Privacy & Identity Lab

Radboud University

Tilburg University
Law School

university of groningen

De technische uitdagingen van privacy by design

Jaap-Henk Hoepman

Privacy & Identity Lab
Radboud University
Tilburg University
University of Groningen

✉ *jhh@cs.ru.nl* // *www.cs.ru.nl/~jhh* // blog.xot.nl // @xotoxot

Privacy gaat over het beschermen van **persoonsgegevens**

Leave alone

Give control

Separate contexts

Privacy vanuit technisch perspectief

- **Privacy goals**
  - Unlinkability
  - Transparency
  - Intervenability
- **Naast**
  - Confidentiality
  - Integrity
  - Availability

- **Dus: echt anders dan beveiliging!**

Wat is een persoonsgegeven?

1) „persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

- **Dus**
  - Naam
  - BSN
- **Maar ook**
  - Kenteken
  - IP adres
  - …

Verschillende soorten data

Verzonden

- **Vrijwillig (“volunteered”)**
  - Wat je *expliciet* antwoordt op een vraag.
- **Geobserveerd (“observed”)**
  - Wat *impliciet* wordt geregistreerd van je gedrag.
- **Afgeleid (“inferred”)**
  - Wat kan worden opgemaakt uit andere data die al over jou bekend is.

[World Economic Forum-rapport Personal Data: The Emergence of a New Asset Class]

Wat is verwerken (Data Processing)?...

Action	Relevant GDPR Personal Data Processing Examples
Operate	Adaptation; Alteration; Retrieval; Consultation; Use; Alignment; Combination
Store	Organisation; Structuring; Storage
Retain	opposite to (Erasure; Destruction)
Collect	Collection; Recording
Share	Transmission; Dissemination; Making Available; opposite to (Restriction; Blocking)
Change	unauthorised third party (Adaptation; Alteration; Use; Alignment; Combination)
Breach	unauthorised third party (Retrieval; Consultation)

Privacy & Identity Lab

Radboud University

Tilburg University

Law School

university of groningen

Privacy by design

Privacy by design

- **Bescherm privacy gedurende het hele (technologische) ontwikkelproces**
  - Van concept …
  - … tot en met realisatie.

Gedurende de hele systeem ontwikkelings cyclus

Privacy by design

- **Bescherm privacy gedurende het hele (technologische) ontwikkelproces**
  - Van concept …
  - … tot en met realisatie.

Gedurende de hele systeem ontwikkelings cyclus

- **Privacy is een software quality attribute (net zoals security, performance,…)**
- **Privacy by design is een proces!**

Waarom privacy by design?

- **Het beperkt privacy risico's**
  - En dus reputatieschade of herstelkosten
  - "Wat je niet hebt kun je ook niet verliezen"
- **Het maakt nieuwe business mogelijk**
  - E.g. Zorg, Internet of Things, Quantified self
  - Net zoals security by design internet bankieren mogelijk maakte
- **Het is verplicht vanaf 2018!**
  - De Algemene Verordening Gegevensbescherming (AVG)


Maar hoe?

