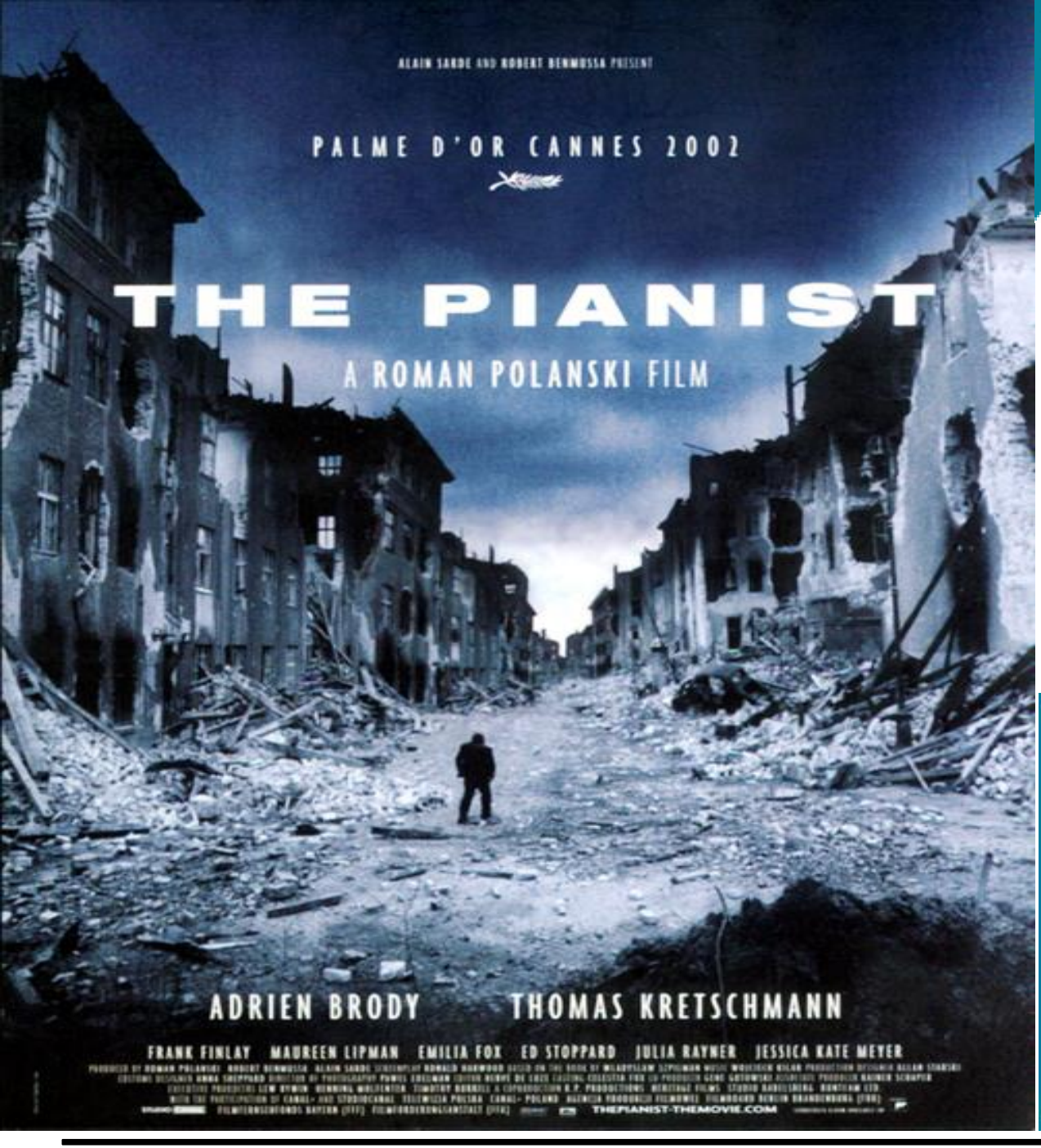
➔ NOREA VAKTECHNISCHE THEMADAG PRIVACY (AVG / GDPR)➔

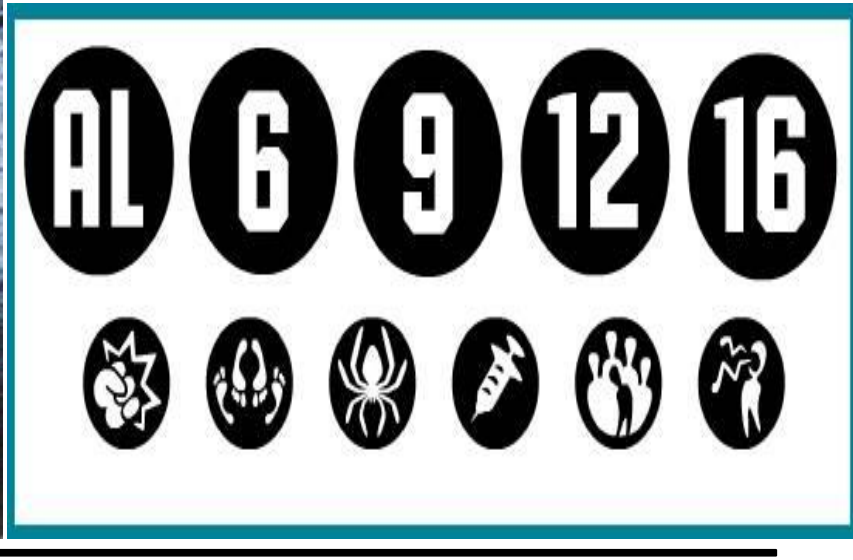
Jan Matto | Mazars Management Consultants

Onderwerpen:
Ervaringen met (pre) privacy impact assessments bij grote en complexe projecten, zoals: eNIK, eID stelsel, Idensys, DigiD, M-Pesa / M-Tiba



KijkWijzer

Niet schieten op de PIA-NIST



ERVARINGEN MET COMPLEXE PRIVACY IMPACT ASSESSMENTS

- Identity management systemen (eID Stelsel, Idensys, DigiD Substantieel en Hoog)
- Elektronische Nederlandse IdentiteitsKaart (eNIK)
- Central Bank of Ireland, Credit Register
- Human Genome Project, Healthcare, Ireland / Iceland
- Politie, Opsporings- & Inlichtingendiensten
- Biometrische gezichtsherkenningsystemen grensbewaking (No-Q)
- Datalek Nederlandse Zorgautoriteit (NZa)
- Privacy Impact assessment en audit, online portaal gezondheidszorg
- M-Pesa / M-Tiba, Kenya

https://www.bof.nl/live/wp-content/uploads/politie-privacy-audits-2012/politie-zeeland/20110906-audit-wpg.pdf

https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/pia/31072015_PIA_Introductieplateau_eIDv1_final.pdf

https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/pia/310715_Managementsamenvatting_van_de_finale_versie_van_de_PIA.pdf

https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/pia/Privacy_impactanalyse_eID_Stelsel.pdf

De relevantie en functie van een PIA

Setting the scene: PIA's voor een duurzame digitale samenleving en economie

Algemeen privacybescherming

- Europees Verdrag Rechten van de Mens

  (EVRM, artikel 8: recht op privacy, zelfbeschikking, vrije nieuwsgaring)
- Realisatie van een digitaal systeem met verwerkingen van persoonsgegevens impliceert (meestal) een inbreuk op grondrecht van de bescherming van de persoonlijke levenssfeer
- Voortgaande digitalisering van maatschappij en economie vergroot de risico's

Andere gerelateerde maatschappelijke ontwikkelingen en risico's

- Wantrouwen in digitale en eGovernment services
- Surveillance door overheden
- Risico voor economische groei
- Verstoringen van marktwerkingen
- Politieke en Bestuurlijke risico's

➔ **Een PIA heeft te maken met maatschappelijkverantwoord ondernemen**

➔**Een PIA gaat over verschaffen van transparantie over verwerken van persoonsgegevens**

Setting the scene: Duurzame digitale samenleving en economie?

