PF

GB

Servicedocument Gegevensbescherming

PENSIOEN FEDERATIE

Pensioenfederatie
De Pensioenfederatie is de overkoepelende belangenbehartiger van bijna alle Nederlandse pensioenfondsen.
Zij vertegenwoordigt namens ongeveer 215 pensioenfondsen de belangen van:

- 5,3 miljoen deelnemers
- 3 miljoen gepensioneerden
- 9,1 miljoen gewezen deelnemers.

Het overgrote deel van alle werkenden is aangesloten bij een collectief pensioenfonds.

De leden van de Pensioenfederatie beheren samen circa 1200 miljard euro.

Met dank aan de commissie Risicomanagement van de Pensioenfederatie die het initiatief nam voor de totstandkoming van dit servicedocument en PGB Pensioendiensten, afd. Legal voor hun uitgebreide inbreng.

Contactinformatie
Prinses Margrietplantsoen 90
2595 BR Den Haag

Postbus 93158
2509 AD Den Haag

T + 31 (0)70 76 20 220
info@pensioenfederatie.nl
www.pensioenfederatie.nl

Pensioenfederatie,
Den Haag, april 2017

1 Inleiding

Een grote herinrichting van de privacywetgeving is in aantocht. Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming EU 2016/679 (AVG). De huidige privacyrichtlijn (95/46/EG) en Wet bescherming persoonsgegevens (Wbp) worden op dat moment ingetrokken. De verordening heeft als doel de privacyrechten van personen te verbeteren en brengt meer en andere verantwoordelijkheden met zich mee voor organisaties die werken met persoonsgegevensbestanden. De AVG bevat belangrijke wijzigingen ten opzichte van de Wbp en is dwingendrechtelijk van toepassing op organisaties die met persoonsgegevensbestanden werken, dus ook op pensioenfondsen en pensioenuitvoeringsorganisaties. Het is dan ook voor alle betrokken organisaties van belang om tijdig voorbereidingen te treffen om te voldoen aan de nieuwe wettelijke verplichtingen en om nieuwe regels in te bedden in de bedrijfsvoering. De wijzigingen zijn ook relevant voor de toekomstige innovaties in de pensioensector op het terrein van digitale informatieuitwisseling en de toegankelijkheid voor deelnemers en werkgevers van gegevens via portalen en 'mijnpensioensites'.

Dit document zet voor u belangrijke wijzigingen op een rij die de AVG aanbrengt ten opzichte van de huidige wetgeving. Een aantal bepalingen van de AVG moet nog worden omgezet in Nederlandse wetgeving. Dat is een taak van het Ministerie van Veiligheid en Justitie. Daarnaast zullen mogelijk veel open normen via beleidsregels worden ingevuld door de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens. Het juridische kader zal zich de komende tijd dus nog verder ontwikkelen.

Dit document is, behalve om u een overzicht van belangrijke wijzigingen te geven, ook bedoeld om u attent te maken op de cultuuromslag die de nieuwe privacywetgeving in feite inhoudt ten opzichte van de oude, die overigens ook al stevige bepalingen bevat waaraan de sector moet voldoen. De nieuwe wetgeving brengt een grotere rol voor de burger met zich mee: zodra de AVG volgend jaar mei rechtskracht krijgt, moeten organisaties die werken met grote persoonsgegevensbestanden van hun 'accountability' kunnen getuigen. Dat wil zeggen dat ze aanspreekbaar zijn op een juiste omgang met privacygegevens en 'bewijs' moeten kunnen produceren van de wijze waarop ze zijn omgegaan met de persoonsgegevens van burgers. De consequenties hiervan voor de wijze waarop organisaties hun omgang met persoonsgegevens moeten documenteren en hun systemen moeten inrichten kan groot zijn. Dit alles vraagt om een actieve en alerte houding van zowel het bestuur als de uitvoeringsorganisatie.

2 Vervolgstappen

De impact van de AVG op pensioenfondsen en pensioenuitvoeringsorganisaties kan dus groot zijn. Naast het vergroten van de bewustwording met behulp van dit servicedocument, heeft de pensioensector de dringende wens geuit om te komen tot een sectorbreed kader. De komende maanden zal door een gezamenlijke inspanning van meerdere pensioenfondsen en uitvoeringsorganisaties invulling worden gegeven aan dit kader met als doelstelling te komen tot een gedragscode die de toezichthouder onderschrijft. Zowel de Autoriteit Persoonsgegevens als het Ministerie van Veiligheid en Justitie verwelkomen het dat de pensioensector het initiatief tot een dergelijk normenkader respectievelijk gedragscode heeft genomen. De nieuwe wetgeving is sterk bepaald op Europees niveau. Als gevolg hiervan is de positie van de Autoriteit Persoonsgegevens als toezichthouder een meer onafhankelijke dan de positie van DNB en de AFM.

