

AVG - VERKLARING VOOR WERKGEVER(S)

v1, MEI 2018

Geachte werkgever(s),

Middels deze verklaring geeft het pensioenfonds u inzicht in de technische –en organisatorische maatregelen die AZL, als verwerker van ons fonds, heeft getroffen om te garanderen dat op een bewuste en veilige wijze met gegevens wordt omgegaan en hiermee de privacy wordt gewaarborgd. Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten als ook met de aard, de omvang, de context en de verwerkingsdoeleinden en de waarschijnlijkheid en ernst van uiteenlopende risico's voor de rechten en vrijheden van personen. Afspraken hieromtrent zijn ook vastgelegd in de verwerkersovereenkomst tussen AZL en het fonds.

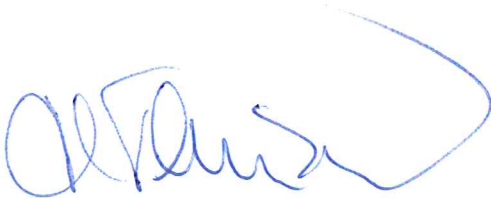
In de AVG wordt geschreven: *'persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid“).'*

De technische en organisatorische maatregelen worden in stand gehouden, geëvalueerd, en indien nodig aangepast om de persoonsgegevens te beveiligen tegen vernietiging, verlies, vervalsing, niet toegelaten verspreiding of ongeautoriseerde toegang, dan wel enige vorm van onrechtmatige verwerking en de continuïteit, betrouwbaarheid en beschikbaarheid van de gegevensverwerkingen en hulpmiddelen te waarborgen.

Door middel van passende technische en organisatorische maatregelen, borgt AZL dat:

- a) het informatiebeveiligingsbeleid voldoet aan de algemeen geaccepteerde normen binnen de informatie(beveiligings)technologie en in overeenstemming is met de toepasselijke wet- en regelgeving waaronder de AVG en de normen zoals opgelegd door De Nederlandsche Bank (DNB);
- b) AZL voorzieningen treft voor een adequate toegangsbeveiliging tot de voor de werkzaamheden relevante persoonsgegevens, zodat alleen daartoe geautoriseerde medewerkers toegang hebben;
- c) daar waar nodig AZL een privacy impact assessment (PIA) uitvoert zodat de privacy risico's in kaart worden gebracht teneinde te bepalen welke maatregelen genomen moeten worden om deze risico's te mitigeren;
- d) bij verwerking van persoonsgegevens:
 - I. het principe van privacy by design (gegevensbescherming door ontwerp) in acht wordt genomen door rekening te houden met de privacy van betrokkenen bij het ontwerp van de bij de verwerking gehanteerde mechanismen en systemen;
 - II. het principe van privacy by default (gegevensbescherming door standaardinstellingen) in acht wordt genomen door het zodanig instellen van standaardinstellingen dat de privacy van betrokkenen zoveel als mogelijk wordt gewaarborgd;
 - III. daar waar nodig en voor zover mogelijk persoonsgegevens worden geanonimiseerd, gepseudonimiseerd of versleuteld;

- IV. uitsluitend die persoonsgegevens worden verwerkt die nodig zijn voor de uitvoering van de werkzaamheden in het kader van de overeenkomst (dataminimalisatie).
- e) AZL zorgdraagt voor adequate back-up, recovery- en uitwijkfaciliteiten en deze ten minste eenmaal per jaar test en zo nodig bijstelt.
 - f) AZL adequate en actuele maatregelen treft om risico's op het gebied van cyberveiligheid, zoals kwaadaardige software waaronder computervirussen te voorkomen, op te sporen en als het zich voordoet de impact daarvan te mitigeren;
 - g) AZL op gezette tijdstippen de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking van persoonsgegevens test en zo nodig bijstelt.



Mw. C.P.M. Teunissen
Voorzitter



Dhr. W.L.M. Schapendonk – Van Horne
Secretaris