Whitepaper AVG APS Pensioen- en Inkomensteam

APS Pensioen- en Inkomensteam en de Algemene Verordening Gegevensbescherming (AVG)

1. Inleiding

Voor wie is deze whitepaper bedoeld?

Deze whitepaper is gericht aan alle betrokkenen van APS Pensioen- en Inkomensteam. APS Pensioen- en Inkomensteam maakt onderdeel uit van Summa Groep. Binnen Summa Groep horen ook de bedrijven: Summa Adviesgroep, Acura en RISE & Partners. Voor de whitepaper AVG van de andere bedrijven binnen Summa Groep verwijzen wij u naar de website van Summa Adviesgroep, Acura en RISE & Partners.

Waarom moeten wij aan de AVG voldoen?

Tussen 1995 en nu is de samenleving in snel tempo gedigitaliseerd. Er is een enorme toename in dataverkeer en de technologie ontwikkelt zich steeds sneller. Als gevolg hiervan is er een toename in het verzamelen en delen van gegevens, de risico's van cybercrime en de vraag van de gewone burger wat er met zijn of haar persoonsgegevens wordt gedaan. De wetgeving was volgens de Europese Commissie toe aan vernieuwing en daarom stelde de Commissie in 2012 de Algemene Verordening Gegevensbescherming voor. Deze wet is in 2016 in werking getreden en per 25 mei 2018 vervangt de AVG de Wet Bescherming Persoonsgegevens.

Wij zien het als onze verplichting om op een integere en veilige manier met de persoonsgegevens van onze klanten om te gaan. Met deze whitepaper geven wij inzicht in hoe wij hiermee omgaan.

2. De AVG in het kort

Op 25 mei 2018 treedt een nieuwe Europese privacywet in werking: de Algemene Verordening Gegevensbescherming (AVG). Deze verordening is internationaal ook wel bekend onder de naam General Data Protection Regulation (GDPR).

Deze regelgeving wordt in alle lokale privacywetten binnen de hele EU en Europese Economische Ruimte (EER) geïmplementeerd. De verordening geldt voor alle organisaties die producten of diensten verkopen aan burgers in Europa en hun persoonsgegevens verwerken, inclusief bedrijven op andere continenten. De verordening biedt burgers in de EU en EER meer controle over hun persoonsgegevens en moet waarborgen dat hun informatie in heel Europa goed wordt beschermd.

De nieuwe AVG vervangt de gegevensbeschermingsrichtlijn 95/46/EG. De AVG is rechtstreeks van toepassing in elke lidstaat en zal leiden tot een betere harmonisatie van gegevensbescherming tussen de EU-landen.

Hoewel veel bedrijven inmiddels al eigen privacy processen en procedures hebben vastgesteld in overeenstemming met de richtlijn, bevat de AVG een aantal nieuwe waarborgen voor EU-Burgers waarvan gegevens worden verzameld. Zodra de AVG van kracht is, dreigen er forse boetes en straffen voor gegevensverantwoordelijken en verwerkers die zich niet aan de regels houden.

De AVG maakt het noodzakelijk dat bedrijven die persoonsgegevens van EU-Burgers verwerken hun verwerkingsproces zodanig aanpassen, dat deze in lijn is met de nieuwe Verordening.

Privacy (en daarmee de AVG) heeft een hoge prioriteit binnen APS Pensioen- en Inkomensteam. Wij bereiden onze mensen, producten en diensten voor om te voldoen aan de vereisten van de AVG.

3. Definities uit de AVG

In de AVG staat (de bescherming van) privacy centraal. Voor een goed begrip van de AVG is enige kennis van de 'AVG-terminologie' noodzakelijk. Onderstaand volgen de definities van enkele kernbegrippen:

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Betrokkene: de natuurlijke persoon waarop de persoonsgegevens betrekking hebben.

Verwerkersverantwoordelijke: de natuurlijke persoon of rechtspersoon, overheidsinstantie, instelling of andere organisatie die - alleen of met anderen - de doeleinden en middelen van de verwerking van persoonsgegevens vaststelt. Soms worden de doeleinden en middelen voor de verwerking van persoonsgegevens echter bepaald door het recht van de Europese Unie of de specifieke lidstaat. In dat geval kan de gegevensverantwoordelijke (of kunnen de specifieke criteria voor het aanwijzen van een gegevensverantwoordelijke) ook worden geregeld in het recht van de Europese Unie of de specifieke lidstaat.

Verwerker: de natuurlijke persoon of rechtspersoon, overheidsinstantie, instelling of andere organisatie die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke.

Toestemming van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling de verwerking van zijn persoonsgegevens aanvaardt.

Gegevensinbreuk: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Verwerking: een bewerking (of een geheel van bewerkingen) met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

4. Onze voorbereiding op de AVG

De AVG stelt de nodige eisen aan het verzamelen, opslaan en gebruiken van persoonsgegevens, bijvoorbeeld met betrekking tot:
- Het identificeren en beveiligen van de persoonsgegevens in onze systemen
- Het voldoen aan de nieuwe transparantievereisten
- Het waarnemen en melden van gegevensinbreuken
- Het trainen van privacy medewerkers en andere werknemers.

