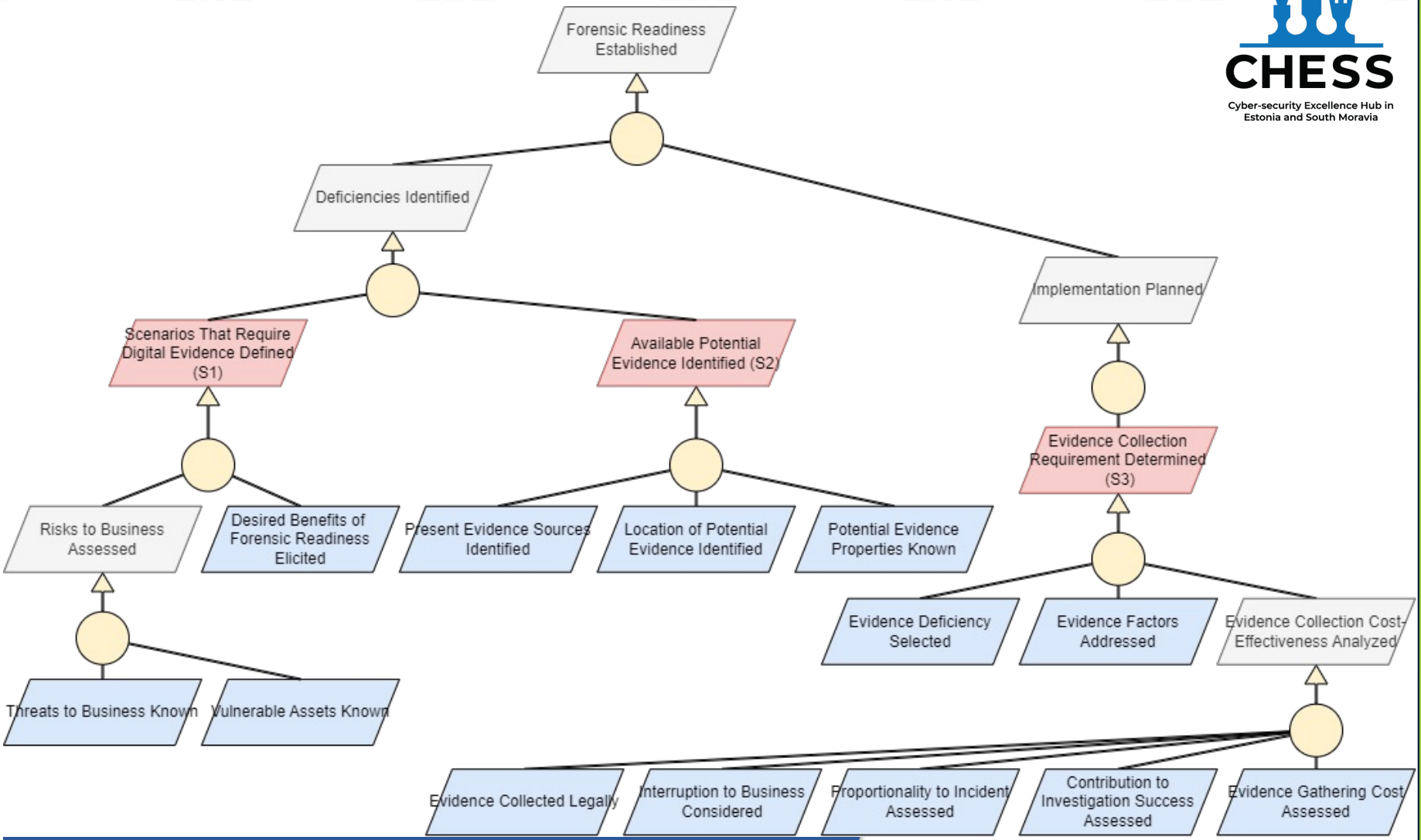
- *Well-known implementation guideline*
- *Lack of detailed legislation*

Goals derived from the ten steps

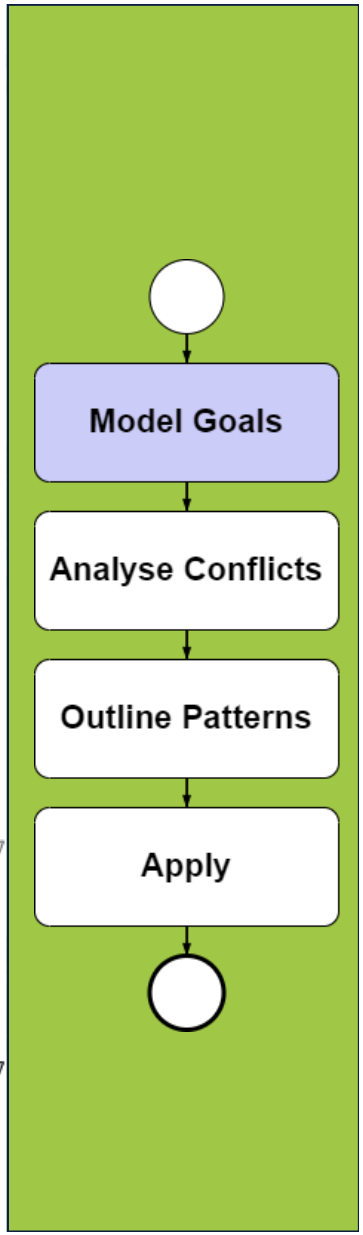
- *Top-down on step content*
- *Bottom-up on a common „why"*



Rowlingson, R.: A ten step process for forensic readiness. Int. J. Digit. Evid. 2 (2004)



