# ‘Gegevensbescherming? Regel het zelf!’
## De Algemene Verordening Gegevensbescherming en informatiemanagement

**‘In de nieuwe Algemene Verordening Gegevensbescherming (AVG) zijn (overheids)organisaties veel meer dan voorheen zelf verantwoordelijk voor de bescherming van persoonsgegevens,’ betoogt Peter Brand in een boeiend artikel over de Algemene Verordening Gegevensbescherming.**

*door Peter Brand*

**We kennen de Wet bescherming persoonsgegevens (Wbp) al sinds 2000. Toen was internet nog een betrekkelijk nieuw fenomeen en stond privacybescherming nog in de kinderschoenen. Momenteel is privacybescherming ‘hot’. En terecht, want het privacy-landschap staat de komende jaren grote veranderingen te wachten. Vanaf 25 mei 2018 geldt namelijk nog maar één privacywet in de hele Europese Unie: de Algemene Verordening Gegevensbescherming (AVG).**
**De AVG zorgt voor versterking van de privacyrechten van burgers en daarmee voor meer verantwoordelijkheden voor organisaties die persoonsgegevens verwerken.**

**Peter Brand, informatieadviseur en jurist, beschrijft in dit artikel de implicaties van de AVG voor de (overheids)organisatie.**

### Van Wbp naar AVG

Op dit moment heeft elke lidstaat binnen de Europese Unie zijn eigen privacywet. In Nederland is dit de Wet bescherming persoonsgegevens (Wbp), een uitwerking van de (oude) Europese privacyrichtlijn uit 1995.
De groei van de interne Europese markt, de snelle technologische ontwikkelingen en de globalisering hebben gezorgd voor nieuwe uitdagingen rond de bescherming van persoonsgegevens. De Europese privacywetgeving moest nodig worden herzien, daar was iedereen het over eens. Dit heeft geleid tot een voorstel van de Europese Commissie (EC) voor een Algemene Verordening Gegevensbescherming (AVG).
Op 25 mei 2016 is deze AVG in werking getreden. Organisaties moeten vanaf die datum hun bedrijfsvoering in overeenstemming brengen met de AVG en hebben daarvoor twee jaar de tijd. In de verordening is opgenomen dat deze pas op 25 mei 2018 van kracht wordt. Tot die tijd blijft de huidige Wbp gelden. Vanaf 25 mei 2018 moet iedere organisatie geheel compliant zijn aan de AVG.

**Privacybescherming is een grondrecht**

- Art. 10 lid 1 van de Grondwet,
- Art. 8 van het Europees Verdrag voor de rechten van de mens EVRM) en
- Art. 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR),

bepalen dat de privacybescherming per wet geregeld dient te zijn zodat ieders recht op privacy is gewaarborgd.

Omdat de AVG een Europese verordening is hoeft deze, anders dan een richtlijn, niet eerst te worden omgezet in nationale wetgeving. Zij heeft namelijk rechtstreekse (directe) werking.

Iedere lidstaat heeft dan dus dezelfde privacywet en iedere lidstaat krijgt een toezichthouder. Voor Nederland is dat de Autoriteit Persoonsgegevens (AP). Organisaties die in meerdere lidstaten opereren, krijgen, om de communicatie te vergemakkelijken, één toezichthouder (ook wel one-stop-shop) toegewezen,.

## Verwerken van persoonsgegevens

Volgens art 4 lid 1 AVG is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon een persoonsgegeven. Van een persoonsgegeven is sprake als een naam wordt gebruikt of een identificatienummer (zoals een telefoonnummer, klantnummer of personeelsnummer). Daarnaast kunnen ook locatiegegevens (adres, IP-adres, e-mailadres, GPS-coördinaten van een mobiele telefoon) tot de persoonsgegevens behoren. Al heel snel is dus sprake van persoonsgegevens.

Onder verwerken van persoonsgegevens vallen, volgens art. 4 lid 2 AVG, allerlei handelingen die je, al dan niet geautomatiseerd, met die gegevens verricht, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, gebruiken, opvragen, raadplegen, verstrekken, verspreiden, aligneren (combineren), afschermen, wissen of vernietigen. Aan alles heeft de opsteller van de verordening blijkbaar gedacht.
De AVG is niet van toepassing als je persoonsgegevens uitsluitend verwerkt voor persoonlijk gebruik of als opsporingsinstanties en het Openbaar Ministerie persoonsgegevens gebruiken voor de opsporing en vervolging van strafbare feiten.