Om ons voor te bereiden op de inwerkingtreding van de AVG zijn wij al geruime tijd bezig met de 10 belangrijkste stappen, zoals gedefinieerd door de Autoriteit Persoonsgegevens.

1. Bewustzijn
2. Rechten van betrokkenen
3. Overzicht van verwerking van persoonsgegevens
4. Data Protection Impact Assessment (DPIA)
5. 'Privacy by design' en 'privacy by default'
6. Functionaris voor de gegevensbescherming
7. Melding van gegevensinbreuken
8. Gegevensverwerkingsovereenkomsten
9. Leidende toezichthouder
10. Toestemming en wettelijk recht op verwerking van persoonsgegevens.

1. Bewustzijn

Er zijn door onze medewerkers diverse opleidingen gevolgd omtrent de AVG. Door diverse bedrijven en organisaties worden themabijeenkomsten en workshops verzorgd, die we zoveel mogelijk volgen om zo op de hoogte te zijn van de praktische uitvoering omtrent de privacyregels binnen onze beroepsgroep. Wij hebben een projectgroep AVG opgericht waarin nieuwe kennis en inzichten gedeeld worden. De leden van deze projectgroep komen uit verschillende hoeken van de organisatie en acteren als ambassadeurs van de AVG binnen de organisatie. Verder worden de diverse benodigde activiteiten tbv de komst van de AVG binnen deze projectgroep uitgevoerd en uitgewerkt.

2. Rechten van betrokkenen

Op grond van de AVG krijgen betrokkenen meer en uitgebreidere privacy rechten. Wij zorgen ervoor dat zij hun privacy rechten naar behoren kunnen uitoefenen. Wij houden rekening met hun bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering maar ook het recht op gegevensoverdraagbaarheid. Wij zorgen ervoor dat de relevante gegevens beschikbaar zijn voor onze betrokkenen.

3. Overzicht van verwerking van persoonsgegevens

Wij registreren onze gegevensverwerking. Dat wil zeggen dat wij documenteren welke persoonsgegevens wij verwerken en voor welk doel. Wij documenteren waar deze informatie vandaan komt, waar deze is opgeslagen en met wie wij deze delen.

4. Data Protection Impact Assessment (DPIA)

Bij een Data Protection Impact Assessment (DPIA) wordt de verwerking beschreven en worden de privacy risico's beoordeeld en maatregelen vastgesteld. Een (D)PIA is alleen vereist als de verwerking "waarschijnlijk tot een hoog risico voor de rechten en vrijheden van natuurlijke personen zal leiden". Op dit moment wordt een methode ontwikkeld voor het uitvoeren van DPIA's en het borgen van privacy middels procedures etc.

5. 'Privacy by design' en 'Privacy by default'

• **Privacy by design** houdt in dat bescherming van persoonsgegevens onderdeel uitmaakt van het ontwerp van producten en diensten.
• **Privacy by default** betekent dat wij technische en organisatorische maatregelen moeten nemen om ervoor te zorgen dat de verwerking van persoonsgegevens standaard geoptimaliseerd wordt voor het

specifieke doel. Daarbij mag niet meer dan de minimaal benodigde persoonsgegevens worden verwerkt om het vooraf gedefinieerde doel te bereiken.
Zowel Privacy by design als privacy by default zal opgenomen worden in bestaande procedures en bij de ontwikkeling van producten en/of diensten.

6. Functionaris voor de gegevensbescherming

Hoewel er nog geen 100% duidelijkheid is omtrent de verplichting om een Functionaris Gegevensbescherming (FG) aan te stellen, hebben wij ervoor gekozen een interne FG aan te stellen. Deze FG staat ingeschreven bij de toezichthouder, de Autoriteit Persoonsgegevens (AP), hierdoor ontstaat een directe link tussen APS Pensioen- en Inkomensteam en de toezichthouder.

Deze FG is apart te benaderen voor zowel medewerkers als klanten en andere betrokkenen via het emailadres: FG@summa.nl. Hier kunt u terecht voor al uw vragen omtrent privacy en de daarmee samenhangende rechten en plichten in de nieuwe AVG.

7. Melding van gegevensinbreuken

Wij dienen alle gegevensinbreuken te documenteren. In geval van een gegevensinbreuk moeten wij deze goed gedocumenteerd melden aan de leidende toezichthouder. De leidende toezichthouder moet kunnen vaststellen of wij hebben voldaan aan de rapportageplicht. Wij hebben een intern protocol voor datalekken en een intern register voor datalekken. Het protocol zal worden herzien en daar waar nodig aangepast aan de vereisten van de AVG.

8. Gegevensverwerkingsovereenkomst

Voor onze gegevensverwerking zijn wij op sommige gebieden aangewezen op diverse externe verwerker(s). U kunt hierbij denken aan onze ICT ondersteuner waar uw gegevens veilig op een back-up opgeslagen worden of vergelijkingssoftware waar wij voor u de beste verzekeraar opzoeken.
De bestaande bewerkersovereenkomsten die wij reeds hebben met de diverse bedrijven zullen worden omgeschreven naar verwerkersovereenkomsten. Daar waar nodig zullen verwerkersovereenkomsten met de bedrijven aangegaan worden.