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

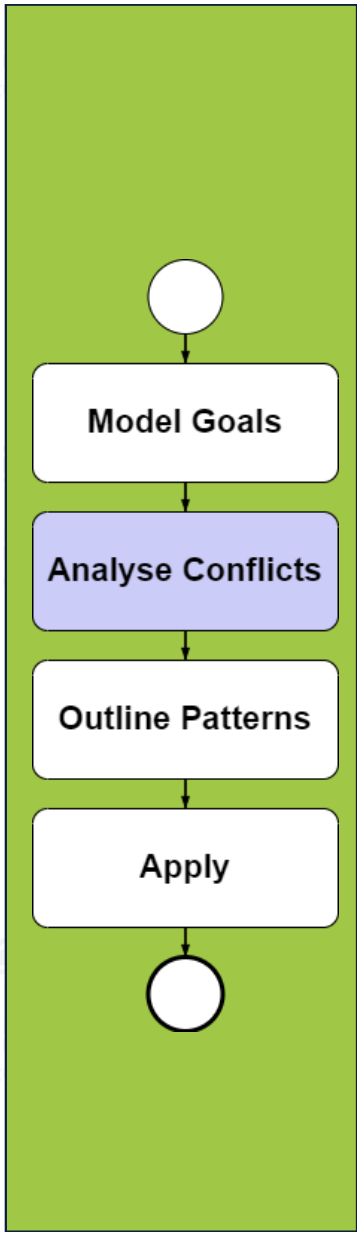
Goal Conflict Analysis

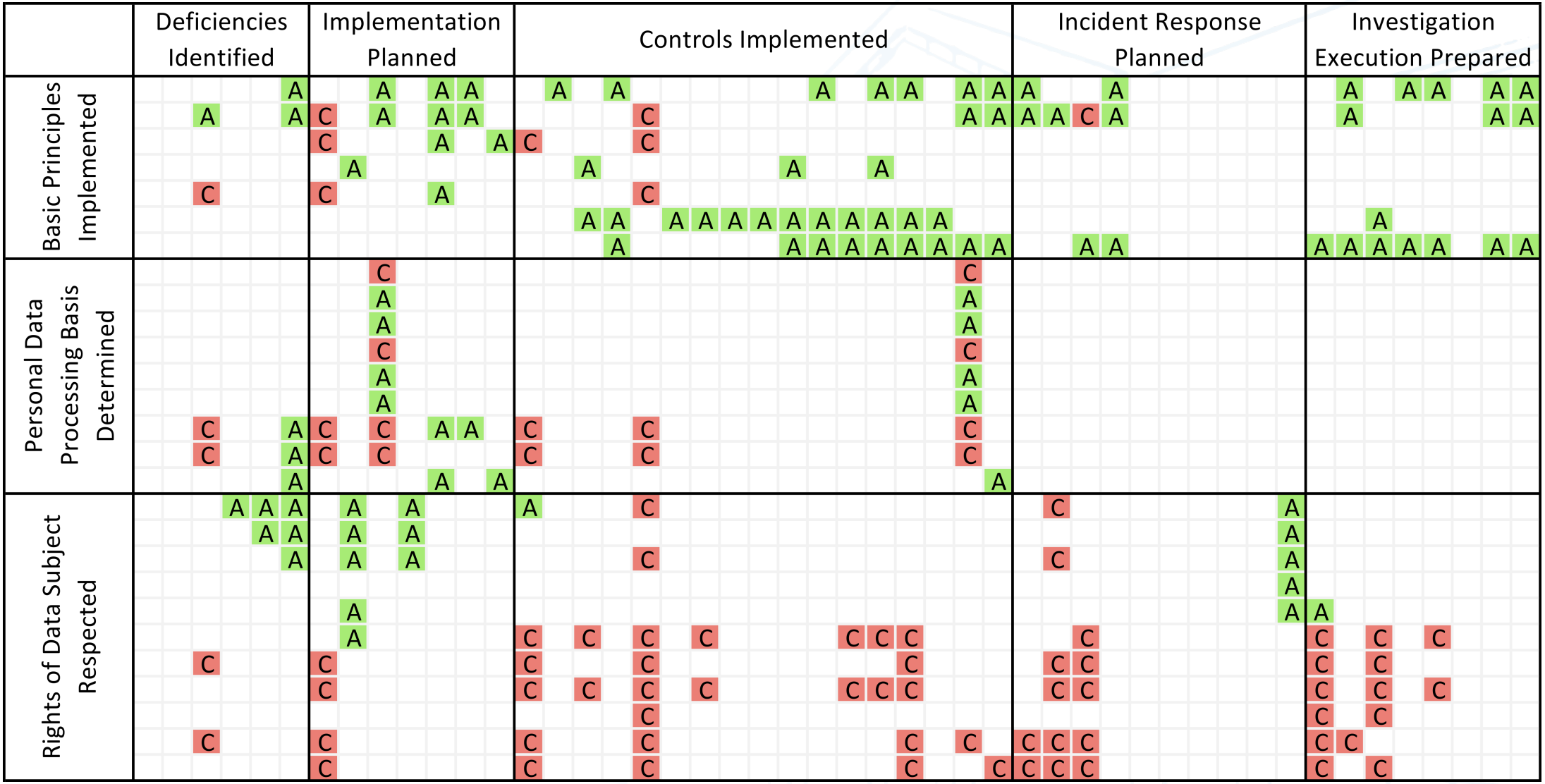
Goals selected and plotted into a matrix

- Assessed each cell
  - *Conflict*
  - *Alignment*
  - *No relationship*

Patterns emerged from the matrix

- Formulated with
  - *Problem description*
  - *General resolution outline*
- Reviewed from a legal perspective




Deficiencies Identified
Implementation Planned
Controls Implemented
Incident Response Planned
Investigation Execution Prepared
Basic Principles Implemented
Personal Data Processing Basis Determined
Rights of Data Subject Respected

Conflict Patterns

Basis (Art. 6)

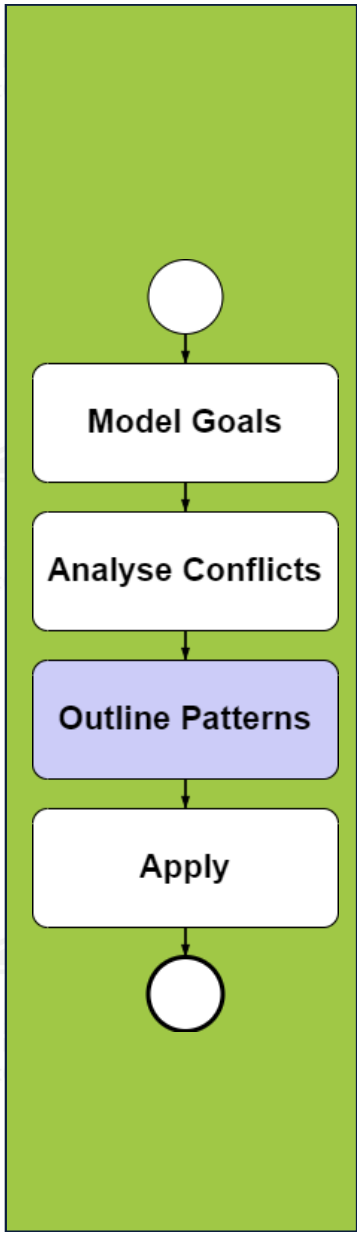
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Some data processing bases are not suitable

- Consent – can be revoked at any time
- Vital interest – data can be used against the subject

Resolution

- Use only suitable bases (e.g., contract)
- Legal obligation
  - *With explicitly specified regulation (e.g., cybersecurity)*
- Legitimate interest
  - *Based on, and appropriate to risks*



Conflict Patterns

Limited Retention (Art. 5.1.e)

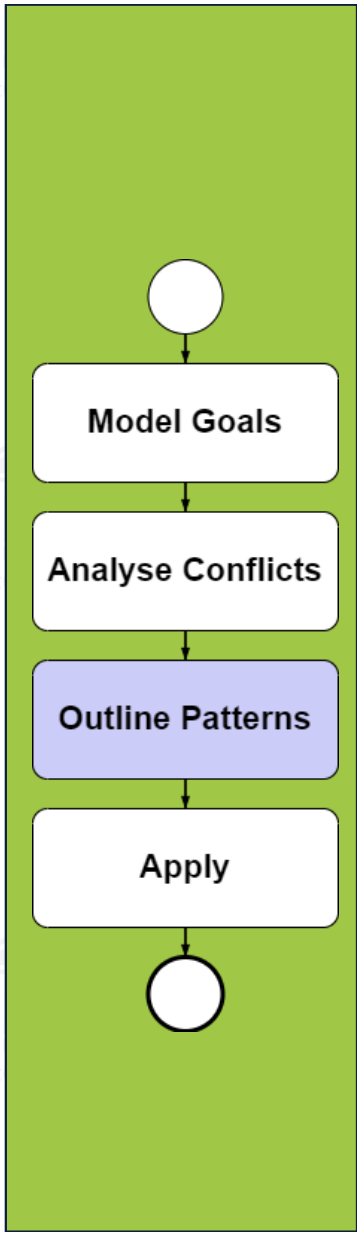
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

