

ALGEMENE VERORDENING GEGEVENSBECHERMING



presentatie 23 mei 2018

© Gerhard Jansen

EUROPESE VERORDENING VAN 27 APRIL 2016




MET RECHTSTREEKSE WERKING EN
VOLLEDIGE GELDING VANAF 25 MEI 2018
IN DE GEHELE EUROPESE UNIE

Vervangt de wet bescherming persoonsgegevens.

Lidstaten kunnen aanvullende bepalingen maken.

VOORNAAMSTE WIJZIGINGEN:

- versterking en uitbreiding van privacyrechten van natuurlijke levende personen;
 - meer verantwoordelijkheden voor organisaties;
 - stevige bevoegdheden voor Autoriteit Persoonsgegevens (AP).
- 

PERSOONSGEGEVENS:

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Voorbeelden:


NAW, werkgever, inkomen, partner, kinderen, telefoonnummer, e-mailadres, foto, video, etc., etc.

Alle gegevens die herleidbaar zijn tot een persoon. Ook bestelgegevens bij Albert Heijn, de apotheek, kentekenfoto's, etc.

Bijzondere gegevens: ras, godsdienst, gezondheid, politieke partij, vakbond, seksuele geaardheid, strafdossier, biometrische gegevens. In Nederland ook: bsn.


VERBOD OP VERWERKING, TENZIJ:

- met schriftelijke toestemming van de betrokkene;
 - in het kader van een overeenkomst met betrokkene;
 - op grond van een wettelijke verplichting;
 - ter bescherming van vitale belangen;
 - in het kader van het algemeen belang;
 - bij gerechtvaardigd belang van de verwerkingsverantwoordelijke;
 - indien nodig voor indiening rechtsvordering;

 - bij bijzondere gegevens: alleen als de wet het toelaat/vereist, of na schriftelijke toestemming betrokkene.
- 

TOESTEMMING:

- moet bewezen kunnen worden, dus schriftelijk;
 - moet gevraagd worden in eenvoudige begrijpelijke taal;
 - kan ingetrokken worden, even makkelijk als het geven ervan;

 - bij kinderen jonger dan 16 jaar: door de ouder/voogd (denk aan: game industrie/internet).
- 

WAT IS VERWERKING?


Simpel gezegd: **alles tussen verzamelen en vernietigen** van gegevens.

Zoals: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Al dan niet geautomatiseerd.

Maar een privé kaartenbakje of bestand is uitgezonderd.

BEGINSELEN INZAKE VERWERKING:

- rechtmatig;
 - behoorlijk;
 - transparant;
 - voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, en alleen voor die doeleinden;
 - zo minimaal mogelijk;
 - juist en actueel;
 - niet langer dan noodzakelijk voor het doel;
 - met passende beveiliging;
 - integer en vertrouwelijk.
- 

ALGEMENE RECHTEN VAN BETROKKENE:

- recht op beknopte, transparante, begrijpelijke, makkelijke informatievoorziening in duidelijke, eenvoudige taal. Je moet daarbij levelen, denk aan informatie voor een kind;
- recht op informatie over de verwerkte persoonsgegevens, de doeleinden waarvoor deze gebruikt worden, de gegevens van verantwoordelijke voor de verwerking, de termijn van opslag, de rechten die de betrokkene kan uitoefenen, informatie over het bestaan van geautomatiseerde besluitvorming, en, bij gebruik voor een ander doel: voorafgaande informatieverstrekking daarover;
- bij gebruik van persoonsgegevens die niet van betrokkene zelf verkregen zijn: alle info over wat, waarom, hoe en over specifieke rechten: binnen een maand aan betrokkene te verstrekken.

Privacy verklaring/statement op website daarom handig, maar niet verplicht!

SPECIFIEKE RECHTEN VAN BETROKKENE:

- recht op inzage;
- recht op rectificatie;
- recht op vergetelheid;
- recht op beperking van de verwerking;
- recht op overdraagbaarheid;
- recht van bezwaar (profiling, direct marketing);
- alles ook in ketenverband;
- recht om een klacht in te dienen bij AP;

Let op: rechten zijn niet absoluut (nationale veiligheid e.d. gaan voor).

VERPLICHTINGEN VOOR VERWERKINGSVERANTWOORDELIJKE EN VERWERKER

- treffen van passende *technische* en *organisatorische* maatregelen voor een verwerking, conform de AVG, rekening houdend met de aard, de omvang, de context en het doel van de verwerking, mede gelet op de waarschijnlijkheid en ernst van uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen;
- verwerker moet dat ook waarborgen in geval van sub-verwerkers;
- vastlegging in overeenkomst verplicht (geheimhouding door medewerkers en in de keten, verwerker verwerkt alleen onder gezag en verantwoordelijkheid verantwoordelijke, hulpverlening/informatievoorziening bij inspecties en audits);
- medewerking verlenen aan toezichthouders.


VERWERKINGSREGISTER:

Bijhouden verplicht voor bedrijven > 250 personen of bij verwerking op grote schaal of van bijzondere gegevens.


Vast te leggen:

- gegevens verantwoordelijke/verwerker;
- verwerkingsdoeleinden;
- categorieën betrokkenen/persoonsgegevens;
- gegevens over doorgifte (ook aan derde landen en int. org.) (van belang bij rectificatie/vergetelheid);
- termijnen voor wissen gegevens;
- beschrijving beveiliging.

