Thank You to Our Sponsors and Hosts!

OWASP
NEW
ZEALAND
owasp.org.nz

AUT
UNIVERSITY
TE WĀNANGA ARONUI O TAMAKI MAKAU RAU

DEFEND™

fastly®

QUANTUM
SECURITY

DATACOM

IriusRisk

snyk

dta
Defence Technology Agency

planit anNRIcompany

FIGHTING
FOR FAIR
FOR KIWI BUSINESS

safeadvisory.

Without them, this Conference couldn't happen.

WHAT

BS ISO 31700-1:2023

INTERNATIONAL STANDARD

ISO 31700-1

First edition
2023-01-31

Consumer protection — Privacy by design for consumer goods and services —

Part 1: High-level requirements

Protection des consommateurs — Respect de la vie privée assuré dès la conception des biens de consommation et services aux consommateurs —

Partie 1: Exigences de haut niveau

TERMS

- Personal information (NZ/AUS)
- Personal data (EU)
- Personally identifiable information (US)

PRIVACY BY DESIGN

1. Proactive not reactive, preventative not remedial
2. Privacy as the default
3. Privacy embedded into design
4. Full functionality– positive-sum, not zero-sum
5. End-to-end security– lifecycle protection
6. Visibility and transparency
7. Respect for user privacy– keep it user-centric

PRIVACY BY DESIGN – PROACTIVE NOT REACTIVE, PREVENTATIVE NOT REMEDIAL

- Privacy needs to be part of the planning of any new or updated product, service, system or process.
- Privacy considerations should help drive the design rather than being bolted on at the end to address a few privacy risks.

PRIVACY BY DESIGN – PRIVACY AS THE DEFAULT

- The default setting of any design should protect the individual's personal information by understanding how the legal requirements apply in this context.

Version as at 15 June 2023

Privacy Act 2020

Public Act 2020 No 31
Date of assent 30 June 2020
Commencement see section 2

PRIVACY BY DESIGN – PRIVACY EMBEDDED INTO DESIGN

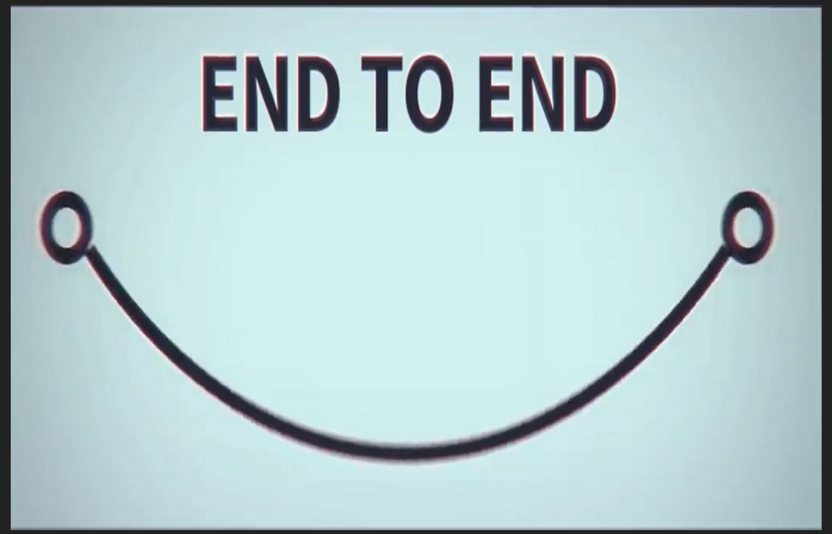
- Privacy should be so integral to the design of the product, service, system or process that it would not function without the privacy-preserving functionality.

PRIVACY BY DESIGN – FULL FUNCTIONALITY

- Design requirements to protect personal information should be treated as an opportunity to design a better product, service, system or process, not as a trade-off with other functionality.

PRIVACY BY DESIGN – END-TO-END SECURITY

- Protection and security of personal information should be considered for every stage of the information lifecycle: collection, storage and security, use, access and correction, disclosure, retention and disposal.



