
# NOG 1 JAAR, BENT U KLAAR?

# GDPR, AVG, FG, DPO, AP, PIA...volgt u het nog?

**De aangekondigde implementatie van de General Data Protection Regulation binnen de Europese Unie, oftewel de GDPR, zorgt momenteel voor een stroom aan afkortingen. In dit whitepaper nemen we u graag mee wat de afkortingen allemaal betekenen en wat hun functie is als de nieuwe privacy wetgeving binnen de EU lidstaten in mei 2018 geïmplementeerd moet zijn. Aan het eind voorzien we dit paper van een aantal practische tips en een samenvatting in de vorm van een paginakaart die laat zien wat de GDPR nu eigenlijk globaal inhoudt voor de Nederlandse markt.**

Door: Maurice van der Woude[1]

Met alle afkortingen wordt het lastig om dit kennisdocument verder te lezen, vandaar dat we beginnen met een verklarende woordenlijst van de termen die in dit document gebruikt worden:

| | |
|---|---|
| **AVG** | Algemene Verordening Gegevensbescherming |
| **GDPR** | General Data Protection Regulation, in het Nederlands "AVG" |
| **CBP** | College Bescherming Persoonsgegevens |
| **AP** | Autoriteit Persoonsgegevens, voorheen CBP |
| **FG** | Functionaris Gegevensbescherming |
| **DPO** | Data Protection Officer, in het Nederlands "FG" |
| **PIA** | Privacy Impact Assessment |

[1]Maurice van der Woude is CEO bij BPdelivery BV en specialist op het gebied van security-, kwaliteit- en (cloud)ketenmanagement

## Algemeen

De te implementeren Europese privacyverordening "Algemene Verordening Gegevensbescherming" (AVG) gaat over de '*bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens*'. Deze verordening vervangt de databeschermingsrichtlijn uit 1995. Die sloot niet meer aan op de huidige digitale wereld en de raad van de Europese Unie wilde een regulering invoeren die voor ALLE Europese lidstaten zou gelden, in tegenstelling tot de huidige versnipperde wetgeving binnen de landen van de Europese Unie in het kader van (de verwerking van) privacygevoelige gegevens.

## Waar gaat het globaal over

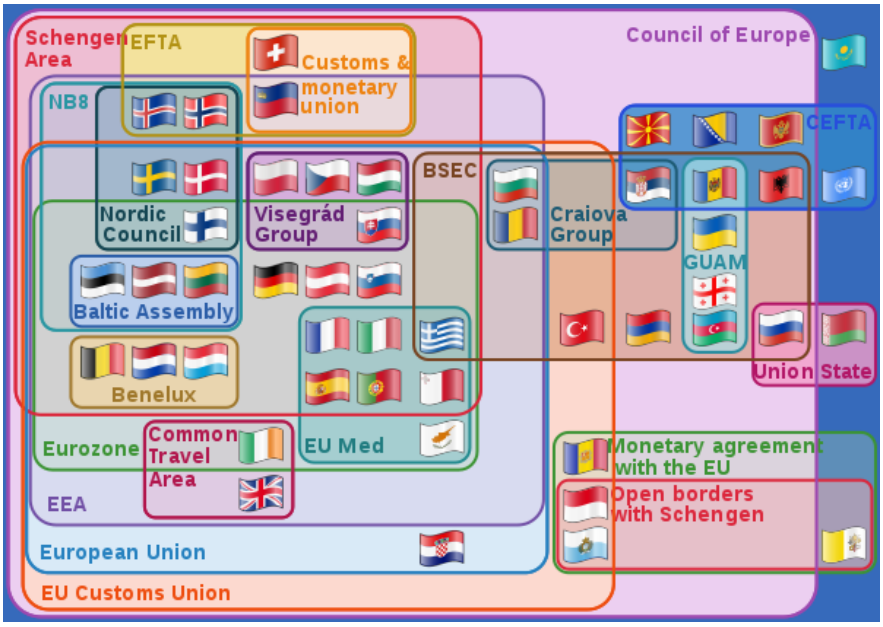
De AVG/GDPR gaat over (bescherming van) persoonsgegevens die met name in databanken worden opgeslagen en waarvan ontsluiting rechtstreeks kan leiden naar een natuurlijk persoon. Het kan zijn dat de persoon in kwestie zelf de eigen gegevens invult op een formulier via een website, maar het kan ook gaan om verwerking van persoonsgegevens in een administratie waarbij deze administratie door een ander wordt gevuld en wordt bijgehouden. De algemene principes die hierbij gehanteerd moeten worden zijn de volgende:

- **transparantie**: de persoon van wie de gegevens verwerkt worden, is hier van op de hoogte, heeft hiervoor expliciet toestemming gegeven en kent zijn/haar rechten.
- **doelbeperking**: de persoonsgegevens worden voor een vooraf bepaald en wettig doel verzameld, mogen niet voor andere zaken gebruikt worden en niet worden doorgegeven aan andere, niet ter zake doende verzameling(en)
- **gegevensbeperking**: enkel de noodzakelijke gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld
- **juistheid**: de persoonsgegevens moeten correct zijn en blijven
- **bewaarbeperking**: de persoons- gegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel. Ook moet de persoon in kwestie op verzoek verwijderd kunnen worden uit de bestanden (het zogenaamde "right to be forgotten")
- **integriteit en vertrouwelijkheid:** de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging

- **verantwoording**: de verantwoordelijke verzamelaar moet kunnen aantonen aan bovenstaande regels te voldoen

## Nu al actief binnen de Europese Unie

In tegenstelling tot wat veel organisaties denken is de AVG in mei 2016 al in werking getreden. Van organisaties wordt momenteel verwacht dat zij hun bedrijfsvoering met de AVG in overeenstemming brengen. Zij krijgen daarvoor tot 25 mei 2018 de tijd. Waar organisaties mogelijk denken dat hiervoor nog tijd genoeg is kan het soms verhelderend werken om nu al te identificeren in welke administraties of gegevensbestanden van applicaties persoonsinformatie opgeslagen en/of verwerkt wordt. Op 6 mei 2018 moeten alle EU-lidstaten deze verordening in hun nationale wetgeving hebben omgezet. Let hierbij op het feit dat het niet uitsluitend gaat over landen die met de Euro betalen, de zogenaamde "Eurozone". Het gaat hier om alle EU-lidstaten. Als u buitenlandse vestigingen heeft waar ook privacy gevoelige informatie verwerkt wordt, kan het zeker geen kwaad om te verifiëren of die vestiging ook onder de AVG valt of niet. Mogelijk zijn aanvullende maatregelen nodig. Zie voor het overzicht van de EU lidstaten het blauwe kader (European union) in de onderstaande figuur. Let erop dat het verenigd koninkrijk bij het actief worden van de verordening een aparte status heeft. Deze status is niet in de figuur verwerkt:



## Boetes

Met het bovenstaande in het achterhoofd, zal het duidelijk zijn dat vanaf 25 mei 2018 iedereen organisaties binnen de Europese Unie mag aanspreken op de naleving van de AVG. De maximale boete voor het niet naleven bedraagt 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet in het geval van een onderneming, afhankelijk van welk bedrag hoger is. Opsporingsinstanties en het Openbaar Ministerie zijn echter van de AVG vrijgesteld, omdat zij onder een aparte privacywetgeving vallen.

## EU-VS privacy schild en overigen

Het EU-VS-privacyschild is een reeds bestaande overeenkomst over de bescherming van persoonsgegevens van EU-burgers die in de VS worden verwerkt. Intercontinentale data uitwisseling dus. Ook voor die Europese landen die geen onderdeel uitmaken van de Europese Unie zal een andere regeling van kracht zijn die met name gestoeld zal zijn op de nationale privacy wetgeving van dat land. Zowel het EU-VS Privacy schild en de nationale bepalingen van overige, niet aangesloten, Europese landen blijven onder de huidige voorwaarden nog steeds actief, al gaan de discussies daarover nog steeds door. Er zijn in dit verband plannen om een "schengen 2.0" te introduceren. Hierbij is het de bedoeling om alle landen die het schengenverdrag ondertekend hebben, onderdeel te laten uitmaken van een groot Schengen Internet(werk). Eenvoudiger gesteld houdt het plan in dat er een nieuw communicatienetwerk wordt gemaakt voor alle bij het Schengenverdrag aangesloten landen, dat enkel gebruik maakt van Europese software en hardware.

