Bezit schept verplichtingen

“

The citizens will divide between those who prefer convenience and those who prefer privacy.

— NIELS OLE FINNEMANN, A PROFESSOR AND DIRECTOR OF NETLAB, DIGHUMLAB IN DENMARK

”

Europese Wetgeving

Richtlijn omzetten in nationaal recht – Het geeft een richting aan lidstaten, moet eerst omgezet worden.

Verordening – direct toepasbaar bijna geen discretionaire bevoegdheid.

Rion Rijker, LL.M

Privacy Jurist

Gemeente Amsterdam • Rijksuniversiteit Groningen / University of Groningen

Utrecht en omgeving, Nederland • 500+

Verwerking andere doeleinden

- (grond 50)De verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel worden toegestaan indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld. In dat geval is er geen andere afzonderlijke rechtsgrond vereist dan die op grond waarvan de verzameling van persoonsgegevens werd toegestaan. Indien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, kan in het Unierecht of het lidstatelijke recht worden vastgesteld en gespecificeerd voor welke taken en doeleinden de verdere verwerking als rechtmatig en verenigbaar met de aanvankelijke doeleinden moet worden beschouwd. De verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, moet als een met de aanvankelijke doeleinden verenigbare rechtmatige verwerking worden beschouwd. De Unierechtelijke of lidstaatrechtelijke bepaling die als rechtsgrond voor de verwerking van persoonsgegevens dient, kan ook als rechtsgrond voor verdere verwerking dienen. Om na te gaan of een doel van verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, moet de verwerkingsverantwoordelijke, nadat hij aan alle voorschriften inzake rechtmatigheid van de oorspronkelijke verwerking heeft voldaan, onder meer rekening houden met: een eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking; het kader waarin de gegevens zijn verzameld; met name de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan; de aard van de persoonsgegevens; de gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; en passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerkingen. Wanneer de betrokkene zijn toestemming heeft gegeven of wanneer de verwerking gebaseerd is op Unierecht of lidstatelijk recht dat in een democratische samenleving een noodzakelijke en evenredige maatregel vormt voor met name het waarborgen van belangrijke doelstellingen van algemeen belang, moet de verwerkingsverantwoordelijke de mogelijkheid hebben de persoonsgegevens verder te verwerken, ongeacht of dat verenigbaar is met de doeleinden. In ieder geval dient ervoor te worden gezorgd dat de in deze verordening vervatte beginselen worden toegepast en dat de betrokkene met name wordt geïnformeerd over dergelijke andere doeleinden en over zijn rechten, waaronder het recht om bezwaar te maken. Het aanwijzen van mogelijke strafbare feiten of gevaren voor de openbare veiligheid door de verwerkingsverantwoordelijke en de doorzending van de desbetreffende persoonsgegevens in individuele zaken of in verschillende zaken die met hetzelfde strafbare feit of dezelfde gevaren voor de openbare veiligheid te maken hebben, aan een bevoegde instantie moeten worden beschouwd als zijnde in het gerechtvaardigde belang van de verwerkingsverantwoordelijke. De doorgifte in het gerechtvaardigde belang van de verwerkingsverantwoordelijke of de verdere verwerking van persoonsgegevens moeten evenwel worden verboden wanneer de verwerking niet verenigbaar is met een wettelijke, beroepsmatige of anderszins bindende geheimhoudingsplicht.

Verwerking andere doeleinden

- Verwerking van persoonsgegevens voor een ander doeleind dan waarvoor ze zijn verzameld is toegestaan, mits dit doeleind verenigbaar is met het oorspronkelijke doel;

- Dit geldt sowieso voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden;

- Het kader waarin de gegevens zijn verzameld; met name de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan; de aard van de persoonsgegevens; de gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; en passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerkingen;

- Informeren betrokkene en hem de mogelijkheid geven om bezwaar te maken tegen de verwerking.