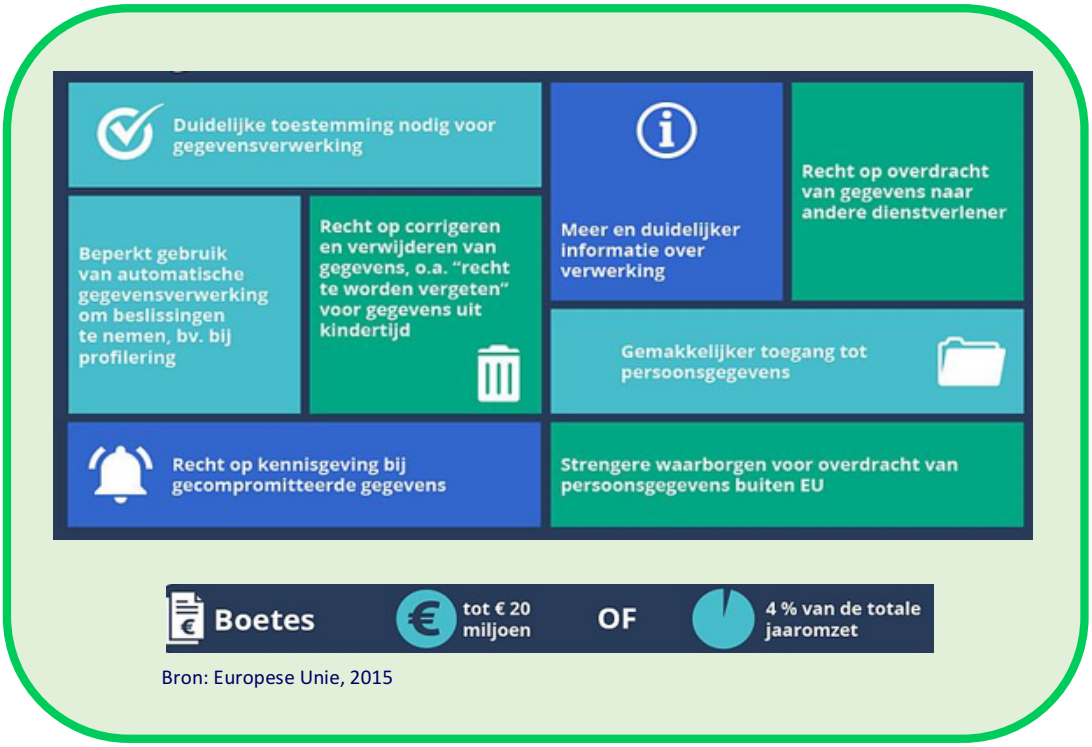
## Waarin verschilt de AVG van de Wbp?

De AVG brengt heel wat veranderingen met zich mee. Hieronder de belangrijkste tien verschillen met het huidige privacyrecht (de Wbp):

- **Accountability**.
  De AVG legt meer nadruk op de eigen verantwoordelijkheid van de organisatie om de privacybescherming na te leven. De organisatie moet kunnen aantonen dat zij zich aan de wet houdt. Iedere organisatie moet straks een actief beleid voeren waaruit blijkt dat zij de AVG naleeft: het is niet meer voldoende om alleen (tamelijk passief) de burger of klant te informeren over het doel en de middelen van verwerking.
- **Privacy by design en privacy by default**.
  De AVG verplicht organisaties hun processen en systemen voor gegevensverwerking zowel door ontwerp (privacy by design) als door standaardinstellingen (privacy by default) te laten voldoen aan de eisen van gegevensbescherming.
  Iedere organisatie moet haar producten en diensten ‘privacy proof’ ontwikkelen, bijvoorbeeld door technieken als versleuteling (pseudonimisering) toe te passen. Ook is een organisatie verplicht dat zij, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het doel dat zij wil bereiken.
- **Transparantie**.
  Iedere organisatie moet volledig transparant zijn over de gegevens die zij deelt en verwerkt. Ook moet zij actief verantwoording afleggen over de gegevensverwerking die zij toepast.
  Transparantie is in de AVG opgenomen als een apart beginsel. Het dient voor een burger of klant transparant te zijn dat zijn persoonsgegevens worden verzameld en verwerkt (dit kan bijvoorbeeld doordat de organisatie een website inricht waarbij de burger wordt geïnformeerd over de verwerking van zijn persoonsgegevens en door hem daarbij de mogelijkheid te bieden om zijn rechten m.b.t. zijn privacy uit te oefenen).