PRIVACY BY DESIGN – VISIBILITY AND TRANSPARENCY

- How the product, service, system or process will use the personal information needs to be clear to the individual providing the personal information.
- The accompanying privacy notice should be written in easy-to-understand, audience-appropriate language.

PRIVACY BY DESIGN – RESPECT FOR USER PRIVACY

- At the centre of any design for product, service, system or process is a person who will use that product, service, system or process.
- It's that person who will bear the harm and impact of any privacy breach or misuse of their personal information.

Recital 1

Data Protection as a Fundamental Right*

[1] The protection of natural persons in relation to the processing of personal data is a fundamental right. [2] Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

HE AHA TE MEA NUI O TE AO

HE TANGATA, HE TANGATA, HE TANGATA

ISO 31700 – PRIVACY BY DESIGN DEFINITION

- “Design methodologies in which privacy is considered and integrated into the initial design stage and throughout the complete lifecycle of products, processes or *services* that involve processing of *personal information*, including product *retirement* and the eventual *deletion* of any associated *personal information*.”

LAW & PRIVACY BY DESIGN

- Privacy Act 2020
  - s 22 Information privacy principle 5
- GDPR
  - Article 25 - Data protection by design and by default
  - Article 32 - Security of processing
- Other Jurisdictions
  - https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/

EU GDPR – PRIVACY BY DESIGN

Art. 25 GDPR

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. [1] The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. [2] That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [3] In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

FINES

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

118 Offence to fail to notify Commissioner

(1) An agency that, without reasonable excuse, fails to notify the Commissioner of a notifiable privacy breach under section 114 commits an offence and is liable on conviction to a fine not exceeding $10,000.

(2) It is not a defence to a charge under this section that the agency has taken steps to address the privacy breach.

(3) It is a defence to a charge under this section that the agency did not consider the privacy breach to be a notifiable privacy breach, but only if it was reasonable to do so in the circumstances.

FINES

2. The Commissioner has decided to issue Interserve with a Penalty Notice under section 155 of the Data Protection Act 2018 ("the DPA"). This penalty notice imposes an administrative fine on Interserve in accordance with the Commissioner's powers under Article 83 of the GDPR. The amount of the penalty is **£4,400,000**.

3. This penalty has been issued because of contraventions by Interserve of Article 5(1)(f) and Article 32 of the GDPR during the period 18 March