VERDERE VERPLICHTINGEN:

- melding van een inbreuk/datalek aan AP:
 - aard;
 - betrokken categorieën;
 - aantal betrokkenen;
 - impact;
 - aanpak;
 - melding datalek aan betrokkenen, tenzij versleuteling/encryptie aanwezig;
 - voorafgaande gegevensbeschermingseffectbeoordeling vóór ingebruikname grote verwerking met hoog risico, met zonodig raadpleging AP;
 - aanstelling functionaris voor de gegevensbescherming (contactpersoon AP, intern adviseur en toezichthouder, onafhankelijk) bij overheidsorganisaties, daarnaast bij organisaties met grote en risicoverwerkingen.
- 

INTERNATIONALE DOORGIFTE:

- binnen EU/EER toegelaten;
 - door EU goedgekeurde landen (bijv. Andorra, Israël, Uruguay);
 - VS en Canada, mits vallend onder specifieke wetgeving (bijv. niet Quebec);
 - anders alleen met vergunning;
 - of op basis van expliciete schriftelijke toestemming van *iedere* betrokkene of ter uitvoering van overeenkomst (denk aan reisbranche/import/export).
- 

TOEZICHT OP NALEVING:

- door nationale AP en EU AP;
 - monitoren/handhaven;
 - bevordert bekendheid/levert informatie;
 - behandelt klachten;
 - doet onderzoek;
 - bevordert certificering/best practices;
 - houdt informatie bij over inbreuken/datalekken;
 - heeft toegang tot alle bedrijfsruimten en in NL: woningen (!);
 - kan waarschuwen/berispen/gelasten/verwerkingsverbod en in NL last onder dwangsom opleggen;
 - kan geldboete opleggen.

GELDBOETE:

- hoogte afhankelijk van aard, ernst en duur van inbreuk, eventuele opzet of nalatigheid, genomen maatregelen tot schadebeperking, samenwerking met autoriteiten, etc., etc.;
- bij bijv. schending rechten kinderen, niet bijhouden verwerkingsregister, niet verlenen medewerking aan AP, beveiliging veronachtzamen e.d.: maximaal € 10.000.000 of bij bedrijven 2% van de wereldjaaromzet als dat meer is;
- bij schending basisbeginselen inzake toestemming, rechtmatigheid, verwerking bijzondere gegevens, rectificatie, vergetelheid, etc.: maximaal € 20.000.000 of bij bedrijven 4% van de wereldjaaromzet als dat meer is.

ZIN EN ONZIN/IMPLICATIES

- regels AVG bestonden grotendeels al onder WbP;
- sinds tweede helft jaren '70 wetsvoorstellen, sinds 1989 wet.
- hoe zou het met de privacy zijn zonder die wetgeving? Zou dan internet een vrijplaats zijn geweest? (Verhofstadt/Zuckerberg);
- klein, maar fijn: AVG is een afweermiddel tegen direct marketing;
- AVG is volgende grote stap in de ontwikkeling:
 - eenduidiger rechten betrokkene, waarvan nieuw: vergetelheid;
 - aanzienlijke toename administratieve lasten bedrijfsleven en organisaties;
 - omkering bewijslast!
 - AP is watching you! Met giga boetebevoegdheid.

ZIN EN ONZIN/IMPLICATIES

- veel gegevens die we als bedrijfsgegevens zien, zijn ook persoonsgegevens. Bijvoorbeeld: jansen@ejbadvocaten.nl is een persoonsgegeven, info@ejbadvocaten.nl niet. Ook voor die persoonsgegevens geldt de AVG.
- veel collectieve mails zullen we BCC moeten gaan versturen, ook als Rotary, om aan de AVG te voldoen, behoudens schriftelijke toestemming van betrokkenen voor dat doel.
- de wereld ziet de AVG als State of the Art privacy bescherming: bijv. Microsoft, Facebook en Rotary International hebben zich inmiddels gecommitteerd aan de AVG.

ZIN EN ONZIN/IMPLICATIES

- AVG geldt al sinds mei 2016;
- nauwelijks iemand was daarmee bezig tot begin 2018;
- nu iedereen, door de dreiging van de boetes!

Ter relativering:

- het aantal fte van de AP bedraagt:
2016: 72,57 2017: 102,69
- groei verwacht naar maximaal 270 fte.

Grote organisaties als eerste in het vizier.

Wie gaat er als afschrikwekkend voorbeeld aan de schandpaal?





AUTORITEIT
PERSOONSGEGEVENS

Nieuwe privacywetgeving vanaf 25 mei 2018 De AVG in een notendop



Op basis hiervan mag je persoonsgegevens verzamelen
De grondslag



Toestemming
van de gebruiker



Vitale belangen



Wettelijke
verplichting



Overeenkomst



Algemeen belang



Goedkeuring
van de bevoegde
autoriteit

Het begint aan de tekentafel
Zorgvuldigheid



Functiegerichte gegevens-
bescherming



Privacy by design



Impact assessment

Technische en organisatorische maatregelen
Verplichtingen



Register met alle
verwerkingen



Gegevens-
beschermingsbeleid



Digitale
beveiliging

Mensen moeten controle kunnen uitoefenen
Rechten van de betrokkenen



Recht om
in te zien



Recht om
te wijzigen



Recht om vergeten
te worden



Recht om gegevens
over te dragen



Recht op
informatie

De AVG geldt vanaf 25 mei 2018

Gegevens zijn
beschermd!



U heeft een goed privacyverhaal



Voor uw
doelgroep



Voor de
Autoriteit Persoonsgegevens



Aan de slag met het AVG-stappenplan!
Bereid je nu voor op de AVG

[Naar het stappenplan](#) →