Grootste bedreigingen voor onze samenleving en economie:

- We leven in een digitale samenleving en economie
- Cybercrime en –risico's nemen toe
- Uitval, verlies data, datalekken, reputatie, aansprakelijkheid, …
- Veel aandacht media / meer bewustwording
- Verknoping van IT-systemen over organisaties heen (informatieketens)
- Organisaties moeten elkaar digitaal kunnen vertrouwen
- Compliance eisen nemen toe

  - Niet aantoonbaar veilig, dan mag je niet meedoen
  - No security, no business
  - Meldplicht Datalekken
  - Een PIA kan hierbij helpen

- Behoefte aan digital transparency en assurance
- Vraag naar een reeks van nieuwe assurance diensten
- Focus op IT-werkelijkheid (en niet alleen procedures en governance)

Wat is een PIA

(AVG: Gegevensverwerkingseffectbeoordeling)

Beoordeling……?

Wat is een Privacy Impact Assessment?

1) Een Privacy Impact Assessment (PIA) is een hulpmiddel bij ontwikkeling van beleid, plannen, wijzigingen van ICT-systemen, wijzigingen in gebruik van systemen en aanleg van databestanden;

2) Een Privacy Impact Assessment kan ook gebruikt worden de mate van privacy compliance in beeld te brengen van een bestaande situatie met als doel om eventueel benodigde optimalisaties te identificeren;

3) Hiermee kunnen privacy risico's op een gestructureerde en heldere wijze in kaart worden gebracht;

4) Een PIA is gedurende een ontwikkelproces iteratief en dynamisch van karakter;

5) Een PIA is geen audit;

6) Een PIA blijkt telkens maatwerk (erg afhankelijk van context en doelstellingen);

Wat is een Privacy Impact Assessment?

7) Door een PIA gedurende het ontwerpproces regelmatig uit te voeren, kunnen (nieuwe) risico's vroegtijdig worden ontdekt en wordt de bewustwording van risico's vergroot. Zo nodig kunnen richtinggevende aanbevelingen worden gedaan om privacy risico's te elimineren of te mitigeren.

8) De PIA is een communicatiemiddel naar alle stakeholders

9) Een PIA rapportage is een gestructureerde vastlegging van bevindingen (in een matrix en rapport) van:

- welke privacymaatregelen zijn getroffen
- per te onderscheiden verwerking van persoonsgegevens en de daarbij onderliggende processen en IT systemen
- per privacy principe en per privacy risico

10) Een PIA is vooral multi-disciplinair

- **Privacy Impact Assessment (Artikel 35 AVG)**

Toets periodiek of getroffen maatregelen nog in lijn zijn met de AVG en met alle privacy principes en risico's en of de doelstelling van de verwerking behaald kan worden via andere wegen of met minder persoonsgegevens.

