

@zwne



VNG | PAPENDAL | 7 NOVEMBER 2016

INLEIDING WET BESCHERMING PERSOONSGEGEVENS (& AVG)

Prof. Mr. Gerrit-Jan Zwenne



programma

achtergrond en context

- privacy en gegevensbescherming

de spelers

- betrokkene
- verantwoordelijke
- bewerker
- autoriteit persoonsgegevens
- functionaris

het speelveld

- verwerking persoonsgegevens
- bestand
- persoonlijk of huishoudelijk
- journalistiek
- territoriale werking


de spelregels

- verwerkingsgrondslag
- doelbinding
- bewaren
- bijzondere gegevens en bsn
- enz.

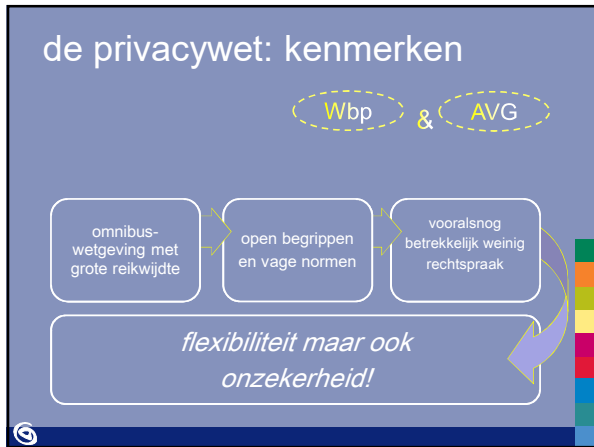
én een uiteenzetting van de **meldplicht datalekken**



CONTEXT











betrokkenen, verantwoordelijken, bewerken, functionaris en college

DE SPELERS



de spelers

Wbp & AVG

<p>betrokkene</p> <ul style="list-style-type: none"> - degene op wie de gegevens betrekking hebben - natuurlijke persoon 	data subject
<p>verantwoordelijke ("verwerkingsverantwoordelijke")</p> <ul style="list-style-type: none"> - heeft zeggenschap over doel en wijze van verwerking - natuurlijk persoon of rechtspersoon, of bestuursorgaan 	controller
<p>bewerker ("verwerker")</p> <ul style="list-style-type: none"> - bewerkt gegevens t.b.v. verantwoordelijke zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen 	processor
<p>Ap of Cbp</p> <ul style="list-style-type: none"> - Autoriteit persoonsgegevens of College bescherming persoonsgegevens 	data protection authority
<p>FG</p> <ul style="list-style-type: none"> - functionaris voor de gegevensbescherming 	data protection officer (DPO)






ijge verkorte opleiding
in 13 november 2016
10:00

voorom
ect perfoon
van 10 miljoen
of 4% van de
verdienste
omzet

Data Protection Officer
Aanstelling privacy professional verplicht vanaf 2018!



Wbp & AVG

(verwerkings)verantwoordelijke

— formeel juridisch, maar ook feitelijk of functioneel

zeggenschap over doel en middelen van verwerking

— wie beslist over bewaartermijnen, verstrekking, inzageverzoeken, etc?

... aan de hand van algemeen in het maatschappelijk verkeer geldende maatstaven moeten worden gezien aan welke natuurlijke persoon, rechtspersoon of bestuursorgaan de betreffende verwerking moet worden toegerekend

uitgangspunt bij de invulling van het begrip «verantwoordelijke» is de bestaande structuur van het civielrechtelijke en bestuursrechtelijke personen- en organisatierecht

binnen de overheid zullen als verantwoordelijke te kwalificeren zijn: de afzonderlijke ministers op rijksniveau, het college van gedeputeerde staten en de commissaris van de Koningin op provinciaal niveau en het college van B&W en de burgemeester op gemeentelijk niveau (MvT)

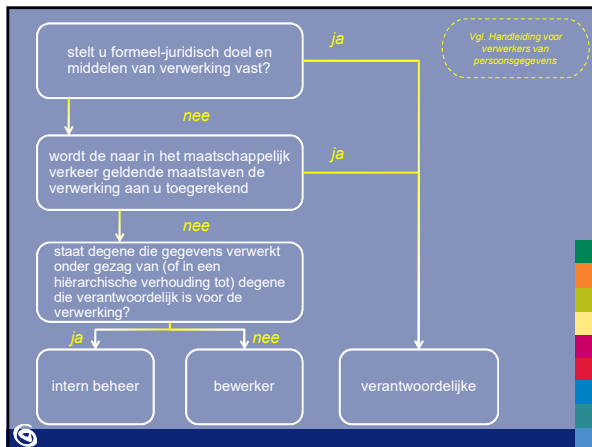
Wbp & AVG

bewerker c.q. verwerker

verwerkt persoonsgegevens ten behoeve van en onder verantwoordelijkheid van verantwoordelijke