- **Documentatieplicht**.
  Je moet als organisatie met documenten kunnen aantonen dat je de juiste organisatorische en technische maatregelen hebt genomen om aan de AVG te voldoen.
  Onderdeel van deze verplichting is het bijhouden van een register waarin je documenteert welke gegevens je verwerkt, de doelen van die gegevensverwerking, welke instanties gegevens van jou ontvangen, welke beveiligingsmaatregelen je hebt getroffen en hoe lang je de gegevens wilt bewaren. De toezichthouder kan dit register op ieder gewenst moment ter controle opvragen.
  Overigens ben je, als je organisatie minder dan 250 medewerkers heeft en je niet 'stelselmatig' persoonsgegevens verwerkt, vrijgesteld van het bijhouden van een register.
- **Geen meldplicht voor verwerkingen maar wel voor datalekken**.
  Organisaties hoeven (anders dan in de Wbp) verwerkingen van persoonsgegevens niet meer te melden bij de Autoriteit Persoonsgegevens. Datalekken moeten ze wel melden. Onder een datalek valt, naast het simpel onterecht vrijkomen (lekken) van gegevens, ook onrechtmatige verwerking van gegevens. Voorbeelden van datalekken: een gestolen laptop, een verloren USB-stick met persoonsgegevens, inbraak in een databestand (hacking).
  In Nederland bestaat de meldplicht datalekken sinds 1 januari 2016. Die meldplicht is nu bijzonder strikt: een vermoeden van een lek geldt al als datalek. Onder de AVG hoef je de toezichthouder alleen te informeren als er daadwerkelijk (aantoonbaar) een lek is geweest dat een risico is voor de vrijheden en rechten van individuen.
- **Privacy impact assessment (PIA)**.
  Als een organisatie persoonsgegevens wil verwerken en dit levert waarschijnlijk een groot privacyrisico op voor personen van wie de gegevens worden verwerkt dan moet eerst een gegevensbeschermings-effectbeoordeling of PIA worden uitgevoerd.
  In de PIA wordt vastgelegd waarom, op welke manier en hoelang persoonsgegevens worden verwerkt. Daarbij moeten de aanwezige risico's worden geïnventariseerd en worden beoordeeld. Door een PIA krijgt de organisatie inzicht in wat de risico's zijn en kunnen passende maatregelen worden genomen om deze te verkleinen.
- **Functionaris gegevensbescherming**.
  Onder de AVG zijn overheidsinstanties, organisaties die stelselmatig op grote schaal personen observeren (om daarmee informatie te vergaren, bijv. d.m.v. 'GPS-tracking') of bijzondere persoonsgegevens verwerken (zoals ziekenhuizen) verplicht een functionaris gegevensbescherming te benoemen.
- **Recht op vergetelheid**.
  Personen hebben nu al het recht om een organisatie te vragen hun persoonsgegevens te verwijderen. Dat blijft zo. Bovendien kunnen ze, onder de AVG, eisen dat de organisatie de verwijdering doorgeeft aan alle andere organisaties die de gegevens hebben ontvangen.
- **Recht op dataportabiliteit**.
  Personen moeten hun persoonsgegevens kunnen meenemen van de ene naar een andere organisatie. Zij hebben het recht te eisen dat die gegevens rechtstreeks van de ene organisatie naar de andere wordt doorgezonden.
  Personen hebben ook het recht om hun persoonsgegevens van de organisatie in een standaardformaat te ontvangen. Zo kunnen ze zelf makkelijk hun gegevens doorgeven aan derden.
- **Hoge geldboetes**.
  Schending van het privacyrecht kan worden bestraft met zeer hoge geldboetes: tot 20 miljoen euro of vier procent van de wereldwijde jaaromzet van de organisatie. Ook als geen sprake is van opzet of ernstig verwijtbare nalatigheid. Bij de Wbp is dit nog een vereiste om een boete te kunnen opleggen. Bovendien zijn de boetes een stuk lager.