HET BRAAFSTE JONGETJE VAN DE KLAS

WBP in een notendop

- Verwerkingsgrondslag;
- Toestemming;
- Subsidiariteit & proportionaliteit;
- Rechten van betrokkene (wijzigen/verwijderen/ inzage);
- Meldplicht datalekken;
- (sub) Bewerkers & Bewerkersovereenkomsten;
- Melden van verwerking aan het AP tenzij vrijstellingsbesluit;
- Administratie van alle datalekken

Te behandelen punten

- Toestemming
- Data portabiliteit
- Recht om gegevens te verwijderen
- Boetes
- Privacy by design
- Privacy by Default
- PIA (risico analyse)
- Bewijs van toestemming
- Aanstellen DPO
- Beveiligingsmaatregelen
- Profiling
- Verwerkingsregister
- Certificering en gedragscodes
- Bestuurders aansprakelijkheid

HEB JE
JAREN GESTUDEERD

WORDT
GEZOND
BOERENVERSTAND
WEER HIP

Loesje

Postbus 1045
6801 BA Arnhem
www.loesje.nl

Casus 1 en 2

1. Henk meldt zich aan voor het PVIB. Bij het aanmelden wordt hem gevraagd of zijn gegevens gebruikt mogen worden voor een welbepaald en duidelijk omschreven doel; met dezelfde toestemming geeft hij ook toestemming voor het doorsturen van zijn gegevens naar een derde partij en voor de nieuwsbrief. Heeft het PVIB op de juiste wijze toestemming gevraagd voor elke afzonderlijke verwerking?

2. In het jaar 2040 vraagt Henk die al 20 jaar gebruikt maakt van het PVIB zich af hoe het ook al weer zat met de toestemming die heeft gegeven voor de verwerking. Is het PVIB verplicht om dit inzichtelijk te hebben?

Toestemming artikel 7

1. **De verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.**

2. H**et verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden**. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.

3. De **betrokkene heeft het recht zijn toestemming te allen tijde in te trekken**. Het intrekken van de toestemming laat de rechtmatigheid van de **verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet.** Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. **Het intrekken van de toestemming is even eenvoudig als het geven ervan.**

Toestemmingsgrond 42:Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.

Toestemming

- vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instem
- Gemakkelijk en begrijpbaar (weten waarvoor)
- Onderscheidbaar
- Gemakkelijk in te trekken
- Bijhouden wie waarvoor toestemming heeft gegeven (toestemmingsregister)
- Verdere verwerking van persoonsgegevens (ander doel) mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld
- Bewijs van toestemming geldt ook voor toestemming gegeven voor de inwerkingtreding van AVG.

Uitwerking casus 1 en 2

Dit betekent dat Henk (redelijkerwijs) begrepen moet hebben waar hij toestemming voor geeft (gemiddelde maatman) en voor elk doel afzonderlijk apart toestemming moet geven. Tenzij de andere verwerking verenigbaar is met waar de gegevens in eerste instantie voor zijn verzameld.

Ook moet de organisatie bewijs kunnen leveren over hoe en wanneer hij hiervoor toestemming heeft gegeven en Henk moet de mogelijkheid krijgen om deze toestemming gemakkelijk in te trekken.

Rechten van betrokkene

- Recht op gegevens wissing art.17
- Recht op overdraagbaarheid van de gegevens art.20
- Bezwaar tegen profilering art. 22

Casus 3 t/m 5

3. Ingrid komt erachter dat PVIB haar gegevens onrechtmatig verwerkt en dient een verwijder verzoek in. Moet de organisatie deze honoreren?

4. Is het PVIB hierna ook verplicht om Ingrid op de hoogte te stellen dat ze de gegevens hebben gewist?

5. Het PVIB komt erachter dat Ingrid op elk evenement alle pennen en notitieblokken met PVIB branding meeneemt en deze vervolgens op marktplaats tegen absurd hoge bedragen verkoopt. Onder de jeugd heeft de afkorting PVIB een hele andere betekenis waardoor de pennen en notitieblokken als hete broodjes over de virtuele toonbank gaan. Het PVIB komt hierachter en wil een civielrechtelijke procedure starten, echter stuurt Ingrid nadat ze het onderzoek zijn gestart een verwijderverzoek. Wat mag en kan het PVIB doen?

Recht op verwijdering artikel 17

Recht van betrokkene maar in sommige gevallen ook een plicht voor verantwoordelijke.

a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;

b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), berust, in, en er is geen andere rechtsgrond voor de verwerking;

c) de betrokkene maakt overeenkomstig artikel 21, lid 1, bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking overeenkomstig artikel 21, lid 2;

d) de persoonsgegevens zijn onrechtmatig verwerkt;

Recht op verwijdering artikel 17

De leden 1 en 2 zijn niet van toepassing voor zover verwerking nodig is:

a) voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;

b) voor het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;

c) om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9, lid 2, punten h) en i), en artikel 9, lid 3;

d) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, voor zover het in lid 1 bedoelde recht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;

e) voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Casus 6 en 7

6. Klaas zit al jaren bij het PVIB en wil zijn verzamelde gegevens doorsturen naar de nieuw opgezette organisatie Security4All waar hij onlangs ook lid van is geworden. Hij dient daarom bij het PVIB een verzoek in om alle gegevens die ze over hem in hun bezit hebben aan te leveren zodat hij deze bij de nieuwe organisatie kan aanleveren. Is het PVIB verplicht om hieraan te voldoen en op welke wijze?