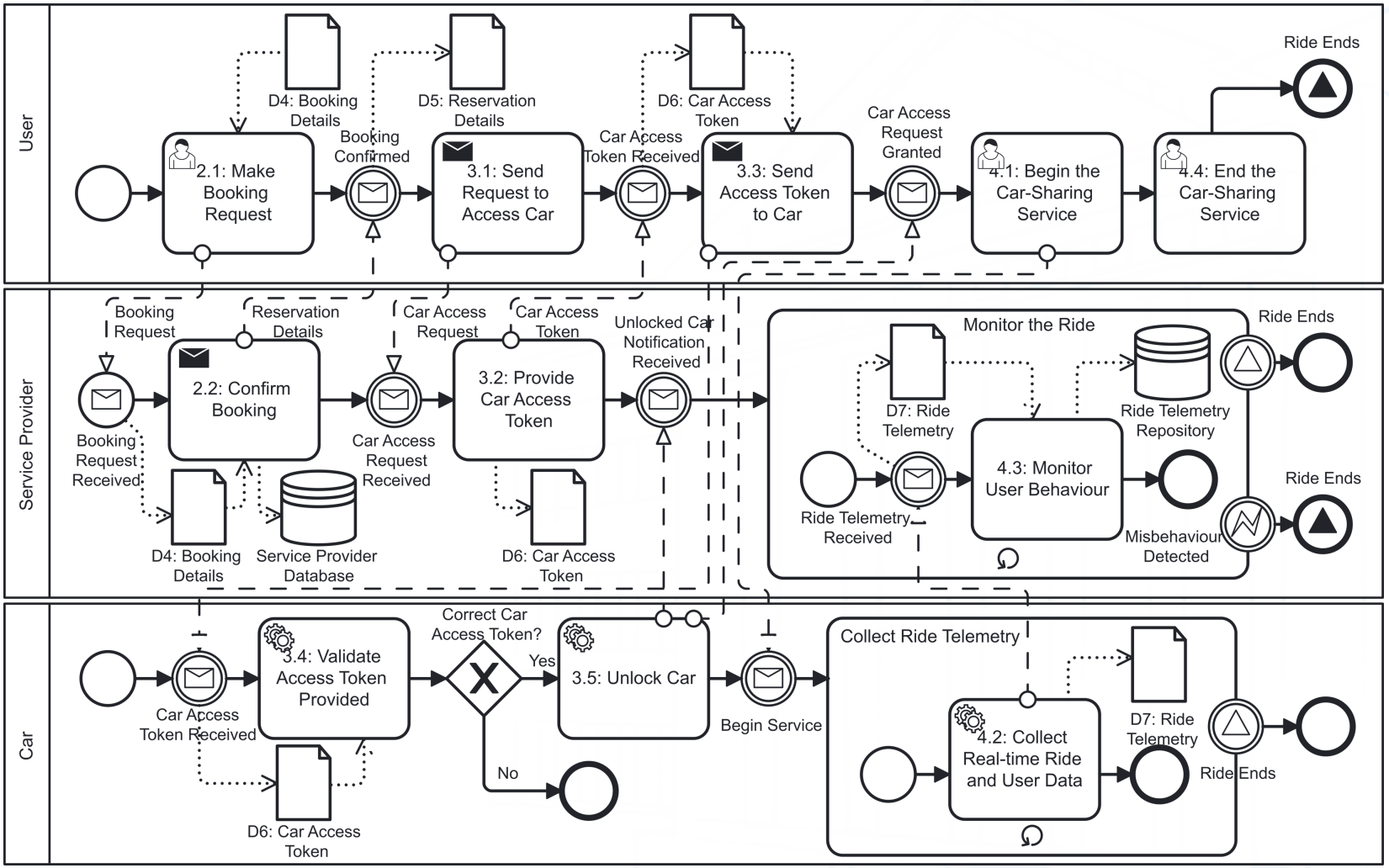
Data cannot be stored indefinitely

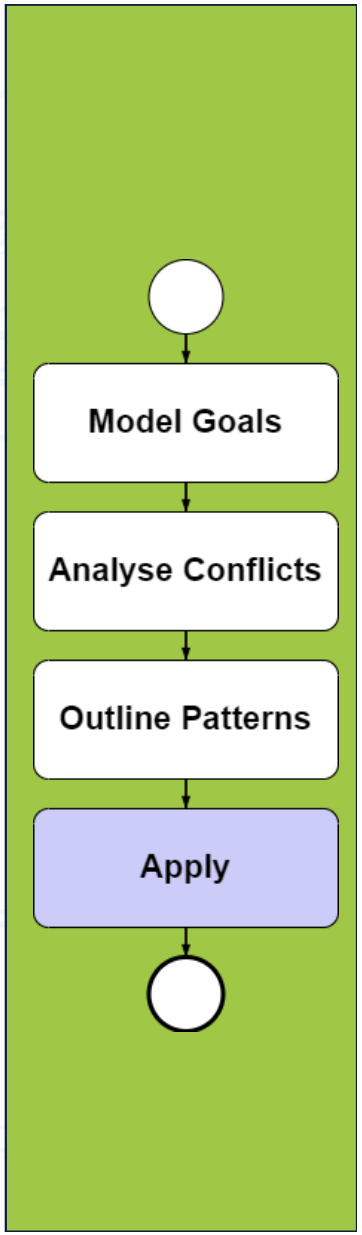
- Not practical and not justifiable
- Diminishing returns in investigating long-past incidents