3 Samenvatting

Per 25 mei 2018 moeten pensioenfondsen en pensioenuitvoeringsorganisaties voldoen aan de nieuwe Europese Privacyverordening (Algemene Verordening Gegevensbescherming). Er komen nieuwe verplichtingen en veel bestaande verplichtingen worden anders ingevuld. De schade bij non-compliance kan groot zijn. De maximale boete wordt € 20 miljoen of 4% van de jaaromzet, in plaats van maximaal € 820.000 nu.

Niet alleen de mogelijke boete is hoog. De privacy-toezichthouder kan ondernemingen ook verplichten hun werkwijze aan te passen en de kosten van het achteraf privacyproof maken van IT-systemen zijn enorm. Een goed begin is dus het halve werk. Daarnaast moet rekening worden gehouden met reputatieschade in geval van privacyschending.

Om op tijd klaar te zijn, zullen pensioenfondsen en pensioenuitvoeringsorganisaties, net als overigens alle andere organisaties die met grote persoonsgegevensbestanden werken, in 2017 stappen moeten zetten. Belangrijke aandachtspunten zijn:

- volledige inventarisatie gegevensverwerkingen (privacy impact assessments uitvoeren bij hoog risico verwerkingen);
- systemen instellen volgens beginselen privacy by design/privacy by default;
- passende beveiligingsmaatregelen documenteren, toepassen en indien nodig updaten;
- intern schriftelijk privacybeleid en externe privacyverklaring opstellen;
- opstellen en bijhouden schriftelijk register van alle gegevensverwerkingen;
- eventueel aanstellen van een deskundige Functionaris Gegevensbescherming (‘Data Protection Officer’);
- aanpassen huidige verwerkersovereenkomsten, afsluiten verwerkersovereenkomsten indien ontbrekend.

4 Verwerkingsverantwoordelijkheid

Hoewel een pensioenfonds volgens de AVG de eindverantwoordelijke is voor de gegevensverwerkingen die zijn uitbesteed, hebben ook de uitbestedingsrelaties zoals bijvoorbeeld pensioenuitvoeringsorganisaties de zelfstandige verantwoordelijkheid om te voldoen aan de AVG. In onderstaand schema wordt daarom geen onderscheid gemaakt tussen verplichtingen ten opzichte van verwerkingsverantwoordelijke (het pensioenfonds) en verwerker (bijvoorbeeld de uitvoeringsorganisatie).

5 Schematisch overzicht belangrijkste wijzigingen

In onderstaand schema zijn de belangrijkste wijzigingen ten opzichte van de huidige wetgeving weergegeven.

Nieuwe verplichting	Toelichting	Art. in AVG	Huidig art. Wbp
Accountability (verantwoordingsplicht)	Aantonen dat aan alle beginselen m.b.t. verwerking van persoonsgegevens is voldaan, via o.a.: • een (op schrift gesteld) privacybeleid, • een intern register van verwerkingen, • overzicht getroffen maatregelen.	5.2	N.v.t.
Data protection policy (gegevensbeschermings-beleid)	Voeren en aantonen van een passend gegevensbeschermingsbeleid.	5.2, 24.2	N.v.t.
Data protection by design & by default	De verwerkingsverantwoordelijke moet zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen treffen zoals pseudonimisering met als doel de gegevensbeschermingsbeginselen van de AVG op doeltreffende manier uit te voeren en nodige waarborgen in te bouwen ter naleving van de AVG. Een goedgekeurd certificeringsmechanisme (art. 42 AVG) kan daarbij gebruikt worden als element.	25.1, 25.2	Sluit aan bij art. 13 Wbp.
Intern volledig register	Verantwoordelijke en verwerker moeten beide een schriftelijk register aanhouden en desgevraagd ter beschikking stellen aan de AP. Dit register bevat o.m. verwerkingsactiviteiten, doeleinden, categorieën van betrokkenen en ontvangers, doorgiften, beschrijving technische en organisatorische beveiligingsmaatregelen.	30	N.v.t.
Privacy Impact Assessments ↓	Een PIA is verplicht als verwerking waarschijnlijk een hoog risico geeft voor de rechten en vrijheden van personen, gelet op aard, omvang, context of doelen ervan. De AP zal lijsten publiceren van verwerkingen waarvoor een PIA in elk geval verplicht is. Ook kan de AP lijsten publiceren van verwerkingen waarvoor een PIA niet verplicht is.	35, 40	N.v.t.