## Verwerker of bewerker

In de "oude" datalekken wetgeving werd nog vaak gesproken over "verwerker" en "bewerker". Wat opvalt in de huidige verordening is dat de term "bewerker" verdwenen is en heeft plaats gemaakt voor de termen "verwerker" en

"verwerkingsverantwoordelijke". Met verwerkingsverantwoordelijke wordt de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens bedoeld. De huidige afgesloten bewerkersovereenkomsten tussen de bewerker en verwerker zullen ongetwijfeld nog steeds actueel blijven, mogelijk dat de terminologie of inhoud aanpassing behoeft om aan te sluiten bij deze nieuwe verordening. Qua melding dient de verwerkingsverantwoordelijke instantie binnen 72 uur melding te maken van een inbreuk die verband houdt met persoonsgegevens.

## Autoriteit Persoonsgegevens

De instantie in Nederland die belast is met de uitvoering en instandhouding van deze verordening (en later in 2018 dus onderdeel van de wet) is de Autoriteit Persoonsgegevens (AP), voorheen het College Bescherming Persoonsgegevens (CBP). Men kent momenteel de AP hoofdzakelijk van de invoering van de wet datalekken op 1 januari 2016 en dat de AP belast is met de uitvoering van die wet en de naleving ervan binnen Nederland. De wet datalekken blijft niet alleen van kracht, De AP krijgt er in 2018 nog meer bevoegdheden bij in het kader van uitvoering van de GDPR. De AP kan echter onmogelijk alle Nederlandse bedrijven die persoonsgegevens beheren, controleren. Hiervoor zijn bedrijven die aan bepaalde verwerkingsvoorwaarden voldoen, verplicht een functionaris gegevensbescherming aan te stellen. Deze FG moet dan ook formeel aangemeld worden bij de AP.

## Functionaris Gegevensbescherming

Een van de gevolgen van de AVG is dat binnen bedrijven die persoonsgegevens verwerken een Data Protection Officer (DPO), in gewoon Nederlands een Functionaris Gegevensbescherming (FG), aan moeten stellen. De aanstelling van een FG is verplicht onder de volgende organisaties of omstandigheden:

### Het betreft een overheidsinstantie of publieke organisatie

Hieronder vallen onder andere rijksoverheid, gemeenten en provincies, maar ook bijvoorbeeld zorg- en onderwijsinstellingen.

### Het betreffen organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen.

Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via wearables.

### Het betreffen organisaties die op grote schaal bijzondere persoonsgegevens verwerken waar dit een kernactiviteit is.

Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden. Rechtbanken zijn overigens uitgesloten van deze verplichting.

Alhoewel er geen specifieke vereisten in opleiding aan de FG worden gesteld, dient deze conform de richtlijn te voldoen aan minstens de volgende aspecten:

- Hij of zij moet ter zake gedegen kennis hebben van de persoons gegevens die door de organisatie verwerkt worden
- Hij of zij moet eenvoudig bereikbaar zijn en kunnen communiceren met zowel de (lokale) verwerkers en de nationale toezichthouder
- Hij of zij moet deskundig zijn in het toepassen van de wettelijke bepalingen die in het kader van de AVG gelden
- Hij of zij beschikt over professionaliteit en de benodigde ethiek in het kader van de AVG en de dataverwerkingen
- Er is geen belangenconflict, de FG kan boven de partijen staan maar hoeft niet perse een medewerker van de organisatie zelf te zijn