PRIVACY BY DESIGN INFRINGEMENT

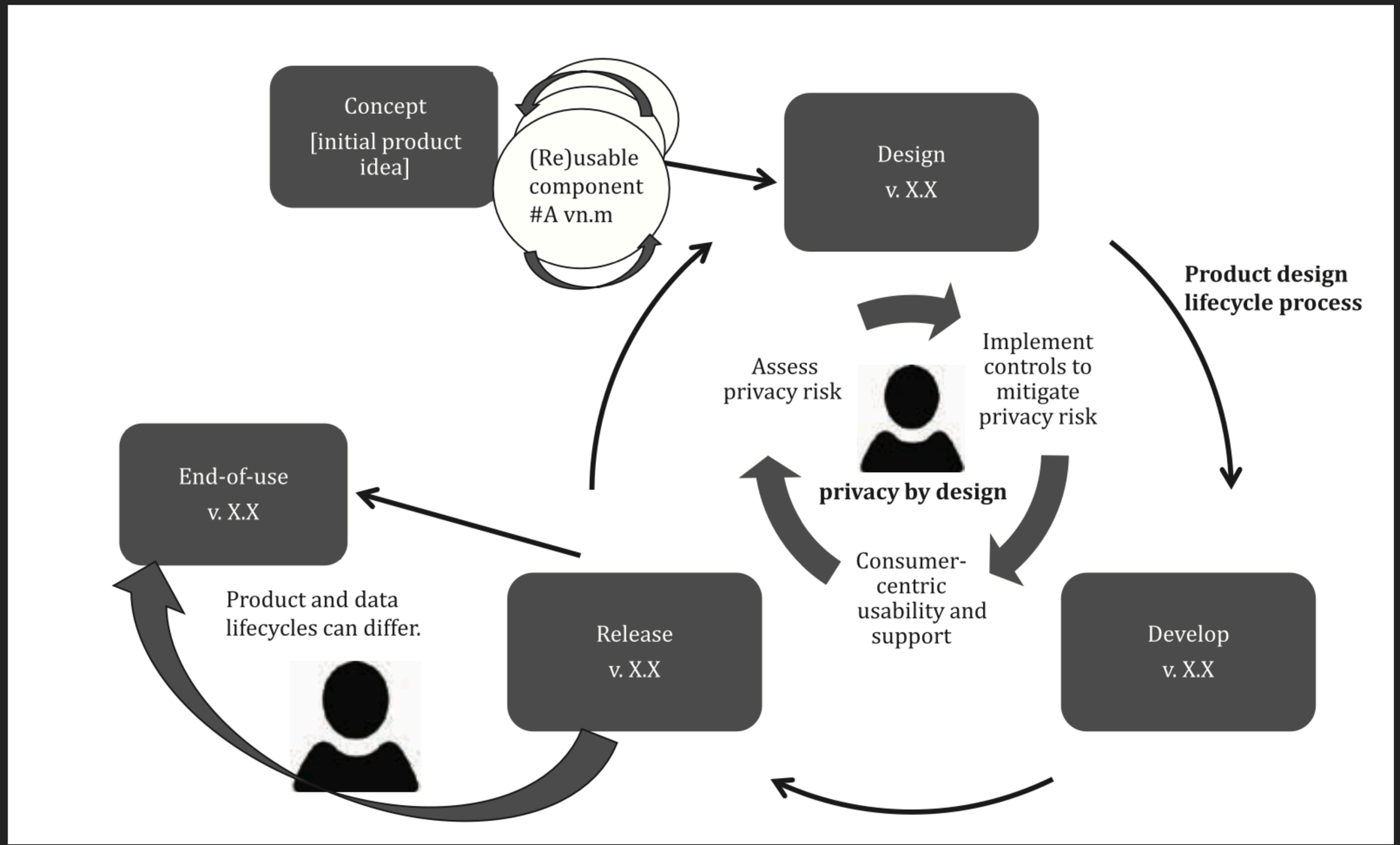
- Meta Platforms Ireland Limited
- Data Protection Commission found infringement of Articles 25(1) and 25(2) of the GDPR
- Imposed a fine of €265 million and a range of corrective measures