Nieuwe verplichting	Toelichting	Art. in AVG	Huidig art. Wbp
→	De PIA moet tenminste bevatten: a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd; b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden; c) een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen, gelet op de aard, omvang, context en de doeleinden van de verwerking; d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie. Bij de PIA kunnen eventuele goedgekeurde gedragscodes in aanmerking worden genomen. De AP kan conceptgedragscodes goedkeuren en maakt goedgekeurde gedragscodes bekend.		
Data Protection Officer (Functionaris Gegevensbescherming)	DPO/FG aanwijzen is verplicht als verwerking waarschijnlijk een hoog risico geeft voor de rechten en vrijheden van personen, gelet op aard, omvang, context of doelen ervan. Een concern kan één FG aanwijzen. De AVG stelt dat een FG deskundig moet zijn op het gebied van de wetgeving en de praktijk van gegevensbescherming, maar stelt geen gedetailleerde eisen. Waarschijnlijk worden deze eisen uitgewerkt in beleidsregels van de AP. De FG moet zelfstandige rol hebben en heeft een geheimhoudingsplicht en ontslagbescherming.	37.1, 38, 39	62
Verwerkersovereenkomsten	Op het ontbreken van een verwerkersovereenkomst staat in de AVG een boete. De AVG geeft concrete eisen voor verwerkersovereenkomsten, en voor een deel andere eisen dan de Wbp voorschreef.	28.3	14.2
Voorafgaande raadpleging toezichthouder	Is verplicht als PIA uitwijst dat hoog risico bestaat (zie criteria bij PIA) en het niet mogelijk is risico's te beperken. AP moet binnen 8+6 weken schriftelijk advies geven.	36.1	N.v.t.
Profiling/Big Data	Voor profiling gelden strenge regels; automatische beslissingen zijn alleen toegestaan als betrokkenen mogelijkheid hebben te protesteren tegen automatische beslissingen en een *human intervention* te eisen. Gevoelige gegevens kunnen alleen via automated decisions worden verwerkt na uitdrukkelijke toestemming.	4.4 en 22	N.v.t.
↓			

Voortdurende (deels aangepaste) verplichting	Toelichting	Artikel in AVG	Huidige verplichting in Wbp
Beginselen voor gegevensverwerking	Toegevoegd is dat in begrijpelijke taal moet worden gecommuniceerd. Moeilijk leesbare, ellenlange privacy statements zijn dus niet toegestaan. De AVG behoudt verder vrijwel gelijke beginselen voor gegevensverwerking: a) eerlijk en rechtmatig wordt: rechtmatig, behoorlijk en transparant; b) welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden, niet verder verwerkt op een wijze die onverenigbaar is blijft gelijk; c) toereikend, ter zake dienend en niet bovenmatig wordt: toereikend, ter zake dienend en beperkt tot wat noodzakelijk is; d) nauwkeurig wordt juist; e) niet langer bewaard in een vorm die identificatie toestaat dan noodzakelijk voor verwezenlijking doel (opslagbeperking) blijft gelijk; f) integriteit en vertrouwelijkheid.	5.1 5.1 (a) 5.1 (b) 5.1 (c) 5.1 (d) 5.1 (e) 5.1 (f)	6 5, 6 lid 1 7, 9 11 lid 1 11 lid 2 10 13
Rechtmatigheid van de verwerking	De limitatief opgesomde rechtmatige grondslagen voor gegevensverwerking blijven vrijwel gelijk: a) toestemming; b) noodzakelijk voor uitvoering overeenkomst; c) noodzakelijk voor voldoen aan wettelijke verplichting; d) noodzakelijk voor vitale belangen betrokkene of andere natuurlijke personen; e) noodzakelijk voor uitvoeren taak van algemeen belang/ uitvoering openbaar gezag; f) noodzakelijk voor de behartiging van gerechtvaardigde belangen, tenzij belangen van betrokkene(n) zwaarder wegen.	6	8, 9
Voorwaarden voor toestemming	Nieuw is: • toestemming per doeleinde • actieve handeling, dus geen voorgevinkte vakjes • verzoek duidelijk, beknopt, niet storend • vrije keus en kunnen intrekken zonder nadelige gevolgen • aparte voorwaarden voor toestemming in geval van kind	7 8	5 lid 2
Doelbinding	Vrijwel gelijke beginselen. Toegevoegd is dat in begrijpelijke taal moet worden gecommuniceerd. Vage omschrijvingen mogen niet.	5.1	7, 9
Minimale gegevensverwerking	De voorwaarde (de gegevensbescherming is) 'niet bovenmatig' is aangescherpt tot 'beperkt tot wat noodzakelijk is'.	5.1	11 lid 1
Juistheid gegevens	Verplichting dat gegevens 'juist en nauwkeurig' zijn is nu beperkt tot 'juist'. Materieel maakt dit waarschijnlijk weinig verschil.	5.1	11 lid 2
↓			