**De AVG: betere bescherming van persoonsgegevens**




Bron: Europese Unie, 2015

**Gegevensbescherming? Regel het zelf!**

*Van 'trust me' naar 'show me'.*
De grootste verandering in de nieuwe verordening zit hem niet in de nieuwe regels, maar in het feit dat organisaties in de praktijk nu zelf iets met die regels moeten doen.
De huidige Wbp werkt voor een groot deel op basis van vertrouwen. Een organisatie kan onder het privacyregime van de Wbp zich vaak met een 'trust me' tegenover de toezichthouder verantwoorden. Dat is bij de AVG niet langer mogelijk. De organisatie moet actief kunnen aantonen dat het AVG-compliant is ('show me').
Onder de AVG zijn (overheids)organisaties veel meer dan voorheen zelf verantwoordelijk voor de bescherming van persoonsgegevens. Het komt erop neer dat de organisatie moet laten zien dat zij zelf middels een 'Privacy impact assessment' (PIA) de risico's in kaart heeft gebracht, zelf de juiste tegenmaatregelen heeft getroffen en zelf actief controleert of de maatregelen binnen de organisatie worden nageleefd. Hiervoor moet de organisatie dus eigenlijk een 'privacy managementsysteem' (PMS) inrichten.

*Hoge boetes vooral om af te schrikken.*
De boetebedragen in de AVG zijn nogal fors. Dat betekent nog niet dat deze enorme boetes veel zullen voorkomen: boetes moeten namelijk altijd (onder de Wbp was dit al zo) evenredig zijn. De maximale boetes zullen dus vooral een afschrikkend effect hebben.
Bovendien is het opleggen van een boete een 'criminal charge' (vervolging) als bedoeld in artikel 6 van het Europees Verdrag voor de rechten van de mens. Dat betekent dat de onschuldspresumptie uitgangspunt is (de overtreder is pas schuldig als hij is veroordeeld door de rechter), de bewijslast

volledig bij de toezichthouder ligt en de rechter het bewijs en de redelijkheid van de boete volledig kan toetsen.

## Tot slot, wat betekent de AVG voor recordmanagement?

*Mogen persoonsgegevens bewaard worden?*
Persoonsgegevens mogen niet langer bewaard worden dan nodig is. Maar met betrekking tot de archiefbescheiden van overheidsorganisaties kan de Archiefwet bepalen dat een deel (lang) bewaard moet worden. Hoe verhoudt zich hier de Archiefwet tot de AVG?

Persoonsgegevens mogen alleen voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor andere daarmee onverenigbare doeleinden (doelbindingsbeginsel, art. 5 lid 1b).
In bepaalde gevallen mogen persoonsgegevens langer bewaard worden. Dit is het geval als aan de persoonsgegevens een andere, nieuwe bestemming wordt gegeven en daarmee een andere doelbinding. Volgens de AVG wordt verwerking van persoonsgegevens in het kader van archivering, wetenschappelijk of historisch onderzoek of statistische doeleinden, als een met de aanvankelijke doeleinden verenigbare rechtmatige verwerking beschouwd.

Naast een bevoegdheid om persoonsgegevens te bewaren, is het in bepaalde gevallen ook verplicht (art. 6 lid 1c van de AVG). Dit artikel bepaalt dat persoonsgegevens alleen mogen worden verwerkt, als (onder meer) de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de organisatie onderworpen is.
Zo kan ook op grond van de Archiefwet een bewaarplicht bestaan voor persoonsgegevens, namelijk indien deze persoonsgegevens in een selectielijst als ‘te bewaren’ archiefbescheiden voorkomen.
De overheidsorganisatie moet voor persoonsgegevens met een archiefbestemming wel een aantal technische en organisatorische maatregelen treffen om te zorgen dat de betreffende gegevens uitsluitend voor dat nieuwe doeleinde worden gebruikt (art. 89 AVG). Zo moeten de gegevens beperkt toegankelijk worden gemaakt.

*Stem af met eigen regelgeving:*
Een overheidsorganisatie kan in een archiefverordening, besluit archiefbeheer of in haar archiefbeheersregels het beheer van persoonsgegevens regelen. Deze regelingen moeten dan wel goed worden afgestemd op de privacyregels die een overheidsorganisatie voor het verwerken van persoonsgegevens binnen zijn organisatie opstelt (bijv. in een privacy protocol).