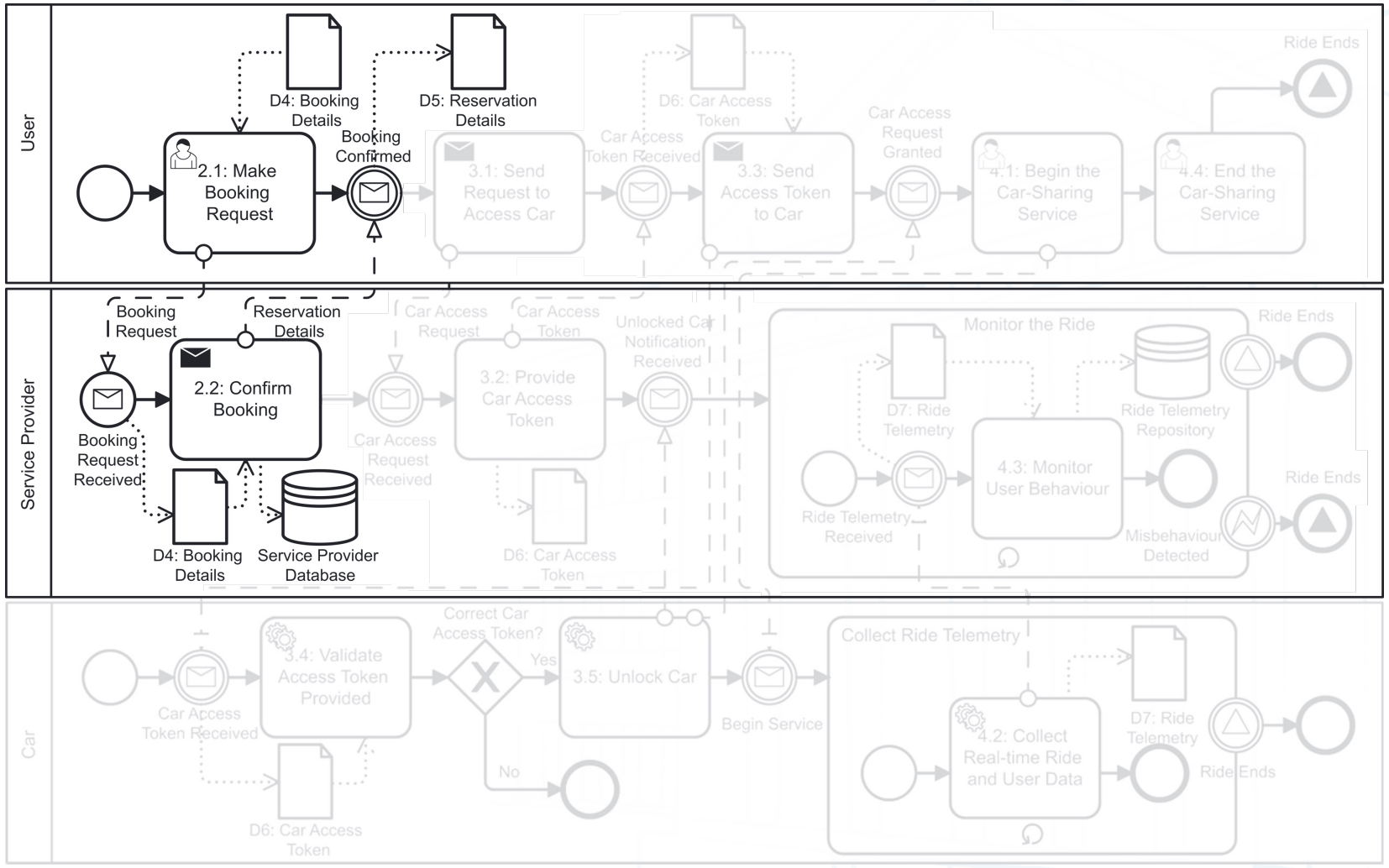
Resolution

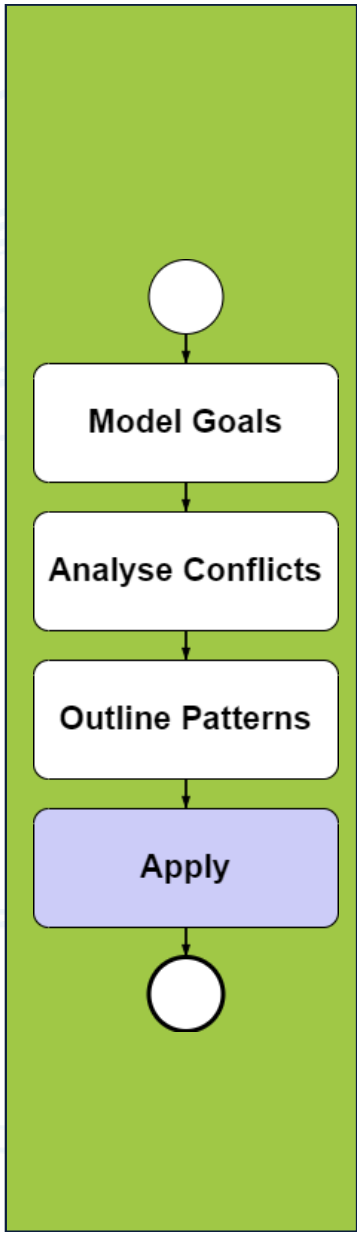
- Establish a feasible investigation period
- Based on specific scenarios
- Delete data afterwards
  - *Effectively, when not useful enough*