7. Klaas vraagt aan het PVIB of ze de gegevens rechtstreeks door willen sturen naar Security4All. Technisch gezien zou dit gemakkelijk kunnen, echter is het PVIB van mening dat als Klaas zelf verantwoordelijk is voor de overdracht. Is het PVIB verplicht om aan het verzoek van Klaas mee te werken?

Dataportabiliteit artikel 20

1. De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, **in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen,** en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, **zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt**, indien:

a) **de verwerking berust op toestemming** of op een overeenkomst.

b) de verwerking via geautomatiseerde procedés wordt verricht.

2. Bij de uitoefening van zijn recht op gegevensoverdraagbaarheid uit hoofde van lid 1 heeft de betrokkene het recht dat de persoonsgegevens, **indien dit technisch mogelijk is, rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere worden doorgezonden.**

Dataportabiliteit

- Je mag altijd gebruik maken van het recht op dataportabiliteit zonder andere beperkingen, je mag ook nog van de initiële dienst gebruik blijven maken.
- Dit geldt ook voor gepseudonimiseerde data.
- Dataportabiliteit ziet ook op de data die gegenereerd is tijdens het gebruiken van de dienst. Zoals bijvoorbeeld zoekgeschiedenis, traffic data en locatiegegevens.
- Dataportabiliteit ziet ook op de data die aangeleverd is door de betrokkene.
- Bedrijven moeten op elk verzoek antwoorden, zelfs als het om gegevens gaat die ze niet kunnen delen.
- Bedrijven hebben er 1 maand te tijd om aan het verzoek te voldoen.

Bron: Article 29 working party

Bezwaar tegen profiling artikel 22

Profiling houdt in het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie. Met profiling kan een organisatie ook het gedrag van mensen voorspellen of een beslissing over hen nemen. Profiling wil dus zeggen dat iemand aan de hand van een (risico)profiel wordt beoordeeld. (bron AP)

Casus 8 en 9

Omdat Karel lid is van het PVIB en hij vaak evenementen bezoekt, heeft het PVIB een profiel over hem opgesteld. Dit is handig omdat ze hierdoor beter op zijn wensen en interesses kunnen inspelen, via bijvoorbeeld de nieuwsbrief of met de uitnodigingen voor evenementen.

Karel heeft tijdens de inschrijving expliciet toestemming gegeven voor het vormen van een profiel.

8. Kan Karel tegen de profilering bezwaar maken en op grond waarvan?

9. Stel Karel had geen expliciete toestemming gegeven verandert dit dan het antwoord van vraag 10?

Bezwaar tegen profiling artikel 22

De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder **profilering**, gebaseerd besluit **waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.**

2. Lid 1 geldt niet indien het besluit:

a) noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;

c) berust op de uitdrukkelijke toestemming van de betrokkene.

Casus 10 en 11

10. Organisatie X heeft een systeem waarin conform wet en regelgeving zeer bijzondere persoonsgegevens worden verwerkt. Dit systeem bestaat al 10 jaar en heeft in die tijd nog nooit problemen gegeven. De nieuw aangestelde Privacy Officer is van mening hier conform de AVG een risicoanalyse op uitgevoerd moet worden. Terwijl de CISO van mening is dat dit alleen moet bij nieuwe systemen conform de AVG en dat het een waste of resources is omdat het systeem al 10 jaar goed draait. Wie heeft er volgens de AVG gelijk?

11. Organisatie X verwerkt via verschillende afdelingen met verschillende partijen persoonsgegevens, de nieuwe privacy officer is van mening dat alle verwerkingen in kaart gebracht moet worden, de business is van mening dat het een waste of time is. Wie heeft er volgens de AVG gelijk?

Verantwoordelijkheden verantwoordelijke artikel 24

Verplichting om aan te kunnen tonen dat de verwerking in overeenstemming met de verordening wordt uitgevoerd. Artikel 40 en 42 stellen hierover dat dit ook kan middels gedragscodes of certificering.

Beveiliging van de verwerking artikel 32

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke onder meer het volgende :

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Dit kan door
Certificering door een bevoegd certificeringsorgaan artikel 42
Gedragscodes voor specifieke sector artikel 40
Binding Corporate Rules artikel 47 (geldt vooral als gegevens aan een derde land worden doorgezonden binnen de organisatie)

Privacy by Design artikel 25

Treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen.

Zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren.

En de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

Gegevensbeschermingseffectenbeoordeling artikel 35

Verplichting tot het uitvoeren van een risico analyse als er waarschijnlijk een hoog risico samenhangt met de verwerking. (in het bijzonder als er nieuwe technologie wordt gebruikt).

Uit artikel 36 volgt dat mocht hieruit blijken dat er een hoog risico samenhangt met de verwerkingen en de verantwoordelijke nog geen passende maatregelen heeft getroffen hij verplicht is om de AP hierover te informeren.

Register van verwerkingsactiviteiten artikel 30

Elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden.

Organisaties zijn nu zelf verplicht om een register bij te houden over de verwerking, dit hoeft dus niet meer gemeld te worden aan het AP.

LET OP: de verwerking van bepaalde gegevens kan nog steeds onderhevig zijn aan aanvullende vereisten.

Casus 12 en 13

12. Bij een organisatie vindt een datalek plaats waarbij er sprake is van een aanzienlijke kans op ernstig nadelige gevolgen dan wel ernstig nadelige gevolgen voor de bescherming van persoonsgegevens. Zijn dit voldoende criteria om volgens de AVG te melden?

13. De organisatie meldt pas na 96 uur het datalek bij de AP. Wat kan van invloed zijn om te bepalen of ze voldaan hebben aan hun wettelijke plicht of niet.

Melden aan AP artikel 33

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, **uiterlijk 72 uur** nadat hij er kennis van heeft genomen, aan de bevoegde toezichthoudende autoriteit.

tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

Casus 14 en 15

14. De organisatie treft na het datalek gelijk maatregelen om ervoor te zorgen dat het lek zich niet meer zal voordoen, aan wie moeten ze het lek allemaal melden?

15. Een datalek treft de plaatselijk bakker in het dorpje Lek die bezorglijsten bijhield met daarop NAW, allergie informatie en informatie betreffende de persoonlijke levenssfeer van betrokkene. Het gaat in totaal om 20.000 individuele records. De bakker heeft geen zin om iedereen apart te informeren dus besluit een bericht in plaatselijke krant te plaatsen want dat scheelt immers kosten, mag dit?

Melden Betrokkene artikel 34

Wanneer de inbreuk in verband met persoonsgegevens **waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen,** deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

a) Niet als de persoonsgegevens onbegrijpelijk zijn voor onbevoegden, **zoals versleuteling;**

b) ***de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;***

c) **de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.**

Casus 16

16. Onder welke omstandigheden is een organisatie verplicht om een FG aan te stellen (3 goed)?

- Bij meer dan 250 medewerkers?
- Bij het verwerking van zeer veel (bijzondere) persoonsgegevens?
- Als ze een overheidsorganisatie zijn?
- Als ze regelmatig en stelselmatig aan observatie van betrokkene doen?
- Als er ander zwaarwegende redenen zijn om dit te doen?

Aanwijzing FG artikel 37

De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin:

a) de verwerking wordt verricht door een **overheidsinstantie of overheidsorgaan**.

b) die vanwege **hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen**; of

c) **grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.**

Casus 17 en 18

17. Hoe hoog is de nieuwe boete die vanuit het AP gegeven kan worden?

- 820 duizend euro
- 10 miljoen euro of 2% van de wereldwijde omzet
- 20 miljoen euro of 4% van de wereldwijde omzet

18. Een CISO is van mening dat niet alleen alle datalekken bijgehouden moeten worden, maar hij wil een administratie bijhouden van alle beveiligingsincidenten (klein & groot). De Privacy Officer binnen de organisatie vindt dit onzin, hij is alleen geïnteresseerd in privacy inbreuken en is van mening dat alleen deze geregisterd hoeven te worden. Wie heeft er onder de nieuwe AVG gelijk?

Boetes artikel 83

Boetes zijn in twee tranches

1e is 10 miljoen euro en 2% van wereldwijde jaaromzet

2e is 20 miljoen euro en 4% van de wereldwijde jaaromzet.

Maar de AP heeft ex artikel 58 ook de mogelijkheid om corrigerende maatregelen te nemen.

Beveiligingsincidenten administreren

Artikel 33 lid 5

*De verwerkingsverantwoordelijke d**ocumenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen**. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.*

Casus 19

19. In de nieuwe AVG is bestuurdersaansprakelijkheid expliciet geregeld, waarbij bestuurders altijd hoofdelijk aansprakelijk zijn. Klopt dit?