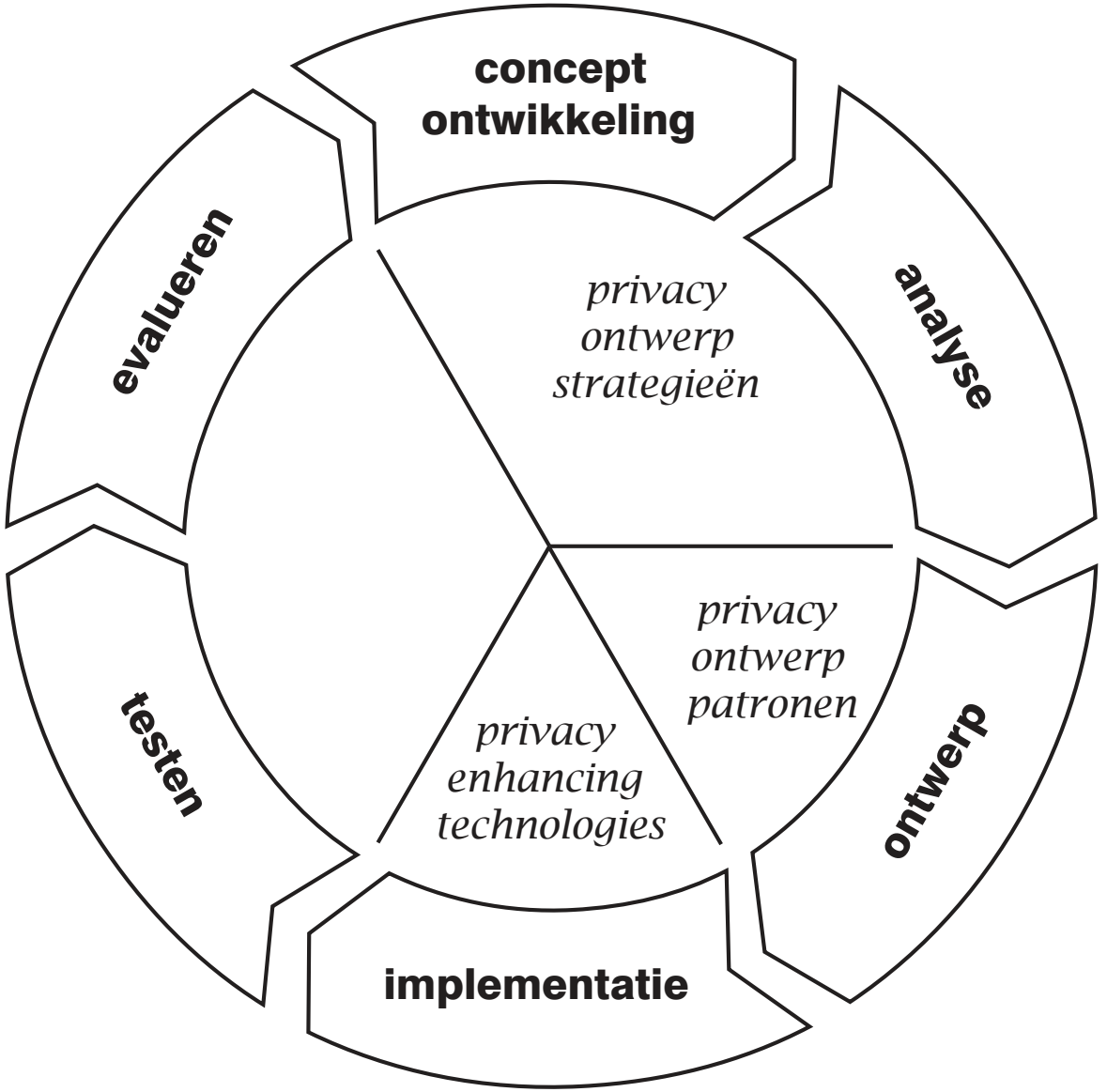
Privacy & Identity Lab

Radboud University

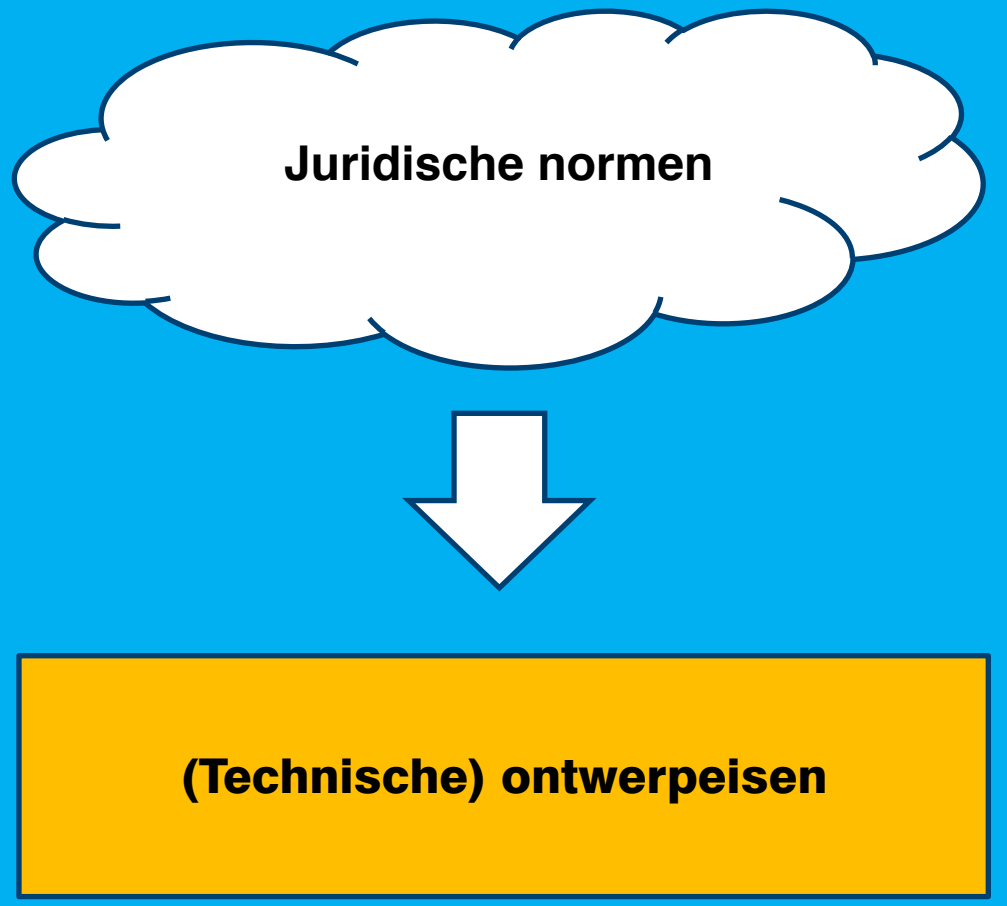
Tilburg University
Law School

university of groningen

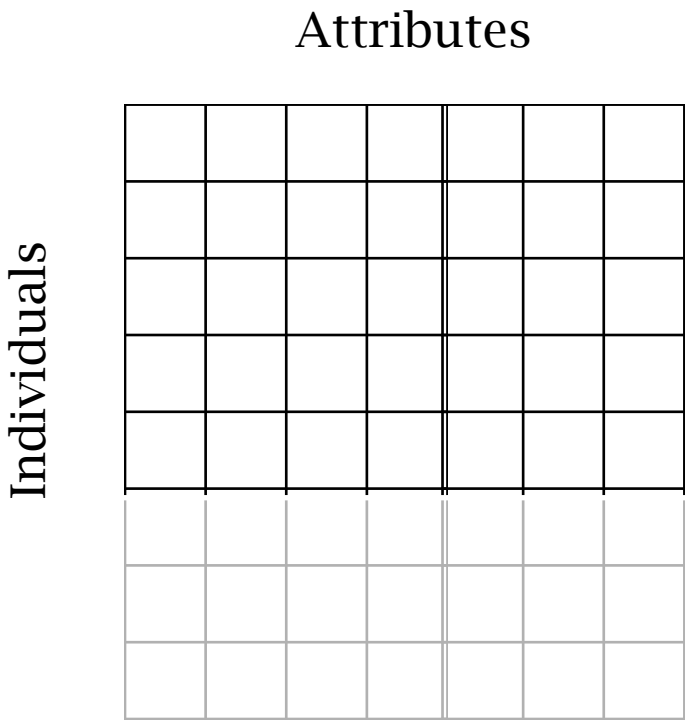
Acht privacy ontwerp strategiën

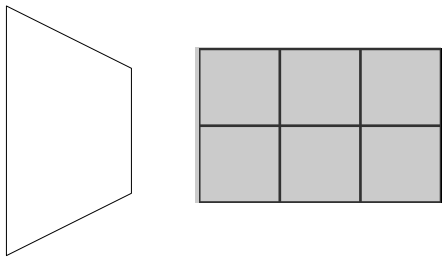

concept
ontwikkeling
analyse
ontwerp
implementatie
testen
evalueren
privacy
ontwerp
strategieën
privacy
ontwerp
patronen
privacy
enhancing
technologies

Privacy design strategieën zetten vage juridische normen om in concrete privacy vriendelijke ontwerpeisen