9. Leidende toezichthouder

Onze gegevens verwerking vindt niet plaats in meerdere EU-lidstaten. Voor APS Pensioen- en Inkomensteam is de Autoriteit Persoonsgegevens (AP) de leidende toezichthouder.

10. Toestemming en wettelijk recht op verwerking van persoonsgegevens

Binnen de AVG is het verzamelen en verwerken van persoonsgegevens slechts onder een van de volgende omstandigheden legitiem:
• als de betreffende persoon (de ‘betrokkene’), na voldoende te zijn geïnformeerd, ondubbelzinnig toestemming heeft gegeven; of
• als de gegevensverwerking nodig is voor een contract, bijvoorbeeld voor facturering, een sollicitatie of een lening aanvraag; of
• als verwerking vereist is op grond van een wettelijke verplichting, of
• als verwerking noodzakelijk is om het vitale belang van de betrokkene te beschermen, bijvoorbeeld de verwerking van medische gegevens van een slachtoffer van een auto-ongeval; of
• als verwerking noodzakelijk is voor het vervullen van taken van algemeen belang of die door de overheid, de belastingdienst, de politie of andere overheidsorganen worden uitgevoerd; of
• Indien de gegevensverantwoordelijke of een derde daartoe een legitiem belang heeft, mits dit belang de belangen van de betrokkene niet schaadt of inbreuk maakt op zijn grondrechten, met name het recht op

privacy. Deze bepaling schrijft voor dat er een redelijk evenwicht moet bestaan tussen de zakelijke belangen van de gegevensverantwoordelijke en de privacy van de betrokkene. De AVG verbiedt de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakbond en de verwerking van gegevens over de gezondheid of het seksleven, tenzij aan een van de uitzonderingscriteria is voldaan. Voor het verwerken van medische gegevens mbt hypotheken en/ of verzekeringen voldoen wij aan de uitzonderingscriteria.

Voor alle (persoons)verwerkingen is het noodzaak om in beeld te hebben welke grondslag hiervoor van toepassing is. Deze worden momenteel in kaart gebracht en daar waar nodig in overeenstemming gebracht met de AVG.

5. Privacy kaart

Deze kaart geeft in vogelvlucht inzicht in hoe wij met uw persoonsgegevens omgaan.

Welke soorten persoonsgegevens verwerken wij?

- Contactgegevens
- Identificatiegegevens
- Gegevens i.v.m. dienstverband
- Financiële gegevens
- Gegevens i.v.m. financiële producten
- Gezondheidsgegevens (in sommige gevallen)
- Gegevens over strafrechtelijke feiten (in bijzonder gevallen)

Waarvoor verwerken we persoonsgegevens?

- Adviseren en bemiddelen financieel product
- Uitvoeren overeenkomst financieel product
- Voldoen wettelijke verplichting (zorgplicht)
- Marketingactiviteiten
- Relatiebeheer
- Versturen nieuwsberichten

Wanneer mogen wij uw persoonsgegevens verwerken?

Als dit noodzakelijk is voor uitvoering van onze overeenkomst met u

Als dit noodzakelijk is om te voldoen aan wettelijke verplichtingen die op ons rusten

Als dit toegestaan is in kader van onze bedrijfsactiviteiten, waarbij wij uiteraard uw belang in acht nemen

Als u uitdrukkelijk toestemming hebt gegeven voor specifiek benoemde doeleinden

Hoe lang bewaren wij persoonsgegevens?

- Zolang we deze nodig hebben, in ieder geval gedurende de looptijd van onze relatie of overeenkomst.
- Gedurende de wettelijke bewaartermijnen die voor ons gelden.

Hoe kunt u controle uitoefenen op verwerking van uw gegevens?


Informatie of wij gegevens van u verwerken


Aanpassing van gegevens


Inzage in uw gegevens


Beperking van gegevens


Bezwaar tegen gebruik gegevens


Wissen van gegevens


Overdracht van gegevens

Let op: wij kunnen mogelijk niet in alle gevallen tegemoet komen aan een verzoek, bijvoorbeeld in verband met wettelijke bewaartermijnen. Als dit het geval is, zullen we u dit gemotiveerd laten weten.

Hoe beveiligen wij persoonsgegevens?

We zorgen voor passende technische en organisatorische beveiligingsmaatregelen.

Wat dient u nog meer te weten?

- Wijzigingen van de privacy statement: op onze website vindt u altijd het meest actuele statement.
- Klachtrecht: neem contact met ons op. U kunt ook een klacht indienen bij de Autoriteit Persoonsgegevens. Kijk daarvoor op www.autoriteitpersoonsgegevens.nl.

Contact

- naam kantoor: APS Pensioen- en Inkomensteam
- telefoon: 0418 65 41 41
- e-mail: FG@summa.nl
- website: www.helderoverpensioen.nl
- postadres: Koeweistraat 2, 4181 CD Waardenburg.