Bestuurdersaansprakelijkheid artikel 82

Een verwerker is slechts aansprakelijk voor de schade die door verwerking is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van deze verordening of buiten dan wel in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld.

Directe bestuurdersaansprakelijkheid geldt alleen als er sprake is van:

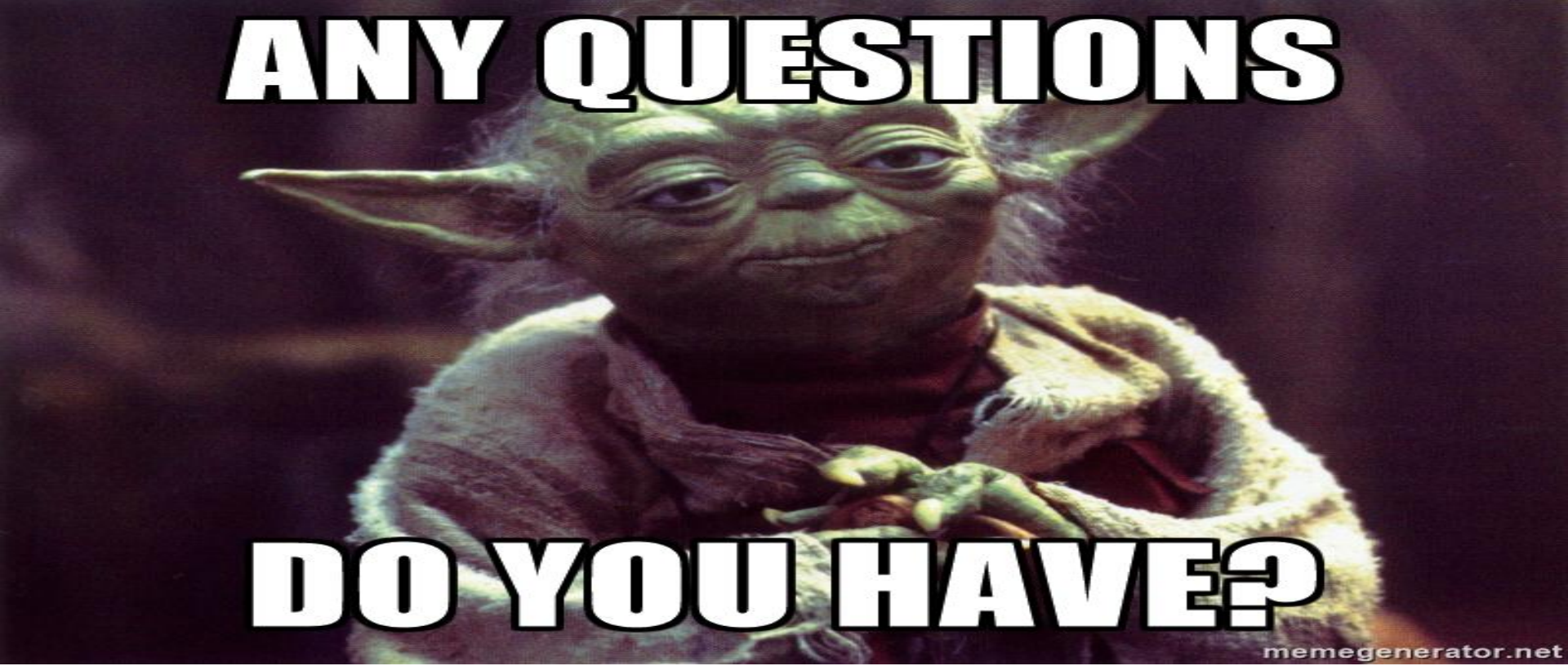
- Onbehoorlijk bestuur
- Onrechtmatige daad
- Strafbaar feit

Slavenburg II criteria

AVG in conclusie

Algemene verplichtingen

- Aanstellen FG indien van toepassing;
- Risico analyse uitvoeren indien daar aanleiding toe is (privacy by design);
- Minimalisatie van dataverwerking (privacy by default);
- Indien hoog risico en geen maatregelen dan melden;
- Privacy boekhouding (Toestemmingenregister, Verwerkerkingsregister);
- Aantonen beveiliging van de verwerking;
- Rechten van betrokkene (verwijder, inzage, wijzig, data portabiliteit, bezwaar tegen profilering)
- Alle beveiligingsincidenten administreren.



Contactgegevens: rrijker@ilionx.com of Linkedin: Rion Rijker