Privacy by Design

Maar dan concret(er)

Frank van Vonderen I Oktober2016

VERDONCK KLOOSTER & ASSOCIATES

Voorstellen

- Frank van Vonderen – audit, informatiebeveiliging & privacy
- frank.vanvonderen@vka.nl | 06-12557358
- 15+ jaar in 6 woorden: Trainee, Big4, ZZP, ondernemer, global company
- Management Consultant bij Verdonck, Klooster & Associates
- Adviseur én ‘in de modder’

- “Het privacy vakgebied is onvolwassen”
- “Ik ken geen enkel vakgebied dat zo veeleisend is en tegelijkertijd zo onduidelijk is”.
- Daar probeer ik wat aan te doen…

Persoonsgegevens

- Persoonsgegevens zijn alle gegevens die direct of indirect tot een levende natuurlijke persoon zijn te herleiden. Voorbeelden:
  - Naam, (Email-)adres, Geslacht, Leeftijd, Geboorteplaats
  - Functie (CEO van bedrijf X) – weliswaar openbare informatie, maar wel persoonsgegeven!
- Indirect herleidbaar
  - Denk aan: locatie, IP-adres, gegevens over vervoer, gegevens over transacties, Mac-adres
  - Combinatie van niet herleidbare attributen, dat alsnog herleidbaar wordt (Big data!)

VERDONCK KLOOSTER & ASSOCIATES

Bijzondere persoonsgegevens

- Speciale regels voor het verwerken van “bijzondere persoonsgegevens” (art. 16 e.v. Wbp):
  - Godsdienst of levensovertuiging
  - Ras
  - Politieke gezindheid
  - Gezondheid
  - Seksuele leven
  - Lidmaatschap van een vakvereniging
- Ook op het oog ‘normale’ persoonsgegevens:
  - Voorbeeld: een busabonnement voor speciaal vervoer (kan gezondheidsgegeven zijn).

Trend: strenger, complexer en administratiever!

2016: Wet Meldplicht datalekken

Protocol, melden aan Autoriteit Persoonsgegevens en/of aan klanten, awareness, vereist actie binnen 72 uur, risicoanalyse.

2016: Boetebeleidsregels Autoriteit Persoonsgegevens

€820.000 of 10% procent van de jaaromzet, cumulatief.

2018: Nieuwe EU Privacyverordening

Boetes: €20.000.000 tot 4% van de internationale jaaromzet

Administratieplicht, betrokkene centraal, privacy impact assessment.

Deadline: Mei 2018

TO DO:

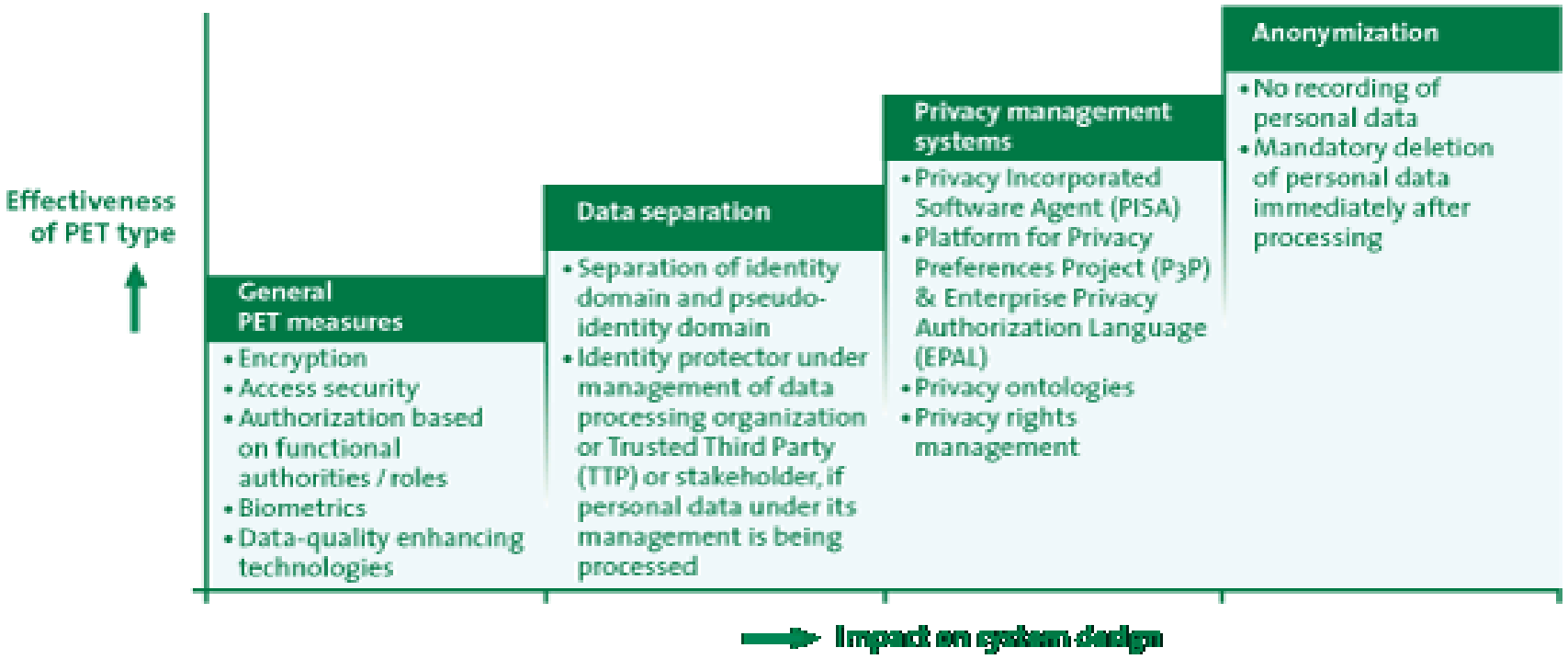
- ☐ Rol van de Privacy Officer binnen uw organisatie (her)definiëren.
- ☐ Registeren waar binnen uw organisatie persoonsgegevens worden verwerkt.
- ☐ Verwerkingen door derden in kaart brengen (ook grensoverschrijdend).
- ☐ Concrete bewerkersovereenkomsten met derden afsluiten conform de nieuwe regelgeving.
- ☐ Datalekprotocol opstellen, periodiek reviewen en oefenen.
- ☐ Privacy Impact Assessments uitvoeren bij potentiële risicovolle verwerkingen.
- ☐ Privacy by Design / Default als standaard in de bedrijfsvoering en ICT invoeren.
- ☐ Processen inrichten voor de uitoefening van rechten van betrokkenen.
- ☐ Transparant, begrijpelijk en toegankelijk privacybeleid opstellen en uitdragen.

By design / by default – poging 1

- AP: Privacy by design houdt in dat u als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.

- The principle of “Privacy by design” means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.

Uit de oude doos: PET



VERDONCK KLOOSTER & ASSOCIATES

Tik(je) concreter – Poging 2

Bron: Cavoukian / CIP

- Proactief en preventief in plaats van reactief en herstellend.
- Privacy by default, comply or explain
- Privacy geïntegreerd in het ontwerp, IT-systemen en handelingspraktijken
- Volledige functionaliteit – win/win in plaats van compromissen
- Bescherming tijdens de volledige levenscyclus – houd rekening met veranderende omstandigheden
- Zichtbaarheid en transparantie – hou het open
- Respect voor de privacy – laat de gebruiker centraal staan

Mijn poging

Privacy by Design gaat over:

- Verstandig gebruik maken van persoonsinformatie
  - een vak voorbedrijfskundigen, informatieanalisten en procesarchitecten
  - meer dan alleen dataminimalisatie
- Voor de gegevens die je nodig hebt technieken inzetten die de privacy vergroten
  - een vak voor ICT-ers en contract- & leveranciersmanagers
  - meer dan versleutelen of anonimiseren

Privacy by Design ontleed

Organisatie	Techniek
Minimaal verzamelen	Versleutelen
Verwijderen na gebruik	Pseudonimiseren / Anonimiseren
Vermijd kopieën	Bij testen?
Bewaak kwaliteit	Bij systeemontwikkeling?
Beperken van het gebruik	Bij Business Intelligence?