... het bepalen van de doeleinden van de verwerking en de zeggenschap daarover doorslaggevend. Of en hoeverre de bewerker de details van verwerkingwijze van persoonsgegevens kan bepalen hangt in grote mate af van [...] de overeenkomst (met de) verantwoordelijke

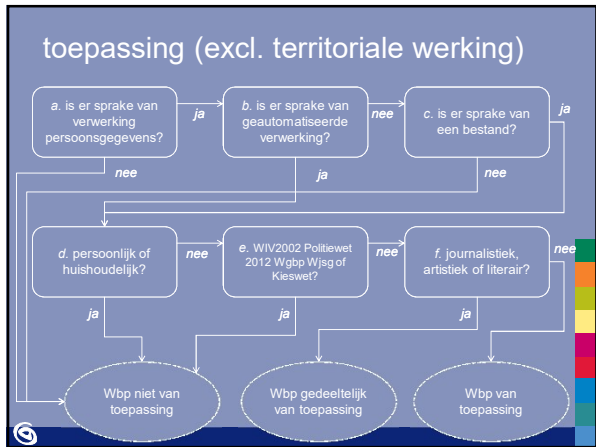
"d.w.z. overeenkomstig diens instructies en onder diens (uiddrukkelijke) verantwoordelijkheid. De bewerker is allereerst een buiten de organisatie van de verantwoordelijke staande persoon of instelling. [D]e bewerker [...] neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc."



(geautomatiseerde) verwerking persoonsgegevens

HET SPEELVELD





toepassing

- geheel of gedeeltelijk geautomatiseerd verwerking van persoonsgegevens
- en soms ook handmatig verwerking

bestand



verwerking persoonsgegevens

persoonsgegevens
gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon

kost het een onevenredige inspanning om aan de hand van het gegeven de desbetreffende natuurlijke persoon te identificeren...?

verwerking
elke handeling m.b.t. persoonsgegevens

verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (enz.)

kenteken

Hof Adam
ECLI:NL:GHAMS:2018:146

Uitgaande van de definitie van artikel 1, onderdeel a, Wbp vormt een kentekengegeven voor de heffingsambtenaar in beginsel wel een persoonsgegeven, omdat hij via Cition de beschikking krijgt over onversleutelde kentekengegevens van voertuigen die binnen de Gemeente Amsterdam geparkeerd zijn en die door hem, na gegevensverstrekking door de RDW, aan een natuurlijk persoon kunnen worden gerelateerd.



naam van rechtspersoon

Vrij Rb. Adam 16 februari 2012
LJN 916122 ("StreetView")

4.8. [...] De naam van een rechtspersoon waarin de naam van een natuurlijk persoon is verwerkt kan niet zonder meer beschouwd worden als een gegeven dat betrekking heeft op die natuurlijke persoon en daarmee onder de werkingssfeer van de Wbp worden gebracht. De band tussen een natuurlijk persoon en de rechtspersoon die zijn naam draagt kan immers zeer divers zijn.

Zelfs is mogelijk dat iedere band ontbreekt of op zeker moment gaat ontbreken zonder dat dit tot naamswijziging van de rechtspersoon leidt. Door [eiser] c.s. zijn geen feiten of omstandigheden gesteld waarom in dit geval de naam van de stichting gevestigd op de [A-straat nr] te [woonplaats], door de doorsnee gebruiker van de informatiediensten van Google met hem als persoon die ter plaatse verblijft in verband zal worden gebracht.

&
Wbp
AVG

nationaal wanbetalersregister

[D]e naam en het kvk-nummer van [eiser] [kan] als de verwerking van persoonsgegevens [...] worden aangemerkt.

[..]

Met de (handels)naam en het kvk-nummer van de onderneming van [eiser] kan immers de voor- en achternaam van [eiser] eenvoudig worden achterhaald.

Vzr Rb Adam 12 september 2014
ECLI:NL:RBAMS:2014.5936
(nationaal wanbetalersregister)

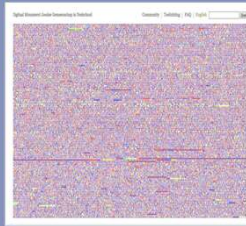


"De Wbp is slechts van toepassing op gegevens die betrekking hebben op identificeerbare natuurlijke personen die nog in leven zijn. Een identificeerbare persoon is, blijkens de wetgeschiedenis een persoon wiens identiteit zonder onevenredige inspanning kan worden vastgesteld.