- **Privacy by Design (Artikel 35 AVG)**

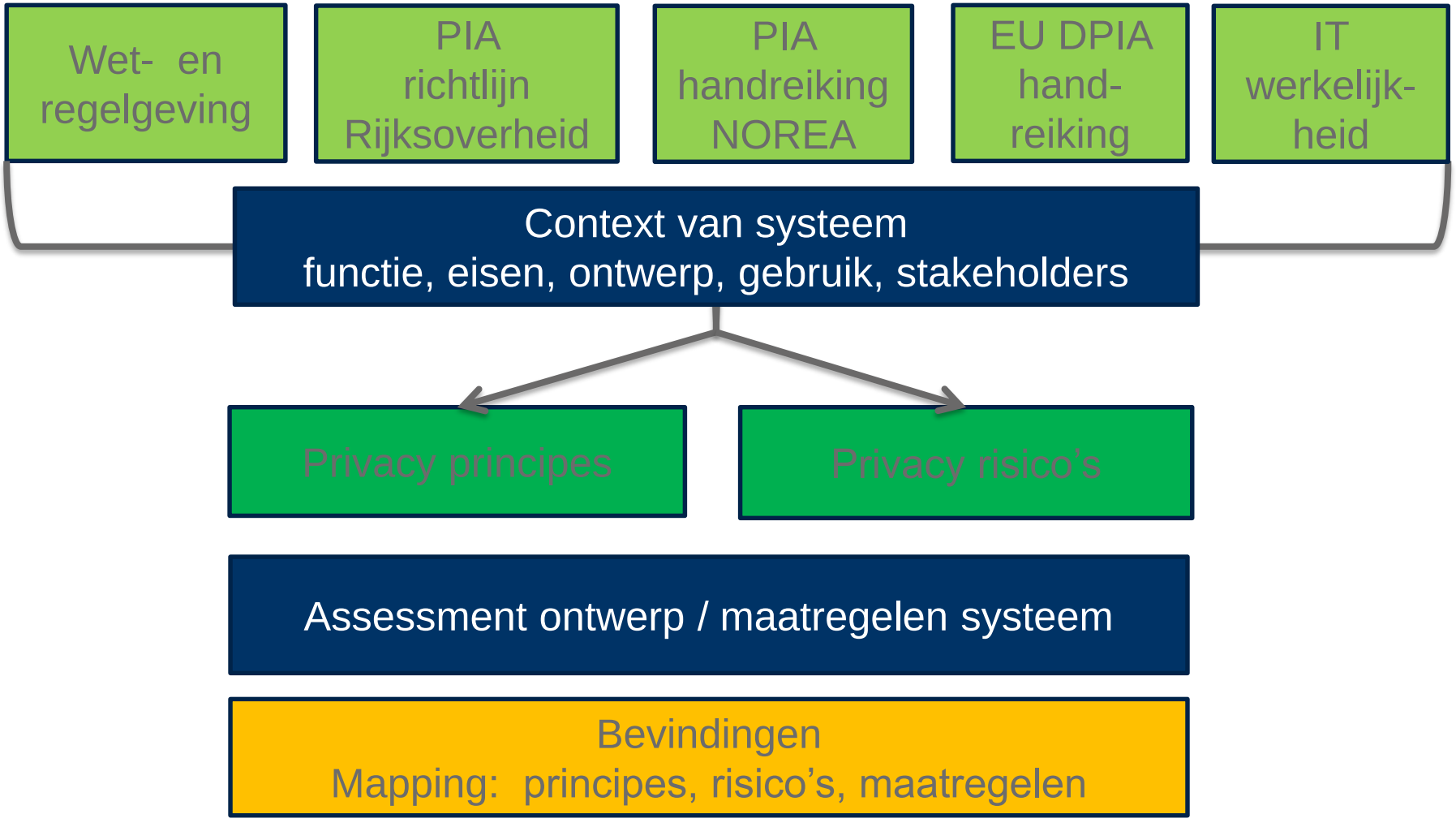
Bij invoering van nieuwe verwerkingen van persoonsgegevens of bij wijzigingen zorg dat vanaf het begin ontwerpcriteria worden gehanteerd waarmee invulling kan worden gegeven aan het principe van "privacy by design". Systemen dienen voordat deze in gebruik worden genomen naar de laatste stand van de techniek zijn beveiligd.

- **Monitoring, periodieke toetsing en evaluatie (artikel 30, 32 AVG)**

Implementeer technische middelen en organisatorische procedures die waarborgen dat de beveiliging van systemen en de daarmee verwerkte persoonsgegevens permanent gegarandeerd wordt. Richt een management cyclus in waarbij zo nodig optimalisaties worden doorgevoerd.