Minimaal verzamelen

- Welke informatie heb je nu eigenlijk nodig
  - Overvragen (initiële aanvraag)
  - Tijdens of na initiële beoordeling nog steeds nodig (CV's en sollicitatiebrieven)
  - Wat is nodig bij een toets? Kennis van het absolute gegeven, of toets je de drempel (leeftijdstoets, inkomenstoets, …)

  - (en hoe verstrek je, via mail)

Verwijderen na gebruik

- Wanneer gooi je weg
- Hoe lang heb je welke gegevens nodig – brei van termijnen
- Als je weggooit, is het dan echt weg (of inactief in de database)
- Hoe vaak gebruik je het archief en hoe toegankelijk moet dit zijn
- Digitaal en fysiek

Vermijd kopieën

- Raadpleeg bronregisters op basis van uitvraag
- Zijn kopieën van bronregisters (die elke dag repliceren / synchroniseren) nodig
- Eenmalige kopieën / exports naar bijvoorbeeld Office
- Mail, DMS, Sharepoint, netwerkschijven
- Faseer oude (sub)administraties uit…
- Schoon de caches

Preventie – 1

Woensdag 09 maart 2016 | Het laatste nieuws het eerst op NU.nl

Voorpagina
Net binnen
Algemeen
Binnenland
Buitenland
Politiek
Economie
Geld
Ondernemen
Beurs
Belastingaangifte
Sport
Voetbal
Champions League
Schaatsen
Wielrennen
MijnTeam
Tech
Internet
Gadgets
Games
Mobiel
Entertainment
Achterklap
Films en series
Muziek
Boek en cultuur
Media

NU.nl > Tech > Internet

Foto: 123RF

Privédata duizenden inwoners Rotterdam en Oegstgeest gelekt

Gepubliceerd: 09 maart 2016 13:03
Laatste update: 09 maart 2016 14:01

De privégegevens van 25.000 Rotterdammers en 8.000 inwoners van Oegstgeest waren ongeveer twee maanden lang toegankelijk voor onbevoegden door een fout van een ambtenaar.

Het gaat om namen, adresgegevens en burgerservicenummers uit belastingbestanden tussen 1996 tot 2004, bevestigt de gemeente Rotterdam woensdag.

Voor de gegevens uit Oegstgeest gaat het om de periode 2007, 2008 en 2009. Deze gegevens waren openbaar toegankelijk wanneer er gericht naar werd gezocht.

De gemeenten hebben slachtoffers van het datalek op de hoogte gebracht middels een brief. Er is een onderzoek ingesteld en melding gemaakt bij de Autoriteit Persoonsgegevens.

VERDONCK KLOOSTER & ASSOCIATES

Preventie – 2

BINNENLANDS BESTUUR

BESTUUR EN ORGANISATIE FINANCIËN RUIMTE EN MILIEU SOCIAAL

WIJKTEAM MAILT GEGEVENS CLIËNTEN NAAR VERKEERDE

Sjoerd Hartholt • 13 apr 2016 2 reacties

De afdeling sociale wijkteams van gemeente Amersfoort heeft per ongeluk een bestand met privacygevoelige informatie van duidend tot vijftienhonderd zorgcliënten naar een verkeerd adres gemaild. Er is inmiddels melding van het incident gemaakt bij Autoriteit Persoonsgegevens.

NAW-gegevens en geleverde zorg

In de verstuurde gegevens waren namen van cliënten met hun adres, woonplaats en een beschrijving van de geleverde zorg terug te vinden. Het college zegt eveneens melding te hebben gedaan bij Autoriteit persoonsgegevens. 'Wij betreuren in hoge mate dat dit heeft kunnen gebeuren. Ons primaire doel is om nu eerst mogelijke nadelige gevolgen voor de in het bestand opgenomen personen te voorkomen. Het belangrijkste is daarom om te voorkomen dat deze gegevens door de ontvanger verder openbaar worden gemaakt.'

Preventie – 3

Veelgestelde vragen

Toon alles / Verberg alles

Wat is er gebeurd met de digitale inbraak via de website van de gemeente Ede?

De website is gehacked door zoekresultaten te manipuleren en zo google-data te beïnvloeden. Het doel hiervan is het doorleiden van mensen naar externe advertentiewebsites over afvallen en het lenen van geld. Dit in plaats van het doorleiden van mensen naar de plek op de Ede-website waar informatie staat waarnaar ze op zoek zijn.