Uit de enkele vermelding "overlevend kind" uit het gezin van haar wel op de website te vermelden vader kan haast onmogelijk -laat staan **zonder onevenredige inspanning**- worden afgeleid dat eiseres de dochter is van die in 1942 in Auschwitz vermoorde vader. Eiseres is dan ook geen identificeerbare persoon

overledenen

Vzr Adam 11 december 2003 LJN AN0893
(digitaal monument)



handmatige verwerking ('bestand')

gestructureerd geheel van persoonsgegevens

- dat volgens bepaalde criteria toegankelijk is, en
- betrekking heeft op verschillende personen

ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze

onderlinge samenhang

- gemeenschappelijke bestemming of
- verzameling die in de praktijk als een geheel worden beschouwd, of
- vooraf aangebrachte structuur van de verzameling of raadpleegmethodiek die samenhang brengt

Art. 1(c)
Wbp

Art. 4(6)
AVG

analoge geluidsopnamen

HR 29 juni 2007 LJN
AZ4663 (Dexia)

...Dexia [bewaart] de opnamen met het oog op haar procespositie en de banden waarop de telefoongesprekken met [verweerder] voorkomen, [zijn] reeds ontsloten door Dexia, aangezien Dexia op het overzicht van 11 mei 2005 de data en exacte tijdstippen heeft vermeld van de telefoongesprekken die zij met [verweerder] heeft gevoerd.

Voorts geldt [,] dat een financiële instelling als Dexia, [...] verplicht is technische en organisatorische voorzieningen te treffen om opgenomen telefoongesprekken en andere persoonsgegevens betreffende de opgenomen telefoongesprekken **zodanig te kunnen traceren en reconstrueren**



uitzonderingen

Art.29 Opinie Sociale Netwerken 2009

"wanneer profielinformatie ook toegankelijk is voor anderen dan zelfgekozen contactpersonen, zoals wanneer een profiel voor alle leden van een sociale netwerkdienst toegankelijk is of de gegevens kunnen worden geïndexeerd door zoekmachines, is er sprake van toegang buiten de persoonlijke of huishoudelijke sfeer"

- persoonlijke of huishoudelijke doeleinden
- Politiewet, Wet Brp, WJD, Kieswet e.d

bepaalde uitzondering voor verwerkingen met journalistieke, artistieke of literaire doeleinden



het gebruik van een camera-systeem, dat door een natuurlijke persoon aan zijn gezinswoning werd bevestigd met als doel de eigendom, de veiligheid en het leven van de eigenaren van het huis te beschermen, maar ook de openbare ruimte in beeld brengt, en waarbij video-opnames van personen met behulp van opnameapparatuur doorlopend worden vastgelegd op bijvoorbeeld een harde schijf, wordt **[niet]** aangemerkt als de verwerking van persoonsgegevens die in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht.

HvJEU 11
december 2014 C-
212/13



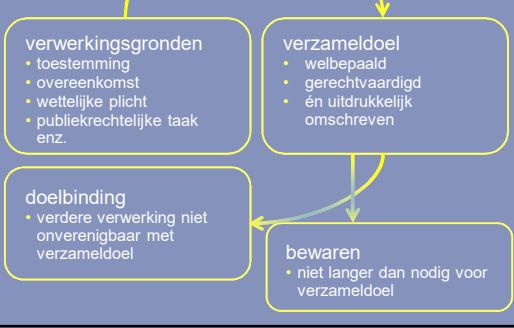


verwerkingsgrondslagen, verzamel- en verwerkingsdoelen, doelbinding, kwaliteit en beveiliging van gegevens, transparantie

DE SPELREGELS

rechtmatige verwerking

Wbp & AVG



verwerkingsgrondslagen

Wbp & AVG

- ondubbelzinnige toestemming
 - uitvoering overeenkomst
 - **wettelijke plicht** *bewaren en verstrekken van persoonsgegevens door belastingplichtigen en anderen (art. 47, 52 en 53 Awr)*
 - vrijwaring vitaal belang
 - publiekrechtelijke taak
 - gerechtvaardigd belang
- opvragen en verwerking persoonsgegevens f.b.v. belastingheffing en andere publiekrechtelijke taken (Uitvoeringsregeling Belastingdienst 2003)*
- Art. 8 a-f Wbp Art. 6(1) a-f AVG

ondubbelzinnige toestemming

- eerst informeren
- aanvaarding algemene voorwaarden met instemmingsbepaling is onvoldoende
- jonger dan 16? dan toestemming door ouders
- intrekken 'te allen tijde' mogelijk
- vrijwillig gegeven...

Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. [...]

An example of the above is provided by the case where the data subject is under the influence of the data controller, such as an employment relationship.

niet voor de hand liggend voor gemeenten!

“auto opt-in...”



please do not tick the box if you do not wish to receive our informative newsletter

vitaal belang

Bonuskaart bleek van onschatbare waarde

Gepubliceerd: 22 augustus 2003 07:58
Laatste update: 22 augustus 2003 09:40



ZAANDAM - De bonuskaart van Albert Heijn is van "onschatbare waarde" gebleken bij het terughalen van Campina-producten die in een winkel van het supermarktcconcern waren verkocht, aldus een woordvoester van Albert Heijn, onderdeel van het Ahold.

"Met de klantgegevens konden we heel snel de mensen achterhalen die het product hadden gekocht", zei ze. Het ging om enkele tientallen stuks. Volgens de woordvoester bleek na onderzoek dat één van de bij de klanten opgehaalde producten ook daadwerkelijk was "gemanipuleerd".

Albert Heijn ging tot actie over toen medio juni een vrouw ziek was geworden na het eten van het betreffende product, zogenoemde verwenkwaark van het merk Mona. Het was de tweede keer dat Albert Heijn "handelend" moest optreden, aldus de woordvoester.

proportionaliteit & subsidiariteit

privacyinbreuk niet onevenredig in verhouding tot belang waarvoor gegevens worden verwerkt

Art. 5(1)a, 6(1)
b-AVG

Art. 6, 8b-f
Wbp

belang kan niet op andere, minder belastende wijze worden gerealiseerd

verzamel- en verwerkingsdoelen

verzameldoel welbepaald uitdrukkelijk omschreven gerechtvaardigd

verdere verwerking niet onverenigbaar

- verwantschap, ver. relatie, en verwerkingsdoelen
- aard van de gegevens
- gevolgen voor betrokkene
- verkregen bij betrokkene of bij derden
- passende waarborgen

Art. 5(1)d en
6(4) AVG

Art. 7-9
Wbp

The screenshot shows a website interface with two main sections. The top section is titled 'Bereken uw premie' and compares three insurance plans: 'Basis', 'Persoonlijk', and 'Persoonlijk+'. The 'Basis' plan is described as 'Een veilig gevoel' and offers a 10% discount. The 'Persoonlijk' plan offers a 20% discount. The 'Persoonlijk+' plan offers a 30% discount. The bottom section is titled 'jouw zorg moeiteloos verzekerd' and features a first aid kit icon. It lists benefits such as '10% korting op de premie' and 'maximaal 70,- per maand'. A source attribution 'bron: @despeid' is present in the top left, and another 'bron: hema.nl' is present in the bottom right.

beveiligingsplicht

en nu ook met
meldplicht!

- passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking
- maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen
- de maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen



bijzondere gegevens

- levensovertuiging of godsdienst
- politieke gezindheid
- lidmaatschap vakbond
- ras, etniciteit
- seksuele leven
- gezondheid
- **biometrische ID-gegevens**
- **genetische gegevens**
- strafrechtelijke gegevens (e.d.)
- én BSN

Art. 9-10
AVG

Art. 16-24
Wbp

NIEUW!

verwerking bijzondere gegevens
verboden, tenzij...

- met uitdrukkelijke toestemming (enz.), of
- door bepaalde verwerkers en voor bepaalde doeleinden
- enz...

rasgegevens: verwerking mag

Art. 18
Wbp

- voorzover onvermijdelijk ter identificatie
- voorzover nodig i.v.m. positieve discriminatie
 - alleen gegevens betreffende geboorteland van de betrokkene, van diens ouders of grootouders,
 - dan wel andere, bij wet vastgestelde criteria

herkenbare foto's op
intranetsmoelenboek
of sociale netwerken
videocameratoezicht

Vgl. Rb R'dam 16 mei
2012 LJN BW5513
(voorkeursbeleid)

doel onderscheid maken...

Alléén als een verantwoordelijke foto's of ander beeldmateriaal publiceert met het **uitdrukkelijke doel** om onderscheid te maken naar ras, is bijzondere oplettendheid geboden. In dat geval acht het CBP het een **redelijke wetstoepassing** om het beeldmateriaal aan te merken als een bijzonder persoonsgegeven. **CBP richtsnoeren**

"... **[onjuist is]** dat in een geval [...] waarin de vordering uitdrukkelijk ook betrekking had op foto's van personen, toepassing van [art. 18 Wbp en 126nf Sv] alleen in aanmerking komt indien met de vordering is **beoogd** de desbetreffende gevoelige [ras] informatie aan die foto's te ontfemen" **HR 23 maart '10**