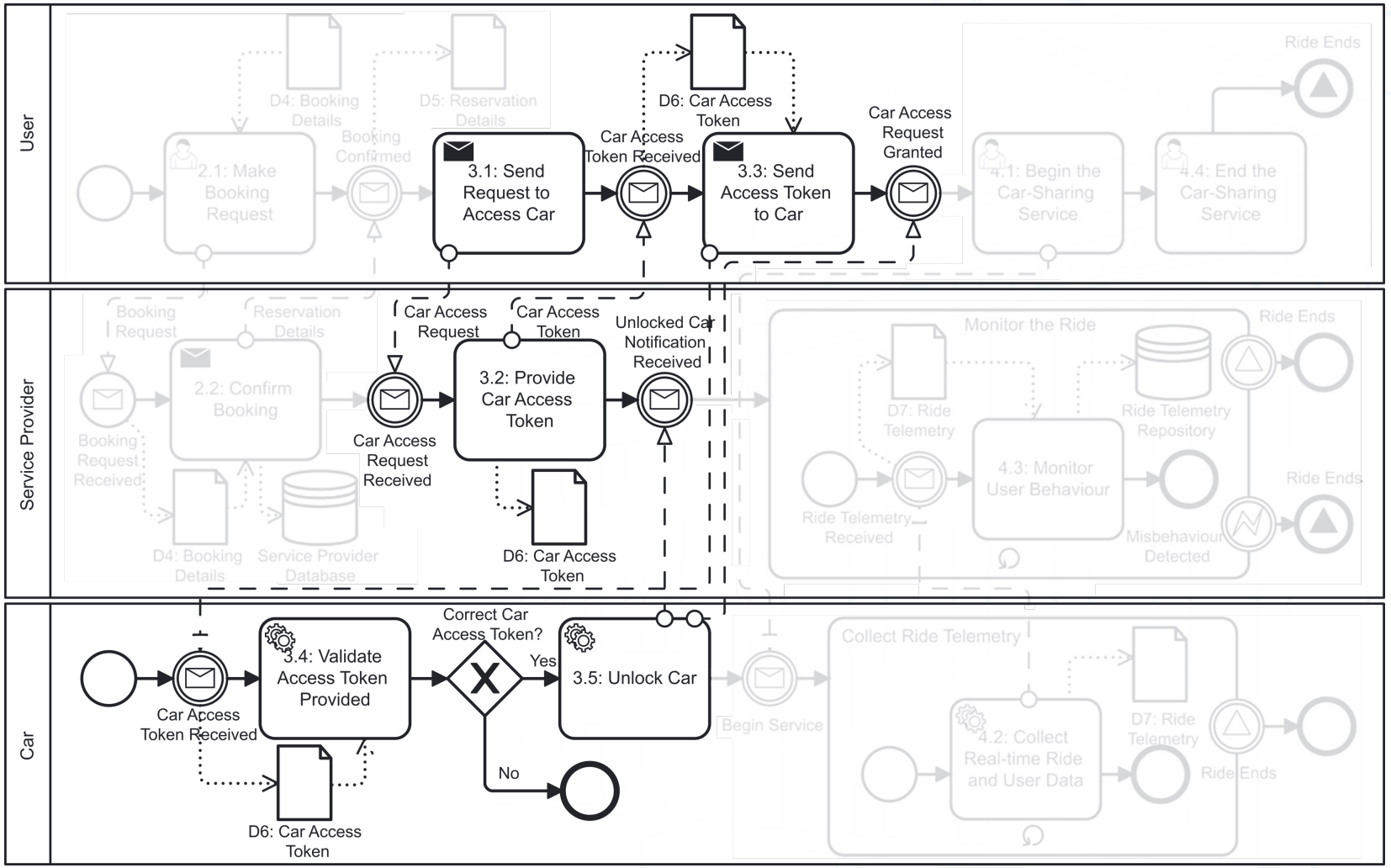


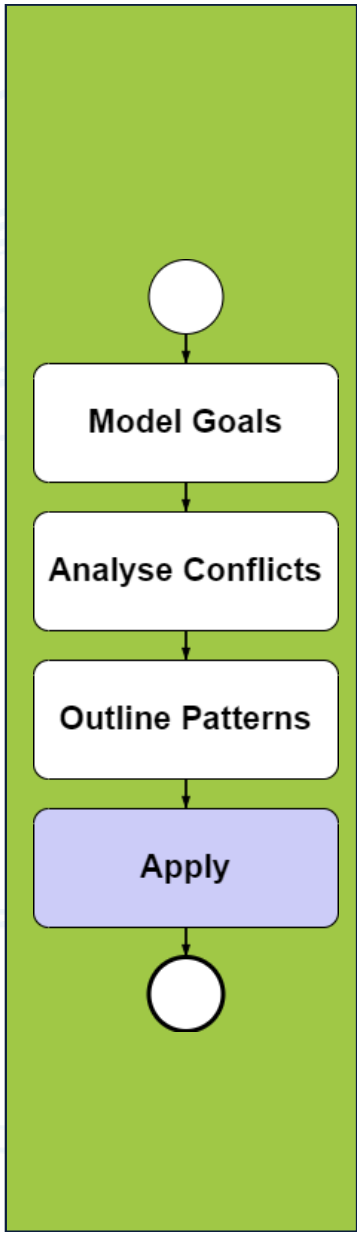

User
Service Provider
Car
D4: Booking Details
D5: Reservation Details
D6: Car Access Token
Ride Ends
2.1: Make Booking Request
Booking Confirmed
3.1: Send Request to Access Car
Car Access Token Received
3.3: Send Access Token to Car
Car Access Request Granted
4.1: Begin the Car-Sharing Service
4.4: End the Car-Sharing Service
Booking Request
Reservation Details
Car Access Request
Car Access Token
Unlocked Car Notification Received
2.2: Confirm Booking
3.2: Provide Car Access Token
Booking Request Received
Car Access Request Received
D4: Booking Details
Service Provider Database
D6: Car Access Token
Monitor the Ride
D7: Ride Telemetry
Ride Telemetry Repository
Ride Telemetry Received
4.3: Monitor User Behaviour
Misbehaviour Detected
Ride Ends
Correct Car Access Token?
Yes
No
3.4: Validate Access Token Provided
3.5: Unlock Car
Car Access Token Received
D6: Car Access Token
Begin Service
Collect Ride Telemetry
4.2: Collect Real-time Ride and User Data
D7: Ride Telemetry
Ride Ends