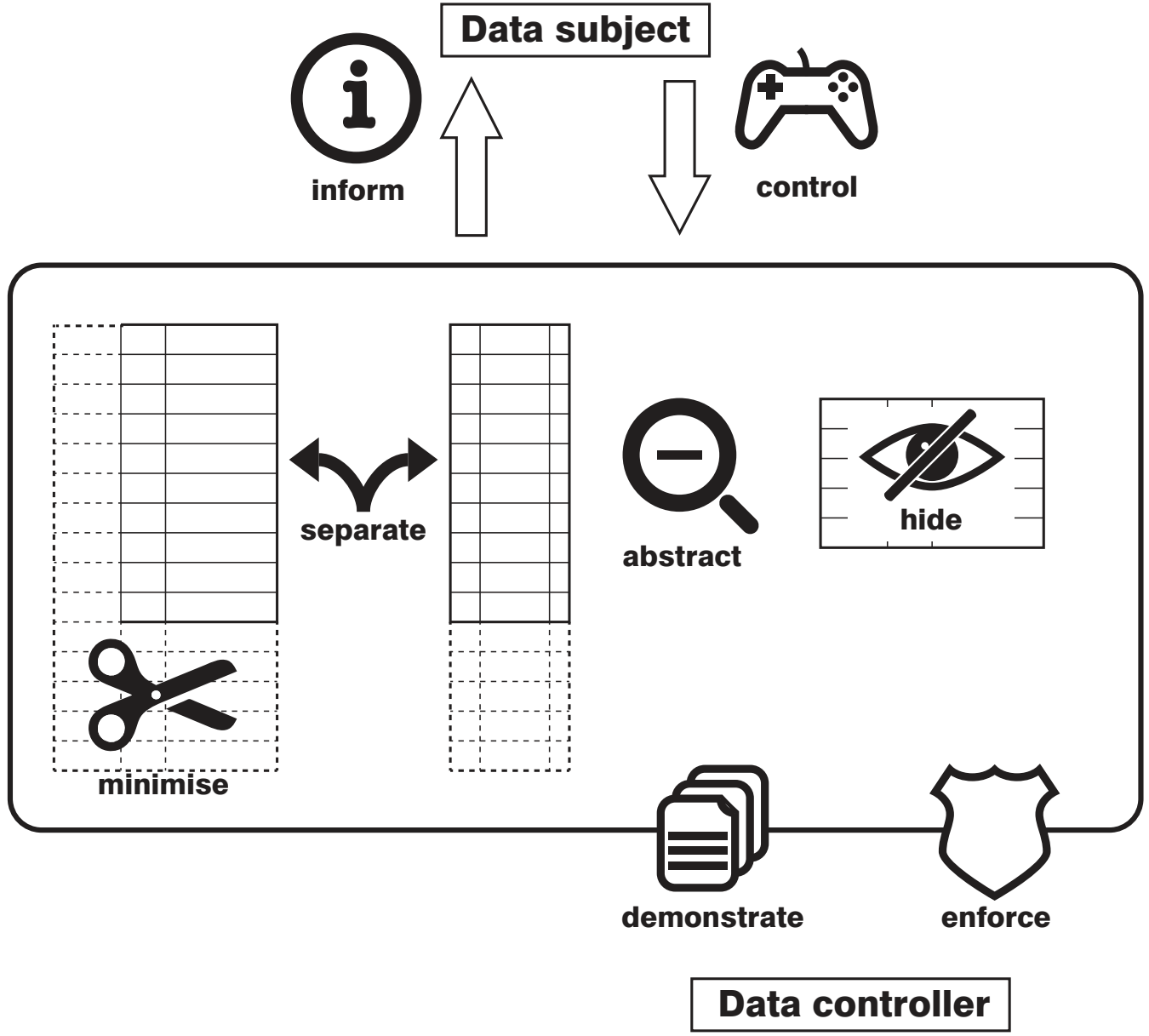


Database tabel





minimise **separate** **abstract** **hide**

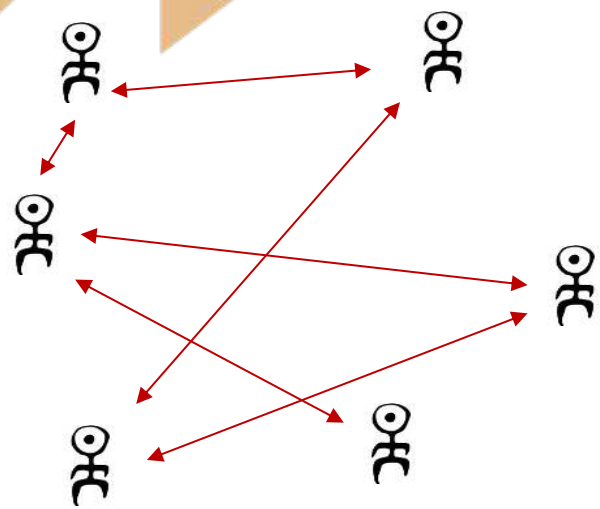

Data subject
inform
control
separate
abstract
hide
minimise
demonstrate
enforce
Data controller

Minimaliseer (Minimise)

- **Definitie**
  - *Beperk zo veel mogelijk de verwerking van persoonsgegevens.*
- **Geassocieerde taktieken**
  - SLUIT UIT (EXCLUDE): Sluit op voorhand bepaalde personen of gegevens uit.
  - SELECTEER (SELECT): Selecteer alleen relevante personen of gegevens.
  - VERWIJDER (STRIP): Verwijder (deel) informatie die niet langer nodig zijn.
  - VERNIETIG (DESTROY): Verwijder volledige persoonsgegevens zodra ze niet langer nodig zijn.
- **Voorbeelden**
  - Select before you collect.
  - Whitelists.
  - Blacklists.

Scheidt (Separate)

- **Definitie**
  - *Scheidt verwerking van persoonsgegevens zo veel mogelijk van elkaar, om correlatie te beperken.*
- **Geassocieerde taktieken**
  - ISOLEER (ISOLATE): Verzamel of verwerk persoonsgegevens (voor verschillenden doeleinden) in verschillende (logische) databases of systemen.
  - DISTRIBUEER (DISTRIBUTE): Distribueer de verwerking (voor één taak) over verschillende fysieke locaties.
- **Voorbeelden**
  - Doe zoveel mogelijk in de apparatuur (PC, smartphone) van de eindgebruiker.
  - Peer-to-peer, bijv. sociaal netwerk.



diaspora*

Abstraheer (Abstract)

- **Definitie**