«bijz. gegevens» verwerking mag ook

- uitdrukkelijke toestemming
- door betrokkene duidelijk openbaar gemaakt
- vaststelling, uitoefening of verdediging van een recht in rechte
- volkenrechtelijke verplichting
- zwaarwegend algemeen belang
 - passende waarborgen én bij wet bepaald
 - of met ontheffing van Cbp
- wetenschappelijk onderzoek

*let op!
uitzondering is
géén
verwerkings-
grondslag!*

persoonsnummers

- nummer ter identificatie van betrokkene bij wet voorgeschreven
- alléén gebruiken ter uitvoering van betreffende wet of voor doeleinden bij wet bepaald
- besluit bsn
 - Stb. 2007, 443



twee meldplichten...



(1) melding bij toezichthouder

bij 'aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens'

(2) melding bij datasubject

bij 'waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer'



aanzienlijke kans op ernstige nadelige en/of waarschijnlijk ongunstige gevolgen

gezondheid, ethicheit, seksuele oriëntatie, politieke voorkeur, geloof, strafrechtelijk, genetisch

aard van de gegevens

- gevoelige gegevens en financieel-economische gegevens
- stigmatiserings-, uitsluitingsrisico's
- gebruikersnamen, wachtwoorden, identiteitsfraude e.d.
- beroepsgeheim

andere criteria

- omvang van lek (aantal personen of hoeveelheid gegevens)
- ingrijpendheid van o.b.v. gegevens genomen beslissingen
- olievlek (bijv. bij ketensamenwerking)
- encryptie, hashing, remote-wipe, Mobile-Iron etc.

eventueel niet melden aan datasubject bij psychosociale hulpvragen van kinderen buiten medeweten van ouders, bedrijfsovernames of risico van een bank-run



	Art. 33(1) en 34(1) AVG	Art. 34a(1) en (2) Wbp
melding bij toezichthouder	<i>tenzij onwaarschijnlijk dat er een risico is voor de rechten en vrijheden natuurlijke personen</i>	<i>aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens</i>
melding bij betrokkene	<i>waarschijnlijk hoog risico voor rechten en vrijheden van natuurlijke personen</i>	<i>waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer</i>



wél melden

- technische storing in ziekenhuis waardoor medische gegevens zijn ingezien door onbevoegden
- kopieën paspoort of rijbewijs, bank- of creditcardnrs, wachtwoorden, enz.
- laptop met onversleutelde financiële gegevens
- tablet met versleutelde gegevens, **maar geen back-up**
- **envelop met creditcardgegevens**

bestand i.d.z.v. art. 1(c) Wbp...?

niet melden

- **foutief geadresseerde brief, ongeopend teruggestuurd**
- zoekgeraakte en ongeopend teruggevonden koffer
- verloren ledenadministratie van tennisvereniging
- verpleegkundige 'leent' wachtwoord van co-assistent

'onverwijld'

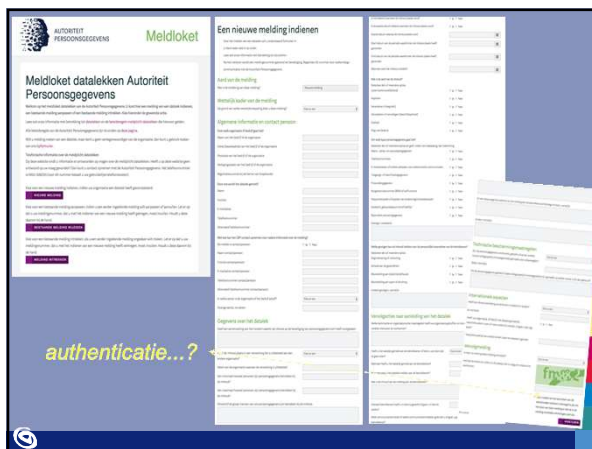
wanneer

- vanaf moment van bekend worden van datalek
- bekend bij verantwoordelijke zelf
- of bekend bij bewerker(!)

zonder onnodige vertraging

- zo mogelijk niet later dan 72 uur na ontdekking
- maar later mag als dat kan worden uitgelegd





authenticatie...?

pro forma melding (een tekstsuggestie)

"Er is naar oordeel van verantwoordelijke géén sprake van een inbreuk op de beveiliging van de persoonsgegevens. Voor het geval dat daarover verschil van inzicht kan bestaan wordt zekerheidshalve, en zonder aanvaarding van enige gehoudenheid daartoe, deze melding gedaan."





@zwnne

vragen?

zwenneblog • g.j.zwenne@law.leidenuniv.nl • @zwnne