## Belangrijkste artikelen uit de AVG (Bijlage)

| Artikel | Onderwerp | Toelichting |
|---|---|---|
| Art. 4 | Definities | Wat zijn persoonsgegevens, wat is verwerking, wat is profilering, wat is pseudonimisering, etc. |
| Art. 5 | Beginselen inzake de verwerking van persoonsgegevens (lid 1a) | Persoonsgegevens moeten op een transparante wijze worden verwerkt, moeten toereikend zijn, juist zijn, etc. |
| Art. 6 | Rechtmatigheid van verwerking | Verwerking van persoonsgegevens is rechtmatig indien en voor zover de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden. Verwerken van persoonsgegevens zonder toestemming is mogelijk, als er een dringende noodzaak voor is (bijv. op basis van een wettelijke plicht). |
| Art. 9 | Verwerking van bijzondere categorieën van persoonsgegevens | Verwerken van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen blijken of gegevens over gezondheid, etc. zijn verboden tenzij aan bepaalde voorwaarden wordt voldaan. |
| Art. 15 | Recht op inzage van persoonsgegevens | Betrokkene heeft het recht om van de organisatie uitsluitsel te verkrijgen over het al dan niet verwerken van zijn persoonsgegevens en om inzage te verkrijgen van die gegevens. |
| Art. 17 | Recht op vergetelheid | Betrokkenen hebben het recht om 'vergeten' te worden, d.w.z. ze hebben het recht zich te laten verwijderen uit databases, tenzij legitieme wettelijke vereisten dit voorkomen. |
| Art. 20 | Persoonsgegevens in standaardformaat | Betrokkene heeft het recht om zijn persoonsgegevens in een gestructureerde, gangbare en machine-leesbare vorm te verkrijgen. Hij heeft het recht een kopie te ontvangen van de persoonsgegevens die over hem zijn verzameld. |
| Art. 20 | Recht op dataportabiliteit | Betrokkene moet zijn data kunnen meenemen naar een andere dienst. De betrokkene heeft het recht dat de persoonsgegevens (indien dit technisch mogelijk is) rechtstreeks van de ene naar de andere dienst worden doorgezonden. |
| Art. 22 | Profilering | Betrokkenen hebben het recht niet te worden onderworpen aan een louter op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit (bijv. data analytics, big data). |
| Art. 24 | Accountability | Organisaties moeten een actief beleid voeren en maatregelen treffen waaruit blijkt dat de AVG wordt nageleefd. |
| Art. 30 | Register van verwerkingsactiviteiten (documentatieplicht) | De organisatie houdt een register bij van verwerkingsactiviteiten. Het register bevat indien mogelijk ook een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1 |
| Art. 33 | Datalekken (meldplicht inbreuk persoonsgegevens) | De organisatie documenteert alle inbreuken m.b.t. persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren. |
| Art. 35 | Privacy impact assessment (PIA) | Situaties waarin een Gegevensbeschermingseffectbeoordeling of PIA verplicht is voorgeschreven. Zie lid 1 en lid 3 AVG. |
| Art. 37 | Functionaris gegevensbescherming (FG) | Aanwijzing van een FG is verplicht voor organisaties die veel persoonsgegevens verwerken (bijv. overheden). De FG is onder meer verantwoordelijk voor het naleven van de AVG. Er mag ook één functionaris worden aangewezen voor meer dan één organisatie. Gemeenten kunnen er bijv. voor kiezen gezamenlijk een functionaris aan te wijzen. |
| Art. 42 | Certificering | De Europese privacywetgeving stimuleert organisaties om een certificering op het gebied van privacy te halen. |
| Art. 83 | Maximum geldboetes (lid 4, 5, 6) | Max. € 10.000.000,- of 2% wereldwijde jaaromzet voor schending van de verplichtingen die veelal meer procedureel van aard zijn.<br>Max. € 20.000.000,- of 4% van de wereldwijde jaaromzet voor schending van de verplichtingen die veelal meer inhoudelijk van aard zijn of de privacy van de betrokkenen directer raken.<br>Max. € 20.000.000,- of 4% van de wereldwijde jaaromzet voor het niet opvolgen van een bevel van een toezichthouder. |

| | | |
|---|---|---|
| Art 89 | Waarborgen bij te bewaren persoonsgegevens (archivering) | Waarborgen i.v.m. verwerking persoonsgegevens in het kader van archivering, wetenschappelijk of historisch onderzoek of statistische doeleinden. |