De aanpak en onderwerpen van een PIA

Aanpak en structuur van een PIA



Stappen in de PIA:

A) Systeemanalyse ➔ IT werkelijkheid

1) Analyse van het ontwerp en de architectuur
2) Analyse van de onderliggende systeemlagen (alle!)
3) In het bijzonder de eigenschappen alle betrokken systeemcomponenten
4) Inventarisatie van alle te verwerken attributen en gegevensstromen

B) Principe / risico / maatregel matrix

5) Inventarisatie maatregelen / privacy principes
6) Inventarisatie maatregelen / privacy risico's

C) Assessment

7) Uitvoering van het eigenlijke assessment

D) Rapportage

8) Rapportage bevindingen

Invulling Universele Privacy Principes (OESO) en in de AVG

- Grondslag, noodzakelijkheid, gerechtvaardigd belang
- Proportionaliteit, subsidiariteit
- Doelbinding
- Verantwoording
- Transparantie
- Datakwaliteit
- Gegevensminimalisatie / gebruiksminimalisatie

  (ook need-to-know / need-to-have, bewaartermijnen)
- Privacy Enhancing Technologies (PET)
- Privacy by Design (PbD)
- Beveiliging
- Rechten betrokkenen / individu:

  - User consent
  - Inzage en correctie
  - Recht om vergeten te worden
- Derde landen buiten EER

Beheersing Universele Privacy risico's

- ➔ Profiling, stigmatisering, uitsluiting
- ➔ Identiteitsfraude
- ➔ Cybercrime en cyberincidenten / datalekken
- ➔ Inbreuken in de persoonlijke levenssfeer
- ➔ Inperking van zelfbeschikkingsrecht
- ➔ Anderen bepalen wat relevant is voor jou
- ➔ Ongebreidelde gegevensverzamelingen / data deluge effect
- ➔ Gegevens gebruiken in een andere context en voor een ander doel dan waarvoor zij eerder verzameld zijn
- ➔ Verstoring level playing field / marktwerking

Beheersing Universele Privacy risico's

Maatregelen treffen die aantoonbaar (universele) privacyrisico's beperken:

- 'Data deluge'-effect
- Ontstaan "hotspots"
- Waardestijging van persoonsgegevens
- 'Function creep'
- Onrechtmatig gebruik van uniek identificerende gegevens
- Inconsistente implementatie en naleving verantwoordingsbeginsel
- Geheime (niet transparante) verwerking van persoonsgegevens
- Niet toegestane verwerking van persoonsgegevens buiten de EU
- Datalekken
- Specifieke risico's ten aanzien van biometrische identificatie en authenticatie
- Onrechtmatig gebruik identificerende gegevens, zoals BSN nummers