Dit soort aanvallen gebeuren vaak vanuit Oost-Europa. Dat is ook hier het geval geweest. Tijdens deze aanval is een database mogelijk ingezien. Tijdens deze zogenoemde hack zijn mogelijk persoonsgegevens uit een database ingezien en/of meegenomen.

Een gespecialiseerd bureau heeft forensisch onderzoek uitgevoerd. Zij hebben geen aanwijzing kunnen vinden dat de database op onze website is geraadpleegd en/of de inhoud ervan is meegenomen, maar kunnen het ook niet voor 100% uitsluiten. Volgens de onderzoekers waren de hackers er niet op uit (persoons)gegevens in te zien.

Het gaat om gegevens die in de periode van 7 januari 2015 tot en met 8 juli 2016 zijn ingevuld in het voormalige contactformulier op deze website.

Bewaak kwaliteit

- Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be
  - *Accurate (inhoudelijk juist)* – 'Bewoner van Dorpsstraat 48 staat in een strafdossier bij voor een zedendelict'
  - *Complete (volledig)* – 'Bewoner van Dorpsstraat 48 staat in een strafdossier bij voor een zedendelict. Deze is één van de getuigen die is gehoord'
  - *Kept up-to-date (actueel) – Bewoner Dorpsstraat 48 is inmiddels verhuisd*

Beperken van het gebruik

Je mag als organisatie het gegeven gebruiken, maar waarvoor?

- Gebruik BSN van eigen werknemers, alleen voor specifieke doeleinden. Niet voor Intranet, Userid, verlofkaarten

Specifieke issues per branche – wat mag je verzamelen, van ketenpartners vragen en wat met wie delen

- Sociaal domein
- Zorgverzekeraars
- Arbo-dienstverlening
- Onderwijs
- Woningcorporaties

Taak voor brancheorganisaties?

Bron: VNG Matrix gegevensuitwisseling bij uitvoering, fraudepreventie en fraudebestrijding Wmo en Jeugdwet

4. Matrix gegevensuitwisseling (bijzondere) persoonsgegevens Wmo 2015 in het kader van rechtmatige uitvoering

Leesinstructie matrix Wmo 2015

1. In de matrix ziet u welke organisaties gegevens met elkaar mogen delen.
2. De letters in de matrix verwijzen naar de wettelijke bepaling op grond waarvan de gegevens kunnen worden verstrekt. De wetsartikelen geven ook aan met welk doel welke en onder welke voorwaarden (bijvoorbeeld toestemming betrokkene) de gegevens mogen worden verstrekt.

VERSTREKKENDE PARTIJEN / INSTANTIES	ONTVANGENDE PARTIJEN / INSTANTIES: COLLEGE VAN B&W*	GEMEENTELIJKE TOEZICHTHOUDER WMO 2015	SVB	AANBIEDER MAATSCHAPPELIJKE ONDERSTEUNING	CAK	ZORGVERZEKERAAR (ZVW)	CIZ	ZORGAANBIEDER (ZVW)	BELASTING-DIENST	ZORGAANBIEDER PGB-HH/PGB-BG	UITVOERDER (WLZ)
COLLEGE VAN B&W*		A B C	A B C	A B C	A B C	J (K)		J (K)			L
GEMEENTELIJKE TOEZICHTHOUDER WMO 2015	I										
SVB	H										
AANBIEDER MAATSCHAPPELIJKE ONDERSTEUNING	E	E M	E		E						
CAK	G										
ZORGVERZEKERAAR (ZVW)	J										
CIZ	D										
ZORGAANBIEDER (ZVW)	J	M									
BELASTINGDIENST	F				F						
ZORGVERLENER PGB-HH/PGB-BG	E	E	E		E						
UITVOERDER (WLZ)	L	M									

*Bij beschermd wonen/opvang zijn via mandatering centrumgemeenten aangewezen voor delen van de uitvoering. Mandaatbesluit geeft in de regel aan wat is overgedragen.