Voortdurende (deels aangepaste) verplichting	Toelichting	Artikel in AVG	Huidige verplichting in Wbp
Opslagbeperking/ bewaartermijn	Vrijwel gelijk.	5.1	10
Integriteit en vertrouwelijkheid	De verwerkingsverantwoordelijke moet passende technische en organisatorische beveiligingsmaatregelen hebben getroffen tegen onrechtmatige verwerking, verlies, vernietiging en beschadiging. Dit moet ook kunnen worden aangetoond, o.m. door een schriftelijk gegevensbeschermingsbeleid (art. 24.2 AVG).	5.1, 24.1	13
Verenigbaarheid verdere verwerking	De AVG laat ruimte aan lidstaten om 'verenigbaarheid' nader uit te werken. Omzetting in Nederlandse wetgeving en/of beleidsregels van de AP zullen dit begrip moeten verduidelijken.	5.1, 6.4	9
Beveiliging	Er moeten passende technische en organisatorische maatregelen worden genomen om een op het risico afgestemd beveiligingsniveau te waarborgen, die waar passend onder meer omvatten: • pseudonimisering en versleuteling van persoonsgegevens; • het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en diensten te garanderen; • het vermogen om bij fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen; • een procedure voor het op gezette tijden testen, beoordelen en evalueren van de doeltreffendheid van de beveiligingsmaatregelen.	32	13, 14
Meldplicht datalekken	Veranderde meldplicht aan AP; alle datalekken melden, tenzij niet waarschijnlijk is dat er een risico is voor rechten en vrijheden van natuurlijke personen. Melden aan betrokkenen als inbreuk een hoog risico inhoudt voor rechten en vrijheden van natuurlijke personen, tenzij vooraf versleutelingsmaatregelen zijn genomen of achteraf maatregelen zijn getroffen waardoor het hoge risico zich waarschijnlijk niet zal voordoen. AP kan verantwoordelijke verplichten tot melding aan betrokkenen.	4.12, 33.1, 33.5 34.3, 34.4	34a
Informatieverstrekking	Informatieverstrekking zowel als data direct (= van betrokkene) als indirect (= niet van betrokkene) is verkregen.	13, 14, 15	33, 34
Doorgifte	Vrijwel gelijke regels voor doorgifte, verschillende mogelijkheden zoals adequacy decision, binding corporate rules en standard contractual clauses blijven bestaan.	44 - 49	76, 78
↓			

Nieuw recht betrokkene	Toelichting	Artikel in AVG	Huidig recht
Recht op rectificatie	Veranderde procedurele aspecten, o.a. nu verplicht *onverwijld* en uiterlijk binnen 1 maand ingaan op verzoek i.p.v. binnen 4 weken.	16, 12, 19	36
Recht op beperking van de verwerking	Hiervoor moeten persoonsgegevens tijdelijk apart kunnen worden opgeslagen.	18, 19	-
Recht op overdraagbaarheid van gegevens (dataportabiliteit)	Persoonsgegevens moeten in gestructureerde, gangbare en machineleesbare vorm kunnen worden verschaft aan betrokkenen, als op basis van toestemming of overeenkomst wordt verwerkt.	20	-
Recht op vergetelheid	Komt neer op het recht van betrokkene dat zijn gegevens zonder onnodige vertraging door de verwerker moeten worden gewist indien verwerking niet langer nodig is.	17, 12, 19	36
Voortdurend (aangepaste) recht van betrokkenen	**Toelichting**	**Artikel in AVG**	**Huidig recht**
Recht van verzet/bezwaar	Dit recht moet o.a. uitdrukkelijk onder de aandacht worden gebracht, duidelijk en gescheiden van andere informatie weergegeven.	21	40, 41
Inzage	Informatieverstrekking zowel als data direct (= van betrokkene) als indirect (= niet van betrokkene) is verkregen.	13, 14, 15	33, 34