SAMENHANG PRIVACYPRINCIPES EN –RISICO'S

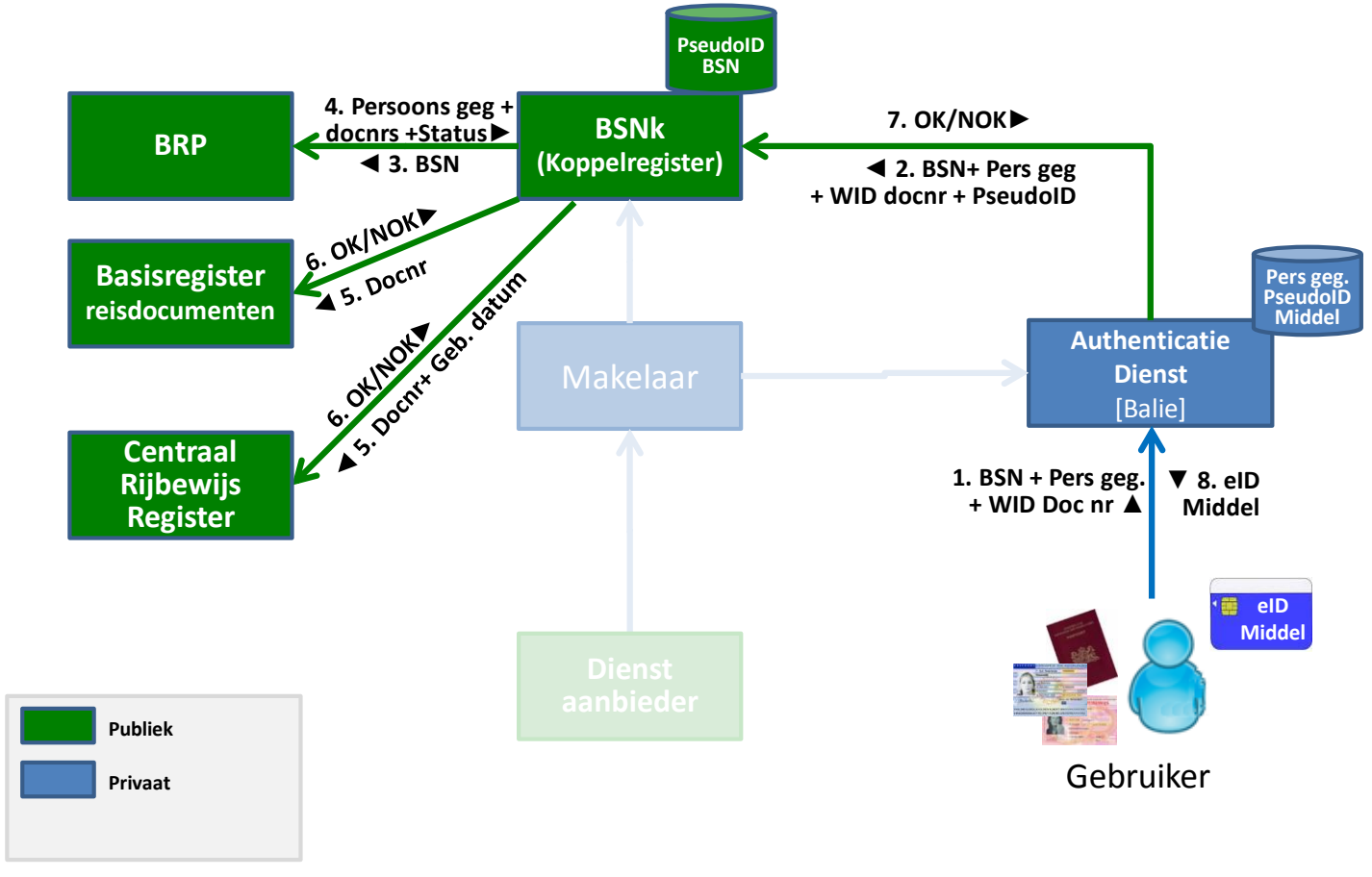
PRIVACY PRINCIPE	Privacyrisico's								
	ID	DD	FC	IV	NT	NE	DL	OB	GC
2.1 Verantwoording		x	x	x	x	x	x		
2.2 Limiteren van het verzamelen van gegevens	x	x	x				x		x
2.3 Doelbinding / limiteren van het gebruik van gegevens	x	x	x		x	x	x		x
2.4 Gegevenskwaliteit	x							x	
2.5 Beveiliging van gegevens (Privacy by Design/Privacy Enhancing Technologies)	x	x	x			x		x	
2.6 Transparantie					x	x	x	x	
2.7 Rechten van betrokkenen					x	x	x	x	x