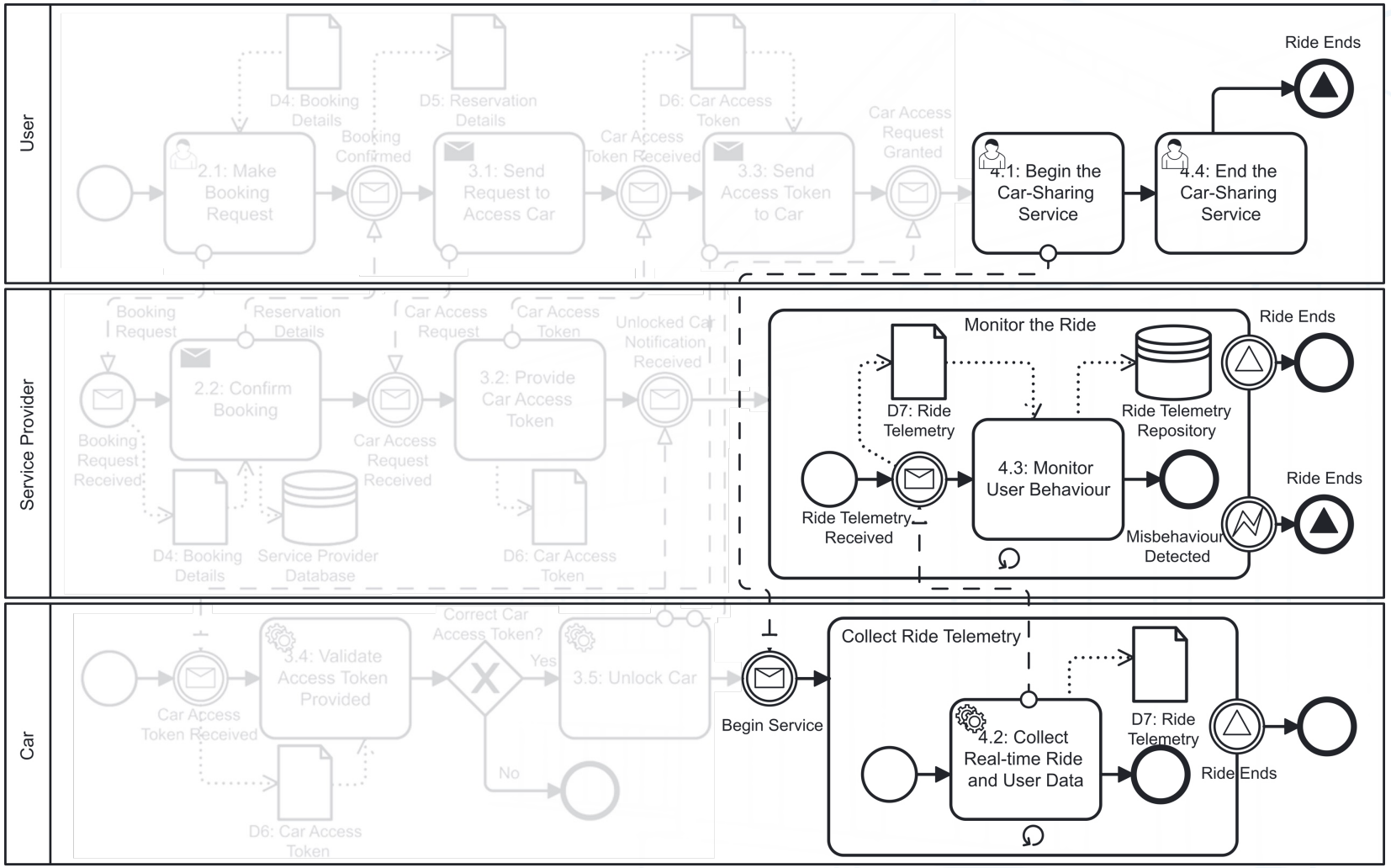

Model Goals
Analyse Conflicts
Outline Patterns
Apply

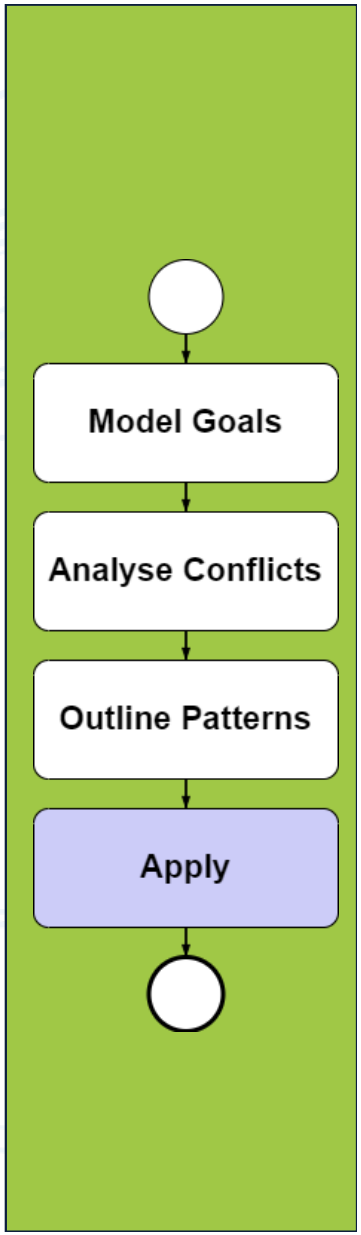

User
D4: Booking Details
D5: Reservation Details
2.1: Make Booking Request
Booking Confirmed
3.1: Send Request to Access Car
D6: Car Access Token
Car Access Token Received
3.3: Send Access Token to Car
Car Access Request Granted
4.1: Begin the Car-Sharing Service
4.4: End the Car-Sharing Service
Ride Ends
Service Provider
Booking Request
Reservation Details
2.2: Confirm Booking
Booking Request Received
D4: Booking Details
Service Provider Database
Car Access Request
Car Access Request Received
Car Access Token
3.2: Provide Car Access Token
D6: Car Access Token
Unlocked Car Notification Received
Monitor the Ride
D7: Ride Telemetry
Ride Telemetry Repository
4.3: Monitor User Behaviour
Ride Telemetry Received
Misbehaviour Detected
Ride Ends
Car
Car Access Token Received
3.4: Validate Access Token Provided
D6: Car Access Token
Correct Car Access Token?
Yes
No
3.5: Unlock Car
Begin Service
Collect Ride Telemetry
4.2: Collect Real-time Ride and User Data
D7: Ride Telemetry
Ride Ends


Model Goals
Analyse Conflicts
Outline Patterns
Apply


User
Service Provider
Car
2.1: Make Booking Request
Booking Confirmed
3.1: Send Request to Access Car
Car Access Token Received
3.3: Send Access Token to Car
Car Access Request Granted
4.1: Begin the Car-Sharing Service
4.4: End the Car-Sharing Service
Ride Ends
D4: Booking Details
D5: Reservation Details
D6: Car Access Token
Booking Request
Reservation Details
2.2: Confirm Booking
Booking Request Received
Car Access Request
Car Access Token
3.2: Provide Car Access Token
Car Access Request Received
Unlocked Car Notification Received
D4: Booking Details
Service Provider Database
D6: Car Access Token
Monitor the Ride
D7: Ride Telemetry
Ride Telemetry Repository
4.3: Monitor User Behaviour
Ride Telemetry Received
Misbehaviour Detected
Ride Ends
Car Access Token Received
3.4: Validate Access Token Provided
Correct Car Access Token?
Yes
No
3.5: Unlock Car
D6: Car Access Token
Collect Ride Telemetry
Begin Service
4.2: Collect Real-time Ride and User Data
D7: Ride Telemetry
Ride Ends


Model Goals
Analyse Conflicts
Outline Patterns
Apply


User
Service Provider
Car
D4: Booking Details
D5: Reservation Details
D6: Car Access Token
2.1: Make Booking Request
Booking Confirmed
3.1: Send Request to Access Car
Car Access Token Received
3.3: Send Access Token to Car
Car Access Request Granted
4.1: Begin the Car-Sharing Service
4.4: End the Car-Sharing Service
Ride Ends
Booking Request
Reservation Details
Car Access Request
Car Access Token
Unlocked Car Notification Received
2.2: Confirm Booking
3.2: Provide Car Access Token
Booking Request Received
Car Access Request Received
D4: Booking Details
Service Provider Database
D6: Car Access Token
Monitor the Ride
D7: Ride Telemetry
Ride Telemetry Repository
Ride Telemetry Received
4.3: Monitor User Behaviour
Misbehaviour Detected
Ride Ends
Car Access Token Received
3.4: Validate Access Token Provided
Correct Car Access Token?
Yes
No
3.5: Unlock Car
D6: Car Access Token
Begin Service
Collect Ride Telemetry
4.2: Collect Real-time Ride and User Data
D7: Ride Telemetry
Ride Ends