## Privacy Impact Assessment (PIA)

Bedrijven kunnen verplicht zijn een PIA uit te voeren op basis van de gegevens die zij in geautomatiseerde systemen verwerken. Een PIA is een instrument om *vooraf* de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. De Rijksoverheid is nu al verplicht om bij de ontwikkeling van nieuwe wetgeving rekening te houden met de resultaten van een PIA. Sinds 1 september 2013 moet binnen de Rijksdienst standaard een privacy impact assessment (PIA) worden

uitgevoerd. Het instrument dat is ontwikkeld bestaat uit een vragenlijst en gebruiksinstructies, is opgenomen in het Integraal Afwegingskader voor Beleid en Wetgeving en het Handboek Portfolio management. Andere organisaties zijn nu nog niet verplicht een PIA uit te voeren. Organisaties die (op termijn) een PIA verplicht uit moeten voeren, zijn die organisaties die ook de verplichting hebben om een FG aan te stellen. Mocht er toch nog twijfel zijn, dan wordt als vuistregel gehanteerd dat als minstens 2 van de 10 onderstaande criteria van toepassing zijn, de organisatie verplicht een PIA dient uit te voeren:

1. Beoordelen van mensen op basis van persoonskenmerken
2. Geautomatiseerde beslissingen
3. Stelselmatige en grootschalige monitoring
4. Gevoelige gegevens
5. Grootschalige gegevensverwerkingen
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Doorgifte van persoonsgegevens buiten de EU
10. Blokkering van een recht, dienst of contract

## Meerdere landen, 1 toezichthouder

Stel dat u een onderneming leidt die in meerdere landen actief is. Dan heeft u met deze nieuwe verordening nog maar met 1 toezichthouder te maken. Dit wordt de 'leidende toezichthouder' genoemd (lead supervisory authority). De leidende toezichthouder is als eerste verantwoordelijk voor het toezicht op organisaties met grensoverschrijdende gegevensverwerkingen. De hoofdregel is dat de toezichthouder van de EU-lidstaat waar de hoofdvestiging van een organisatie is gevestigd, de leidende toezichthouder is. Deze coördineert al haar activiteiten in samenwerking met de toezichthouders in de andere landen waar de organisatie actief is. Voor Nederland is deze toezichthouder de Autoriteit Persoonsgegevens.

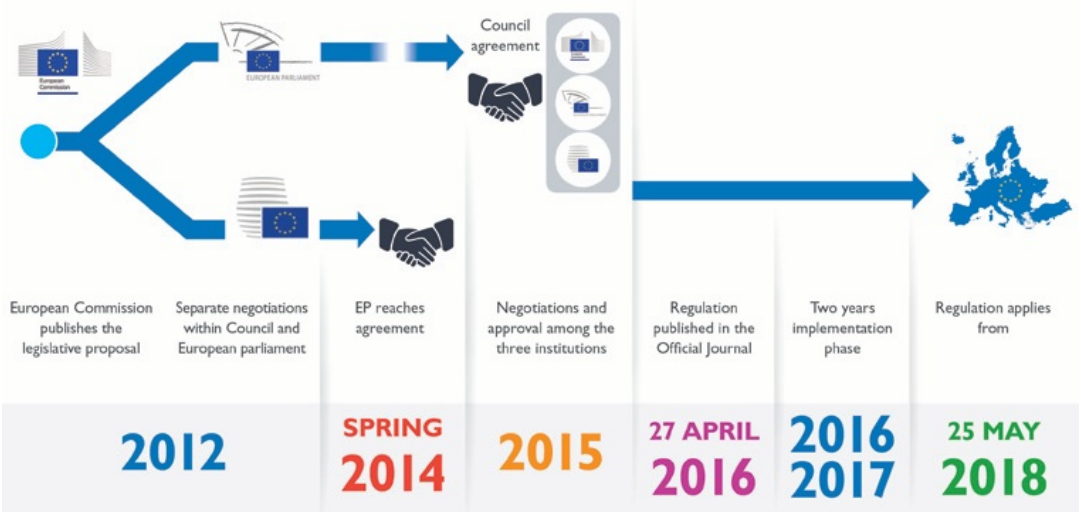
## Hoe verder

Wij kunnen ons voorstellen dat er een enorme bult van informatie op u afkomt en dat u binnen uw onderneming met behoorlijk wat kwesties rekening moet gaan houden om ervoor te zorgen dat u voldoet aan de implementatie en activering van de AVG. Wij adviseren u in ieder geval het volgende te gaan doen:

1. Identificeer welke databestanden u verwerkt waarbinnen privacy gevoelige informatie opgeslagen en/of onderhouden wordt;
2. Indien die bestanden aanwezig zijn, ga dan na of u aan de wettelijke eisen van de verordening voldoet met betrekking tot de verwerking van deze gegevens;
3. Ga, aan de hand van de 10 punten checklist onder PIA, na of uw organisatie verplicht is/kan zijn om een Privacy Impact Assessment uit te voeren;
4. Ga aan de hand van bovenstaande na of u een registratie/verwerking bij de autoriteit persoonsgegevens moet aanmelden;
5. Ga aan de hand van bovenstaande na of u een FG (Functionaris Gegevensbescherming) moet aanstellen. Deze functionaris dient u ook aan te melden bij de Autoriteit Persoonsgegevens;
6. Als u al een certificering bezit op Informatiebeveiliging (bijv. ISO2700x), u heeft een security officer of privacy officer benoemd en er is geen verplichting tot het aanstellen van een Functionaris Gegevensbescherming, ga dan na of de rol/functie van de security of privacy officer aanpassing nodig heeft op basis van deze verordening;
7. Controleer in eventueel bestaande "bewerkersovereenkomsten" of deze nog steeds voldoet aan de bepalingen vanuit de nieuwe verordening.

## De GDPR Tijdlijn

Het mag duidelijk zijn dat de complexiteit van de invoering van de GDPR in de landen niet alleen een gedegen voorbereiding vergt vanuit de beleidsmakers maar ook tijd vergt om zowel landen als organisaties te laten inlezen op de materie maar ook de invoering, en controle op naleving, is een complex systeem. Daarnaast hebben nogal wat landen hun inbreng moeten kunnen geven op de materie en moest ook het Europese parlement haar goedkeuring nog geven aan het geheel. Het zal u daarom niet verbazen dat met de eerst publicaties over dit onderwerp al in 2012 een start gemaakt is. Hieronder ziet u de tijdslijn vanaf de eerste publicaties tot de definitieve invoering.



## Meer Informatie

Wilt u meer informatie naar aanleiding van dit kennisdocument of advies hoe u uw organisatie het beste kan voorbereiden in het kader van deze wetgeving? Neemt u dan contact met ons op;

Kerkstraat 85
6871 BJ, RENKUM
The Netherlands
mail: info@bpdelivery.com
web: www.bpdelivery.com

## Over BPdelivery

BPdelivery richt zich op de optimalisatie van geautomatiseerde bedrijfsprocessen tussen service-, ICT- en facility organisaties, hun interne gebruikers en externe leveranciers. Daarnaast wordt BPdelivery veel gevraagd voor adviestrajecten op Informatiebeveiliging, kwaliteitsmanagement, NEN7510, SOC/ISAE en overige organisatie vraagstukken van strategische aard.

Geraadpleegde bronnen:

Http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL
Http://privacytrends.nl/overig/vooruitblik-de-gdpr-in-hoofdlijnen/
http://www.earonline.nl/index.php/PIA_-_Privacy_Impact_Assessment
Http://www.justitia.nl/privacy/data-protection-officer.html
http://www.ejure.nl/2015/09/schengenverdrag-2-0-meer-bescherming-van-eu-burgers-op-het-europees-internet/
https://nl.wikipedia.org/wiki/Algemene_verordening_gegevensbescherming
https://autoriteitpersoonsgegevens.nl/nl

## De AVG in een notedop