ID: Identiteitsfraude
DD: Data deluge'-effect
WA: Waardestijging van persoonsgegevens
FC: 'Function creep'
OU: Onrechtmatig gebruik van uniek identificerende gegevens
PF: Profiling
VB: Verkeerde behandeling in sociaal en economisch maatschappelijk verkeer
SK: Stigmatisering door koppeling van gegevens
IV: Inconsistente implementatie en naleving verantwoordingsbeginsel
NT: Geheime (niet transparante) verwerking van persoonsgegevens
NE: Niet toegestane verwerking van persoonsgegevens buiten de EU
CC: Nieuwe ontwikkelingen op het terrein van cloudcomputing waarbij gegevens over de gehele wereld kunnen worden verplaatst.
DL: Data lekken
OB: Omkering van de bewijslast voor de betrokkene
GC: Consumenten worden gedwongen om in te stemmen met het gebruik van hun gegevens

Een PIA in een grote complexe omgeving

Idensys / eID Stelsel / DigiD

Ontwerp Idensys / cluster van verwerkingen en verantwoordelijkheden



Privacy Principes en Privacy Risico's

- Digitale identiteit is uiterst gevoelig persoonsgegeven (profiling / data deluge / function creep, fraude, et cetera)
- Diefstal / misbruik van digitale identiteit heeft grote impact in de persoonlijke levenssfeer
- Post issue reparatie kan moeilijk of onmogelijk zijn bij compromittering IDs (in het bijzonder BSN, maar geldt in feite voor elk ID)
- Er ontstaan meer gevoelige / stigmatiserende persoonsgegevens door het gebruik van systemen dan door directe invoer van persoonsgegevens ➔ "hotspots"
- Misbruik kan leiden tot verlies vertrouwen in / ontwrichting van het "systeem"
- Lastige vraagstukken over verantwoordelijkheden en verhoudingen

Enkele bevindingen PIA Idensys / eID Stelel / DigiD

ISSUE	AANBEVELING / MAATREGEL
1) BSN gebruik in private domein	➔ Aanpassing regelgeving
2) Ondermijning door bestaande componenten	➔ Afscheiding systemen
3) Data kwaliteit / fraude detectie	➔ Regulering fraudeonderzoek
4) Datakwaliteit	➔ Maatregelen interne beheersing
5) Metadata / loggings	➔ Aanscherpen doelstellingen en reductie
6) Hotspots	➔ Verregaande compartimentering
7) Privacy enhancing technology	➔ Blijven doorontwikkelen
8) Gevoelige gegevens	➔ Gedifferentieerde behandeling (eIDAS)
9) Bewaartermijnen	➔ Gedifferentieerd naar type gegeven
10) Gedrag dienstaanbieders	➔ Regulering toelating dienstaanbieder
11) Doorbreking functiescheidingen	➔ “Chinese muren” / compartimenteren
12) BSN Koppelregister	➔ Afzondering van de Authenticatiedienst
13) Risico niet doorontwikkelen	➔ Actieplan doorontwikkeling
14) Toenemend gebruik = groter risico	➔ Limitering data opslag

Doorkijk naar toekomst

- Non persistente pseudo identiteiten (gerandonimiseerde polymorfe pseudoidentiteiten)
- BSN - loze authenticatiedienst
- Hypersegmentering
- Elke componenten een andere pseudo-ID
- Cryptografische bescherming op processor / machinetaal niveau

Ten Slotte: PIA's en de rol van de IT auditor

- Duurzame digitale samenleving en economie waar vertrouwen in is
- Vraag naar transparantie en assurance over security en privacybescherming
- Het gaat om de betrokkenen
- Onafhankelijk onderzoek is daarbij belangrijk
- IT werkelijkheid is de basis van het onderzoek
- Hier ligt een publiekbelang waar de IT auditor een belangrijke rol kan spelen
- PIA's moeten publicabel zijn

VRAGEN / DISCUSSIE

CONTACT

Jan Matto RE RI

- E-mail: jan.matto@mazars.nl
- T: +31 (0)88 277 13 99
- M: +31 (0)6 53 57 8232
- Twitter: @Jan_Matto

Dank voor uw aandacht!