Model Goals
Analyse Conflicts
Outline Patterns
Apply

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

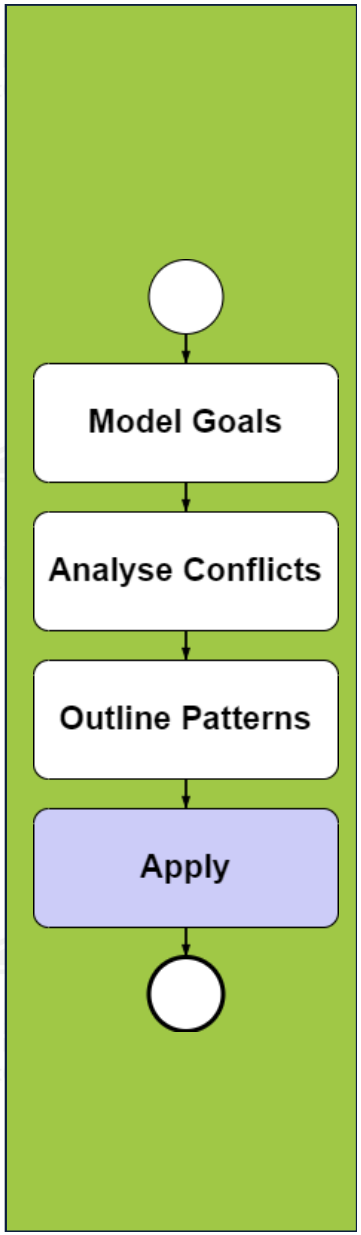
Based on risk-based methodology

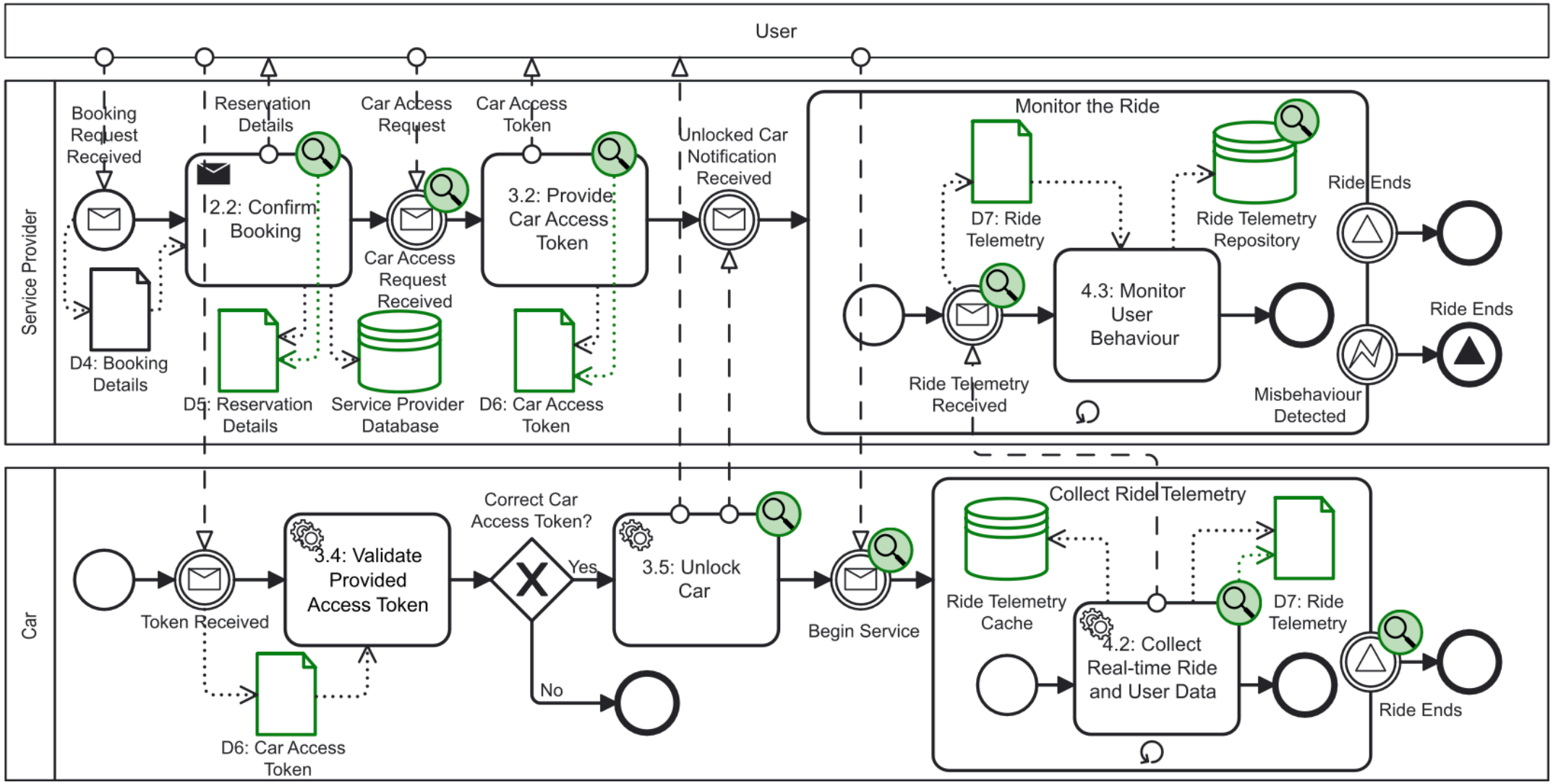
- *Forensic-Ready Information Systems Security Risk Management (FR-ISSRM)*

Scenario enhancements

- *Enrichment of ride telemetry*
  - *Investigation of car theft and access token misuse*
  - *Adding potential evidence*
- *Remote car data storage*
  - *Investigation of car theft, supporting evidence release*
  - *Preservation of potential evidence*