Legenda kleuren schema: Meer informatie op pagina 8 | Meer informatie op pagina 9 | Meer informatie op pagina 10

VERDONCK KLOOSTER & ASSOCIATES

Techniek – versleutelen

- Versleutelen klinkt simpel, maar is het niet
- Algoritme, lengte
- Symmetrische encryptie, asymmetrische encryptie, hashen (met en zonder salt)
- Wie beschikt over de sleutel (Whatsapp, Amazon, Oracle), wie beheert stelsel van asymmetrische versleuteling
- Sleutelbeheer en delen / overdragen van sleutels

Techniek – anonimiseren / pseudonimiseren

- Pseudonimiseren is een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Het algoritme kan voor een persoon altijd hetzelfde pseudoniem berekenen, waardoor informatie over de persoon, ook uit verschillende bronnen, kan worden gecombineerd.
- Daarin onderscheidt pseudonimiseren zich van anonimiseren, waarbij het koppelen op persoon van informatie uit verschillende bronnen niet mogelijk is.

(bron nl.wikipedia.org)

Techniek – Gebruik persoonsgegevens bij testen

- ‘Mag ik een kopietje productie’

- Gegevens nodig bij alle testen? Nee
  - OTAP – bij O en T veel minder noodzakelijk dan bij A

- Werken met standaard testset, of… niets weerbarstiger dan de werkelijkheid
- Verwijderen na gebruik
- Wie voert de testen uit

Privacy bij systeemontwikkeling

- Waterval ontwikkeling (achteraf checken) vs Agile (oeps, het draait al)
- In beide gevallen net zozeer een non-functional als ‘kwaliteit’ of ‘beveiliging’

- Slim ontwerp bedrijfsprocessen
- Hanteren van ontwerpprincipes
- Kennisniveau beveiliging / privacy bij ontwikkelaars

Privacy by Design – big data

enisa

	PRIVACY BY DESIGN STRATEGY	DESCRIPTION
1	Minimize	The amount of personal data should be restricted to the minimal amount possible (data minimization).
2	Hide	Personal data and their interrelations should be hidden from plain view.
3	Separate	Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4	Aggregate	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	Inform	Data subjects should be adequately informed whenever processed (transparency).
6	Control	Data subjects should be provided agency over the processing of their personal data.
7	Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	Demonstrate	Data controllers must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

Table 1: Privacy by design strategies [6]

Toepassing principes binnen Big Data value chain

	BIG DATA VALUE CHAIN	KEY PRIVACY BY DESIGN STRATEGY	IMPLEMENTATION
1	Data acquisition/collection	MINIMIZE	Define what data are needed before collection, select before collect (reduce data fields, define relevant controls, delete unwanted information, etc), Privacy Impact Assessments.
		AGGREGATE	Local anonymization (at source).
		HIDE	Privacy enhancing end-user tools, e.g. anti-tracking tools, encryption tools, identity masking tools, secure file sharing, etc.
		INFORM	Provide appropriate notice to individuals – Transparency mechanisms.
		CONTROL	Appropriate mechanisms for expressing consent. Opt-out mechanisms. Mechanisms for expressing privacy preferences, sticky policies, personal data stores.
2	Data analysis & data curation	AGGREGATE	Anonymization techniques (k-anonymity family, differential privacy).
		HIDE	Searchable encryption, privacy preserving computations.
3	Data storage	HIDE	Encryption of data at rest. Authentication and access control mechanisms. Other measures for secure data storage.
		SEPARATE	Distributed/ de-centralised storage and analytics facilities.
4	Data use	AGGREGATE	Anoymisation techniques. Data quality, data provenance.
5	All phases	ENFORCE/ DEMONSTRATE	Automated policy definition, enforcement, accountability and compliance tools.

Table 2: Privacy by design strategies in the big data value chain

Privacy en BI – Boerenverstand

- Heldere strategie, wat wil je en hoe gebruiken
- Privacy notice en toestemming aanpassen

- Anonimiseren / pseudonimiseren

- Risico's:
  - 'Doen omdat het kan'
  - Standaard rapportages vs 'even uitproberen'
  - Ruime autorisaties op rapportagemodule

More reading

- Enisa, Privacy and Data Protection by Design – from policy to engineering, December 2014
- Kuiper en Van Vonderen – Privacy by Design is een business vraagstuk, InformatieBeveiliging Magazine, September 2016
- CIP - Handleiding Privacy by Design, 31 mei 2016