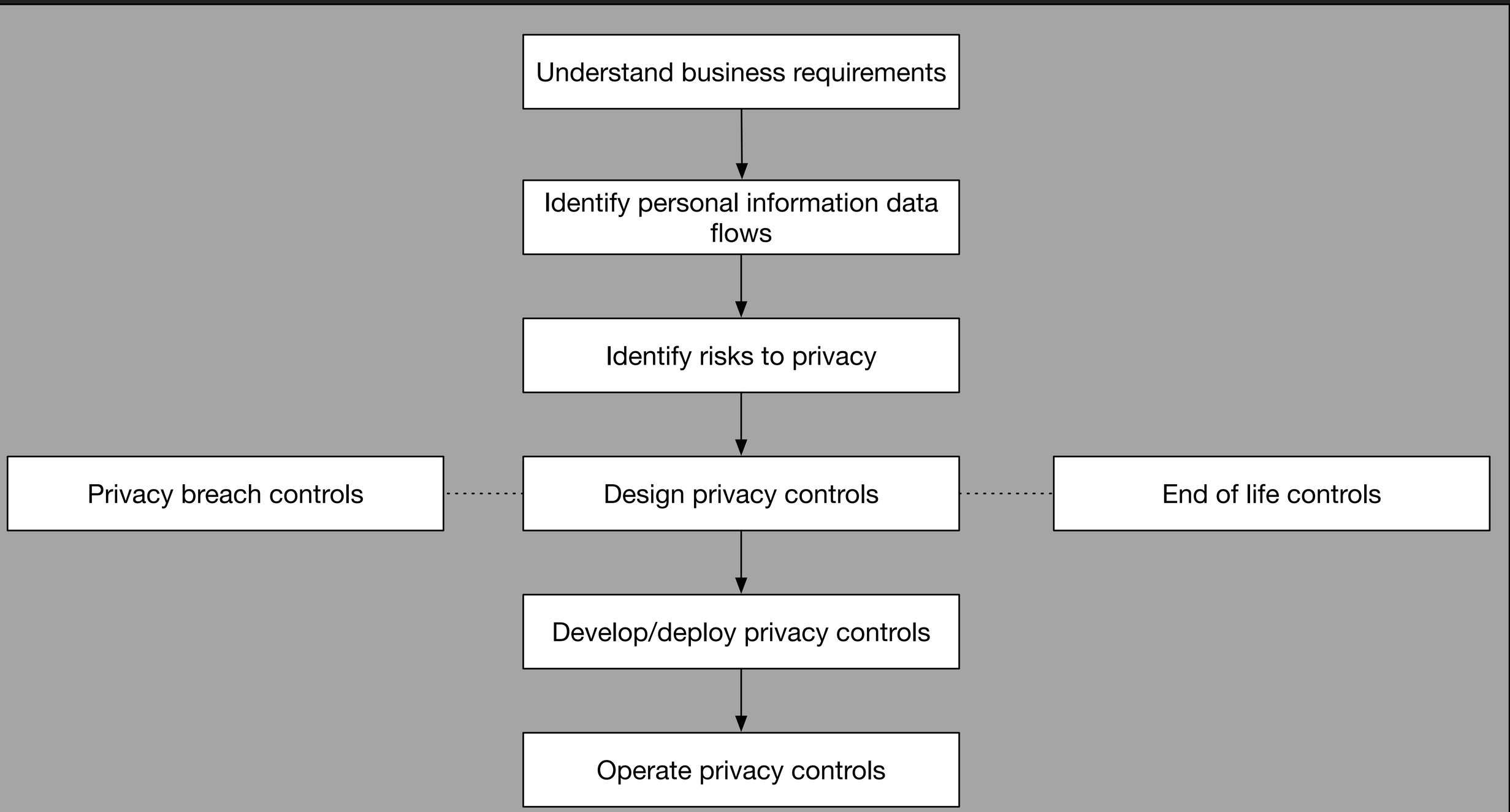
> 169. I find that MPIL infringed Article 25(1) GDPR by failing to implement appropriate technical and organisational measures, which are designed to implement data protection principles, specifically the principles provided for in Article 5(1)(b) and (f) GDPR, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

ISO 31700 – FRAMEWORK

- Management
- Risk
- Controls
  - Design
  - Development/deployment
  - Operation
  - Verification