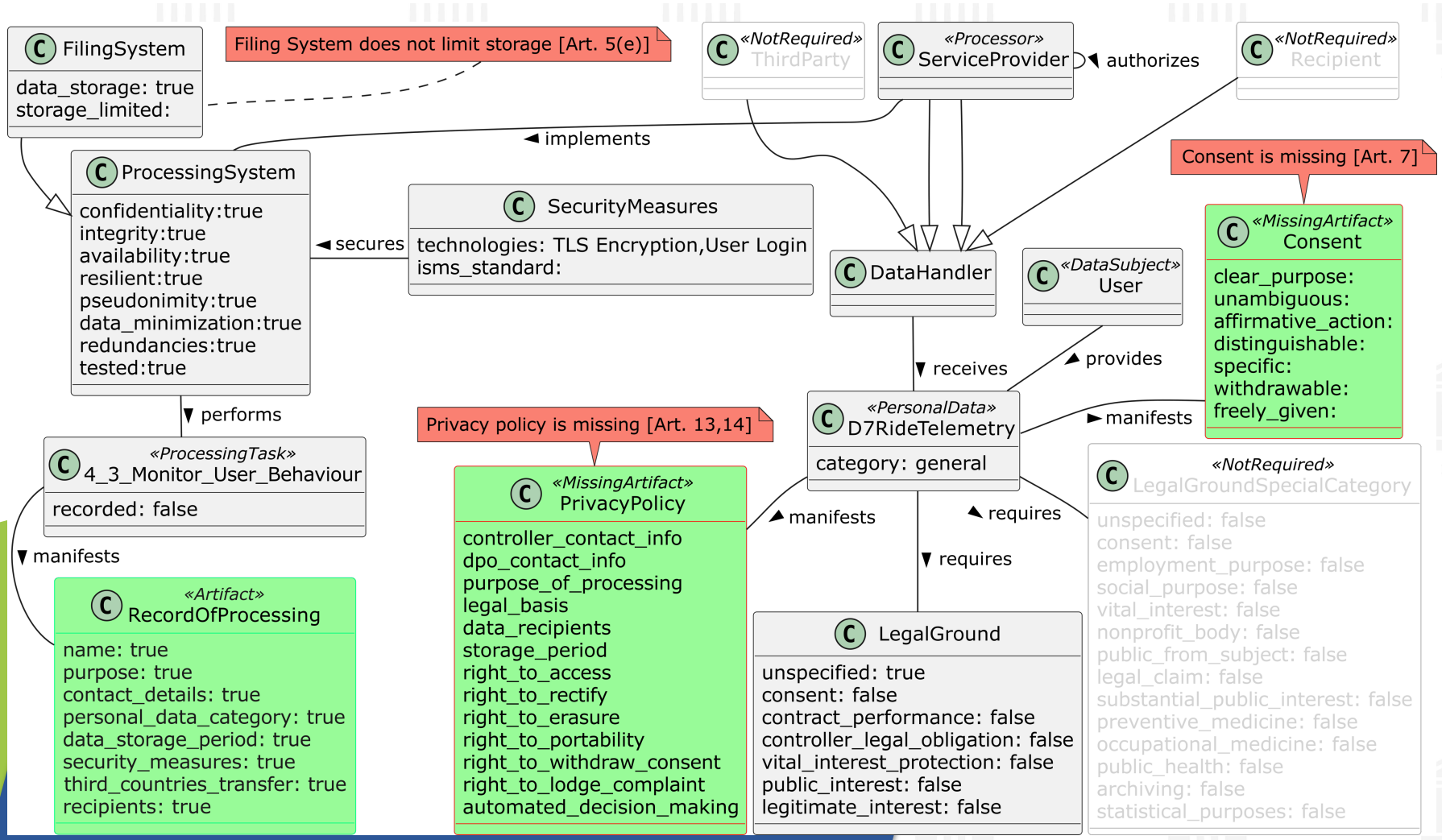
Forensic Readiness Design



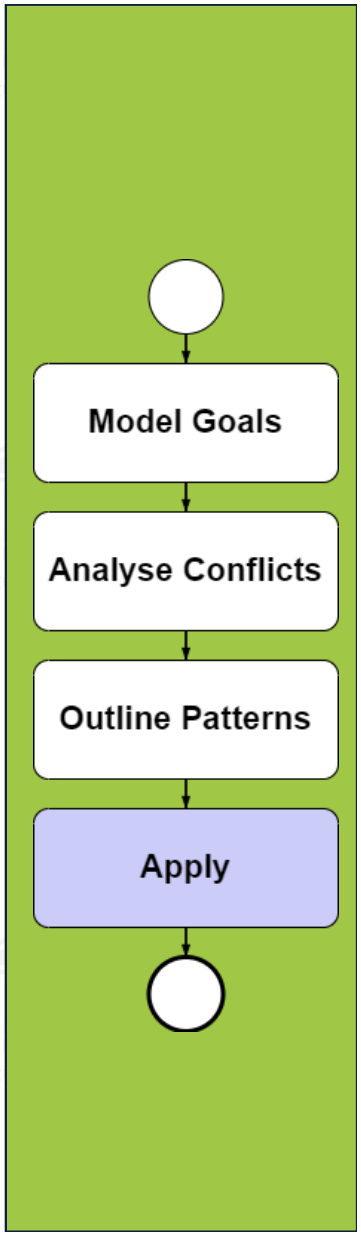


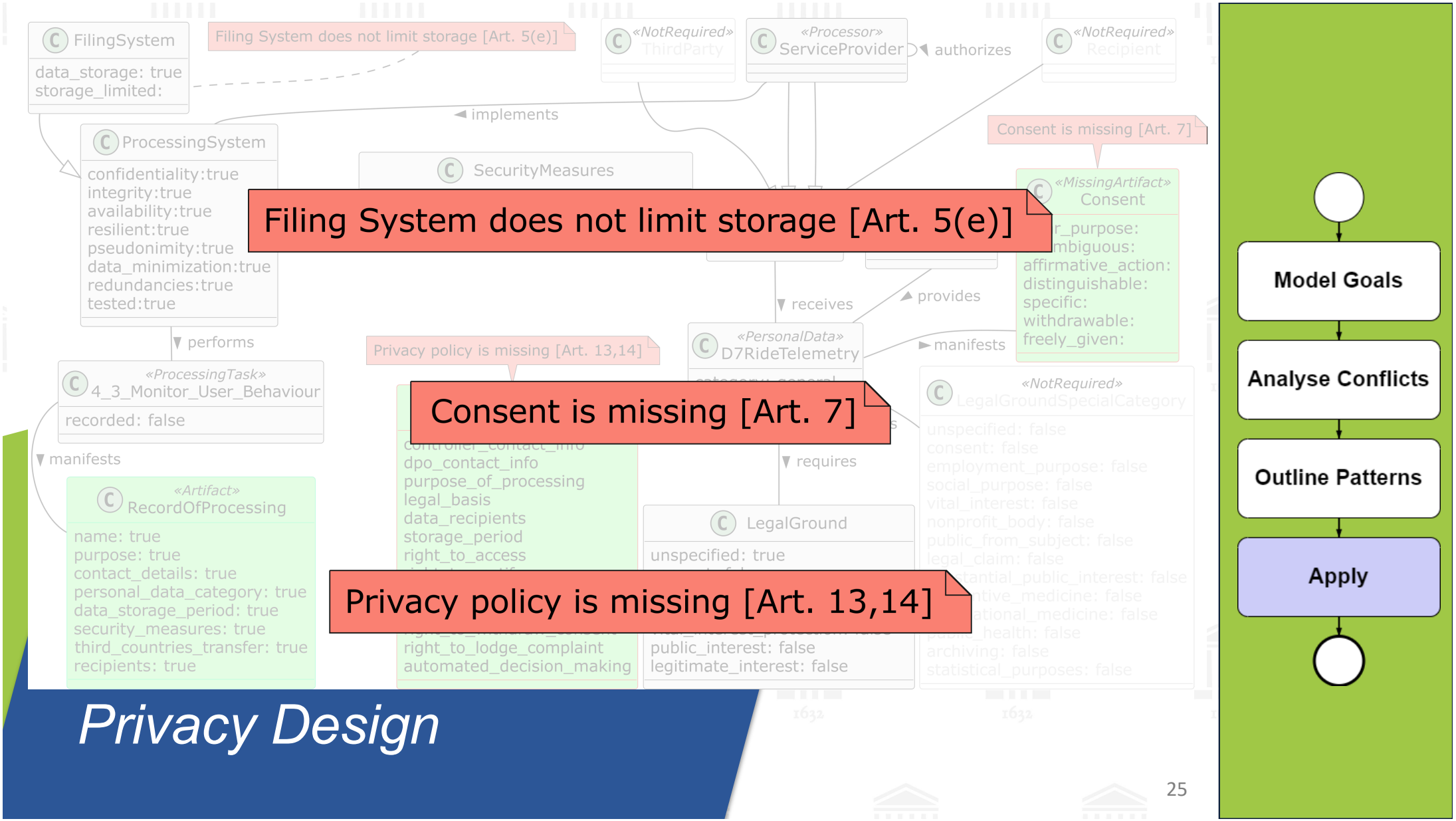
Forensic Readiness Design

https://freas-tools.github.io/wiki/



Privacy Design





Privacy Design

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Missing basis and consent

- Basis (Art. 6)
- Ride telemetry processed on legitimate interest (Art. 6.1.f)

Proportional to explicitly formulated risks

- *e.g., car theft*
- Legal obligation also plausible (Art. 6.1.c)

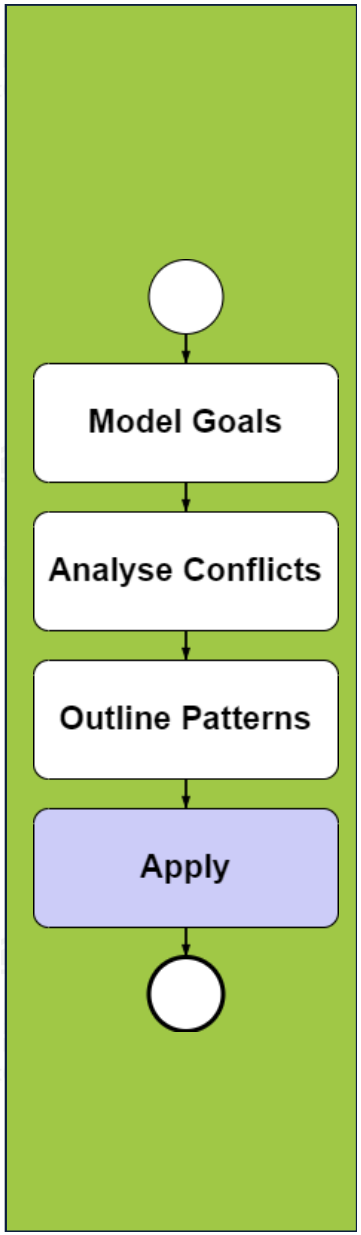
Data storage is not limited

- Limited Retention (Art. 5.1.e)
- Ride telemetry stored for one year

Reasonable window for investigation

- *Diminishing returns after year*
- Anonymised afterwards

Conflict Resolution



Answer to Research Questions

How to resolve the conflicts between the goals of forensic readiness and the goals of privacy?

Assessment of goal models

Conflict patterns encapsulating resolutions

- *Avoiding unsuitable alternatives*
- *Purpose rooted in risks*
- *Acceptable limitations*

Limited scope

- *GDPR articles*
- *High-level goals*

Conclusion

Forensic readiness and privacy can coexist

- *Identified as aligning with goals*

Goal modelling shown useful in reconciliation

- *Further work needed for fine-grained goals*

Conflict patterns

- *Guiderails for implementation*

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

THANK YOU

https://infosec.cs.ut.ee/
https://chess-eu.cs.ut.ee/

Co-funded by the European Union

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them