  - *Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.*
- **Geassocieerde taktieken**
  - GROEPEER (GROUP): Aggregeer informatie over categorieën personen, in plaats van data voor ieder individu te verwerken.
  - VAT SAMEN, GENERALISEER (SUMMARIZE): Vat gedetailleerde informatie samen in meer abstracte attributen.
  - RUIS TOEVOEGEN, VERSTOREN (PERTURB): Voeg ruis toe, of benader de werkelijke waarde van een gegeven.

- **Voorbeelden**
  - Registreer leeftijd ipv. Geboortedatum.
  - Verzamel het energieverbruik in een wijk ipv. per huishouden.
  - Benader de werkelijke locatie van een gebruiker (met een resolutie van bijv. 10 km^2).

Bescherm, maak onherleidbaar (Hide)

- **Definitie**
  - *Voorkom dat persoonsgegevens openbaar of bekend worden.*
- **Geassocieerde taktieken**
  - BEPERK TOEGANG (RESTRICT): Beperk toegang tot persoonsgegevens.
  - VERSLEUTEL (ENCRYPT): Versleutel persoonsgegevens (zowel op het netwerk als bij opslag).
  - VERBREEK LINK (DISSOCIATE): Verbreek de link tussen personen en gegevens.
  - MENG (MIX): Maak data onherleidbaar, bijvoorbeeld door deze te mixen of te anonimiseren.
  - MAAK ONBEGRIJPBAAR (OBFUSCATE): Hash persoonsgegevens (bijvoorbeeld om er pseudoniemen van te maken) of maak ze anderszins onbegrijpbaar.
- **Voorbeelden**
  - Mix netwerken / Tor.
  - Pseudomimiseren.
  - Differential privacy.
  - Access control.
  - Attributer based credentials.