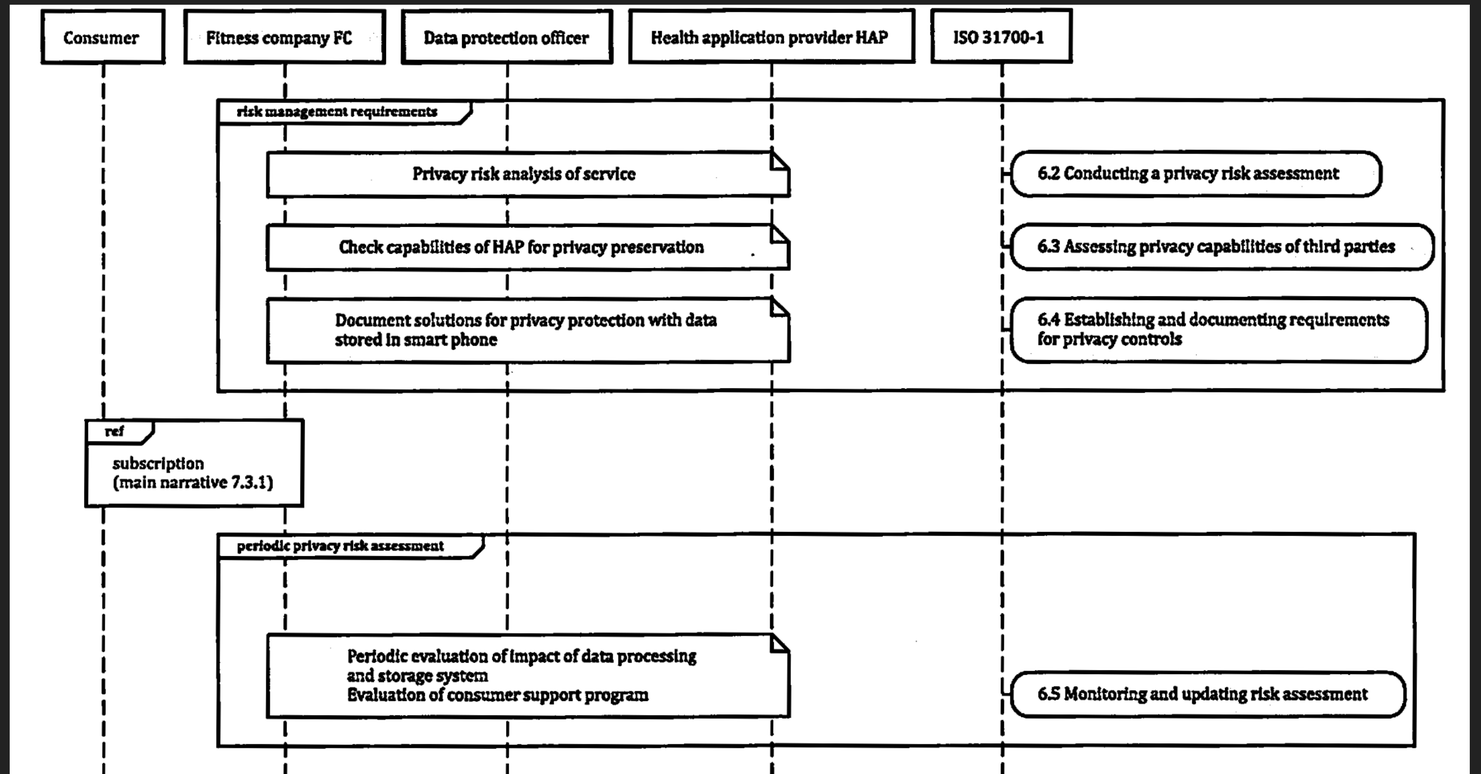
ISO 31700 – FRAMEWORK




Understand business requirements
Identify personal information data flows
Identify risks to privacy
Privacy breach controls
Design privacy controls
End of life controls
Develop/deploy privacy controls
Operate privacy controls

ISO 31700-2— FRAMEWORK - USE CASE - EXAMPLES

- Uses a specific format of written use
- Illustrated by UML sequence diagrams
- Use what works



RISK

- Risk to privacy - to persons
  - Harms
    - Emotional distress
    - Financial
    - Physical harm
- Risk of a privacy breach - to organisation
  - Harms
    - Fines
    - Cost of responding to breach

PRIVACY RISK ASSESSMENT

PRIVACY THREAT TYPES (LINDDUN)

- Linking
- Identifying
- Non-repudiation
- Detecting
- Data disclosure
- Unawareness & Unintervenability
- Non-compliance

PRIVACY CONTROLS – ARTICLE 32 GDPR

- Taking into account:
  - the state of the art,
  - the costs of implementation
  - and the nature, scope, context and purposes of processing
- The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks

WHAT ARE THE BUSINESS REQUIREMENTS

- Right here, right now
- No “It might be good in the future to…”
- Minimum personal information requirements
  - Fields
  - Retention

WHAT ARE THE BUSINESS REQUIREMENTS

- “A system to identify violations of mooring/parking rules”

USE CASES

- Observe
- RegistrationID
  - Location
  - ObservationTime
- Identify
- Issue violation
- Manage violations

PRIVACY CONTROLS – SYSTEM ISOLATION

- Bounded Contexts
- Segregation

PRIVACY CONTROLS – DATA REDUCTION

- PI being stored
  - Data fields
  - Retention
- PI being shared

PRIVACY CONTROLS – ENCRYPTION

- Storage of PI
  - Application level to provide encryption of specific fields
  - Not transparent or disk based
- Network communication of PI
- Key management

PRIVACY CONTROLS – ACCESS CONTROL

- Fine grained
- User
- System

PRIVACY CONTROLS – TOKENISATION

- One way
- Two way
- NB: Re-identification may be possible

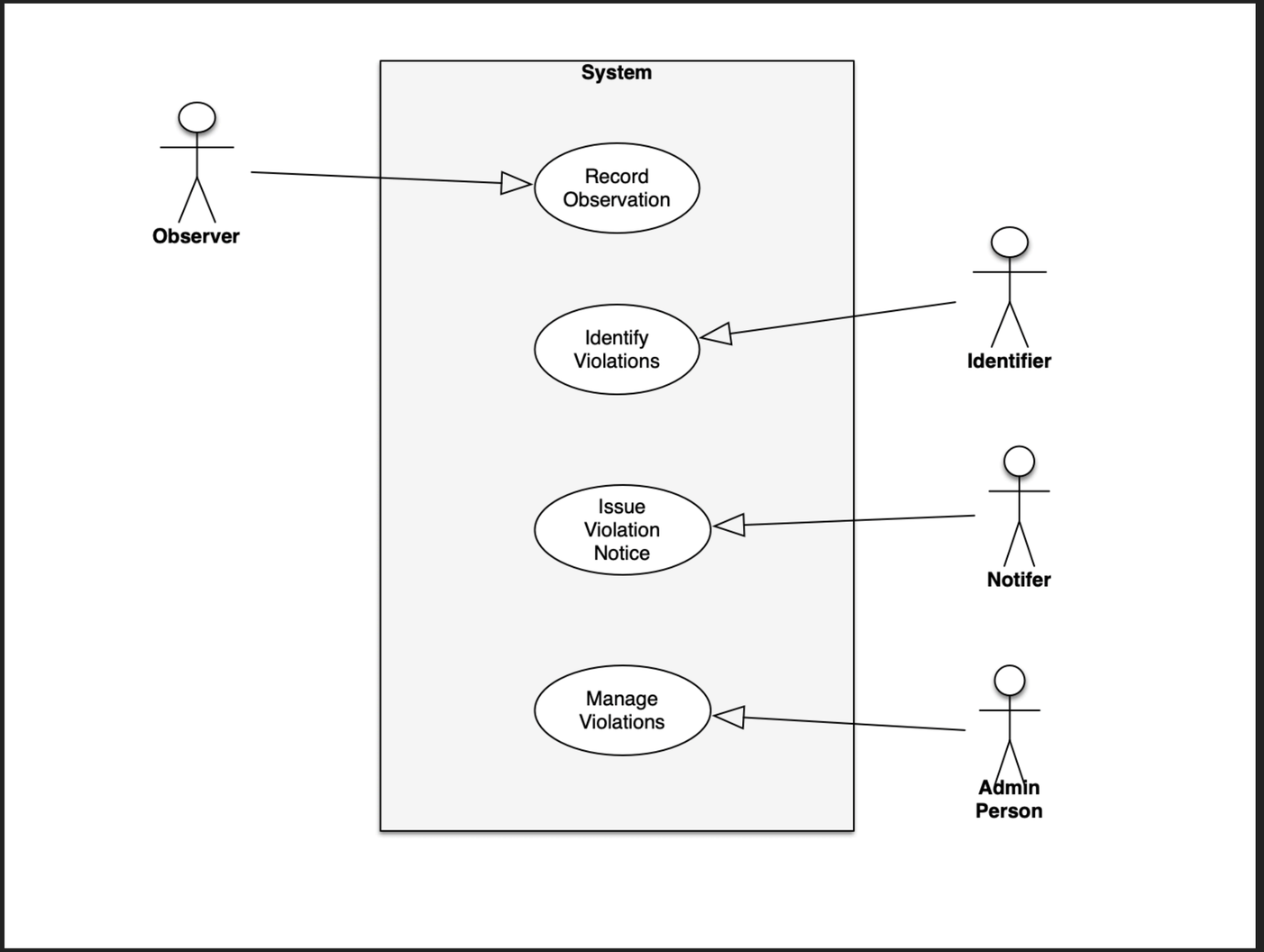
PRIVACY CONTROLS – LOGGING, REVIEWING, ALERTING

PRIVACY CONTROLS

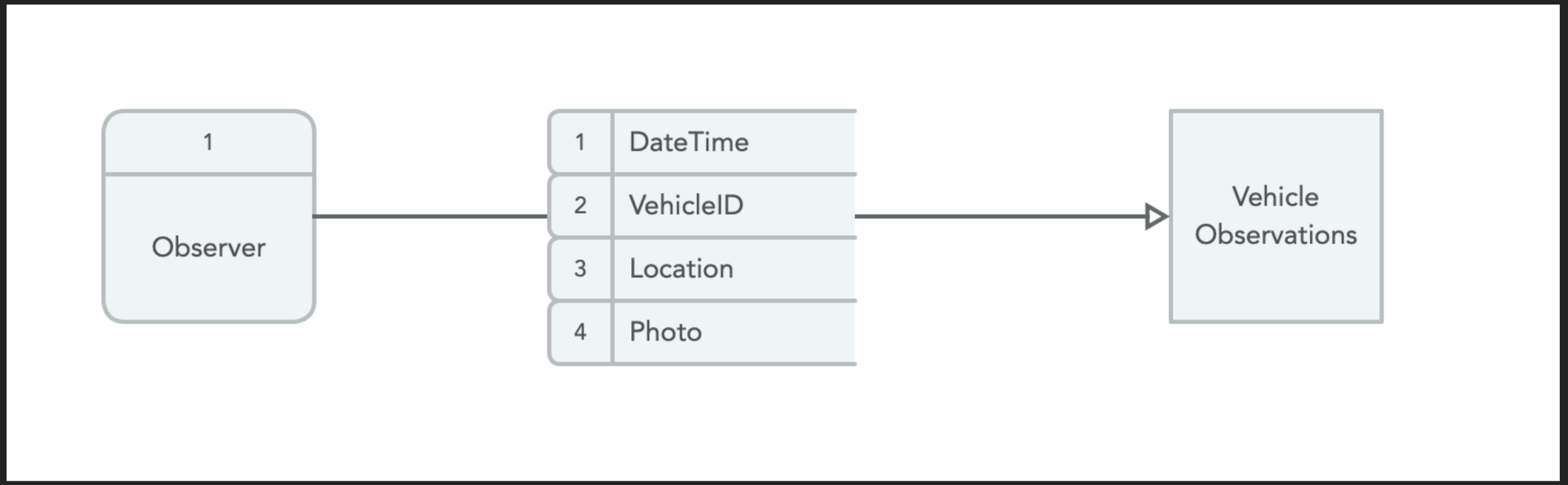
- Application Level
  - Context Specific
  - e.g Request to access functionality

EXAMPLE DOMAIN

EXAMPLE


System
Observer
Record Observation
Identify Violations
Identifier
Issue Violation Notice
Notifer
Manage Violations
Admin Person

EXAMPLE


1
Observer
1
DateTime
2
VehicleID
3
Location
4
Photo
Vehicle Observations

SUMMARY

- ISO 31700
- Privacy by design