Informeer (Inform)

- **Definitie**
  - *Informeer gebruikers over de verwerking van hun persoonsgegevens.*
- **Geassocieerde taktieken**
  - INFORMEER (SUPPLY): Vertel welke persoonsgegevens worden verwerkt, op welke manier en tot welke risico's dat kan leiden.
  - LEG UIT (EXPLAIN): Doe dit op een duidelijke en voor leken begrijpbare manier, en leg uit waarom de verwerking noozakelijk is.
  - WAARSCHUW (NOTIFY): Waarschuw gebruikers als hun persoonsgegevens gebruikt worden, of als deze gelekt zijn.
- **Voorbeelden**
  - Leesbare privacy policy.
  - Privacy icons.
  - Algoritmische transparantie.

Geef controle (Control)

- **Definitie**
  - *Geef gebruikers controle over de verwerking van hun persoonsgegevens.*
- **Geassocieerde taktieken**
  - VRAAG TOESTEMMING (CONSENT): verwerk alleen gegevens waarvoor expliciete toestemming is gegeven.
  - GEEF KEUZE (CHOOSE): laat gebruikers selecteren welke gegevens wel/niet verwerkt worden.
  - CORRIGEER (UPDATE): Geef de mogelijkheid om persoonsgegevens te corrigeren…
  - VERWIJDER (RETRACT): …of te (laten) verwijderen.
- **Voorbeelden**
  - Opt-in ipv opt-out.
  - Privacy dashboard.

Dwing af (Enforce)

- **Definitie**
  - *Committeer je aan een privacy vriendelijke verwerking van persoonsgegevens, en dwing dit af.*
- **Geassocieerde taktieken**
  - STEL VAST (CREATE): Leg beleid vast dat beschrijft op welke wijze je privacy wilt beschermen.
  - BEHEER (MAINTAIN): Beheer dit beleid, en pas dit aan waar nodig.
  - DWING AF (UPHOLD): Dwing het beleid af, en maak mogelijk dat het uitgevoerd wordt.
- **Voorbeelden**
  - Privacy policy.
  - Beleg verantwoordelijkheden.
  - Controleer het beleid, en de implementatie daarvan, regelmatig, en pas waar nodig aan.
  - Neem noodzakelijke technische en organisatorische maatregelen.

Toon aan (Demonstrate)

- **Definitie**
  - *Toon aan dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt.*
- **Geassocieerde taktieken**
  - LEG VAST (LOG): Verzamel logs (en kom in actie bij anomalieën).
  - AUDIT: voer regelmatig audits uit op de verwerking van persoonsgegevens.
  - RAPPORTEER (REPORT): Rapporteer de resultaten aan de verantwoordelijken.
- **Voorbeelden**
  - Privacy management systeem (a la ISO 27001 security management).
  - Certificering.

Acht privacy design strategieën

Data oriented

- **Minimaliseer (Minimize)**
  - *Beperk zo veel mogelijk de verwerking van persoonsgegevens.*

- **Scheidt (Separate)**
  - *Scheidt persoonsgegevens zo veel mogelijk van elkaar, om correlatie te beperken.*

- **Abstraheer (Abstract)**
  - *Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.*

- **Bescherm, maak onherleidbaar (Hide)**
  - *Voorkom dat persoonsgegevens openbaar of bekend worden.*

Process oriented

- **Informeer (Inform)**
  - *Informeer gebruikers over de verwerking van hun persoonsgegevens.*

- **Controleer (Control)**
  - *Geef gebruikers controle over de verwerking van hun persoonsgegevens.*

- **Dwing af (Enforce)**
  - *Committeer je aan een privacy vriendelijke verwerking van persoonsgegevens, en dwing dit af.*

- **Toon aan (Demonstrate)**
  - *Toon aan dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt.*

Meer informatie

- G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, and S. Schiffner. Privacy and Data Protection by Design - from policy to engineering. Technical report, ENISA, December 2014. ISBN 978-92-9204-108-3, DOI 10.2824/38623. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

- M. Colesky, J.-H. Hoepman, and C. Hillen. A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering – IWPE'16, San Jose, CA, USA, May 26 2016. http://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf

Vragen / discussie

[Monty Python's
Argument Clinic sketch]