Regeling datalekken

SBZ Pensioen is een handelsnaam van Stichting Bedrijfstakpensioenfonds Zorgverzekeraars kvk 41178751

Inhoud

Inleiding

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) in werking getreden. Sindsdien geldt een meldplicht voor datalekken. Deze meldplicht houdt in dat het fonds Datalekken onverwijld moeten melden aan:

- de Autoriteit Persoonsgegevens (AP),
- in bepaalde gevallen aan De Nederlandsche Bank[1], en
- in bepaalde gevallen aan de betrokkene(n).

Kenmerken van een Datalek zijn dat het een inbreuk vormt in verband met persoonsgegevens en daarmee is het te kwalificeren als een Integriteitsincident conform de Integriteitsincidentenregeling van het fonds. Waar in de Regeling Datalekken (de regeling) gesproken wordt over een incident heeft dat dus uitsluitend betrekking op een Datalek, tenzij specifiek anders aangegeven.

Als een incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens, is er geen sprake van een Datalek maar van een beveiligingsincident (zijnde een IT-incident met uitsluitend operationele gevolgen), dat afgehandeld wordt als een Operationeel Incident volgens de Operationele Incidentenregeling. Melding aan de Autoriteit Persoonsgegevens (AP) of aan eventuele betrokkenen is dan niet nodig, het beveiligingsincident dient echter wel opgenomen te worden in het incidentenregister net als feitelijke Datalekken. De Uitvoerende Bestuursleden analyseren ieder beveiligingsincident en adviseren of het nodig is om aanvullende beheersmaatregelen te implementeren om herhaling te voorkomen.

Artikel 1 Definities

Betrokkene Wbp: Degene op wie een persoonsgegeven betrekking heeft (artikel 1f, Wbp).

Beveiligingsincident: een IT-incident met uitsluitend operationele gevolgen, dat niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens. Er is daarbij geen sprake van een Datalek.

Datalek: een inbreuk op de beveiliging (zoals bedoeld in artikel 33 en 34, AVG) waarbij persoonsgegevens zijn blootgesteld aan vernietiging, verlies, wijziging, gelekt of gedeeld zijn aan- of met een verkeerde of onbevoegde ontvanger, of er sprake is van een andere onrechtmatige verwerking[2]. Er zijn drie soorten datalekken:

1. **Inbreuk op de vertrouwelijkheid**: Hierbij zijn persoonsgegevens openbaar gemaakt of is er toegang geweest tot persoonsgegevens door iemand die daartoe niet bevoegd is, of per ongeluk.
2. **Inbreuk op de integriteit**: Persoonsgegevens zijn gewijzigd door iemand die daartoe niet bevoegd is, of per ongeluk.
3. **Inbreuk op de beschikbaarheid**: De organisatie kan niet meer bij de persoonsgegevens komen, of de gegevens zijn (per ongeluk) vernietigd door iemand die daartoe niet bevoegd is.

Afhankelijk van de omstandigheden kan een datalek in meer dan één van deze categorieën vallen

Functionaris gegevensbescherming: diegene die is aangewezen om als zodanig voor het fonds te fungeren. Dit is de heer Albert de Jong, bereikbaar via a.dejong@compliance-instituut.nl, 088-99 88 100 of 06-83 17 29 15.

[1] Pensioenfondsen zijn gehouden toezichtincidenten te melden bij DNB. Het gaat om incidenten die het vertrouwen in het pensioenfonds of financiële markten kunnen schaden. Daaronder kunnen ook IT-incidenten vallen waarbij bijvoorbeeld persoonlijke informatie van deelnemers uitlekt door een beveiligingslek.

[2] Dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 5 onder f, AVG) bescherming moesten bieden.

Incident: een gedraging of gebeurtenis die een ernstig gevaar vormt of kan vormen voor de beheerste en integere bedrijfsuitoefening van het fonds inclusief een datalek zoals gedefinieerd in de Algemene Verordening Gegevensbescherming.
Integriteitsincidenten: incidenten met een of meerdere kenmerken van een (ernstig) integriteitsincident zijn een gedraging of gebeurtenis als die in ieder geval:

a. Een strafbaar feit oplevert,
b. een schending inhoudt van interne of externe regelgeving of beleidsregels, waaronder de gedragscode,
c. autoriteiten of personen die belast zijn met de uitvoering van of het toezicht de naleving van wettelijke regelingen, of wettelijke opsporingsambtenaren beoogt te misleiden,
d. beoogt dat informatie over de hiervoor genoemde feiten wordt achtergehouden of,
e. op enigerlei wijze direct of indirect de goede naam van het fonds kan schaden.
f. leidt tot datalekken zoals beschreven in artikel 33 en 34 AVG (ook als zij een IT-component kennen).
g. leidt tot een Misstand, waarbij het maatschappelijk belang in het geding is bij de schending van een wettelijk voorschrift, een gevaar voor de volksgezondheid, een gevaar voor de veiligheid van personen, een gevaar voor de aantasting van het milieu of een gevaar voor het goed functioneren van het fonds als gevolg van een onbehoorlijke wijze van handelen of nalaten. Ook ongewenst gedrag kan in bepaalde situaties een misstand zijn.

- IT-incident met een of meerdere kenmerken van een (ernstig) Integriteitsincident: een incident (op zichzelf staande- of als onderdeel van een samenhangende gebeurtenis) die de veiligheid van een netwerk en informatiesystemen negatief beïnvloedt en/of negatieve gevolgen heeft op de beschikbaarheid, betrouwbaarheid, integriteit of vertrouwelijkheid van (persoons)gegevens en/of de diensten die aangeboden worden vanuit of namens het fonds. Het fonds beschikt over een aparte procedure voor het melden van IT-incidenten.

Melder: iedere persoon die in het kader van de Regeling datalek een melding doet van een Datalek.

Persoonsgegeven: elk gegeven (of combinatie van gegevens) betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4, AVG).

Toezichthouder: De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de fiscus en overige publieke toezichtorganen met jurisdictie ten aanzien van (de werkzaamheden van) SBZ Pensioen.

Verbonden persoon (overeenkomstig artikel 1.1 van de gedragscode van SBZ Pensioen):

a. De leden van het Bestuur van SBZ Pensioen (verder: het fonds);
b. De leden van het Verantwoordingsorgaan van het fonds;
c. Externe leden van commissies;
d. Sleutelfunctiehouders;
e. het Bestuur kan andere (groepen van) personen als verbonden persoon aanwijzen.

Medewerkers van uitbestedingspartners zijn geen Verbonden personen, tenzij deze op basis van lid e van dit artikel wel als zodanig door het Bestuur zijn aangewezen. Het fonds heeft afspraken met uitbestedingspartijen over het verplicht melden van incidenten aan het fonds.

Verwerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 4 AVG). De Pensioenuitvoeringsorganisatie (PUO) is in veel gevallen een verwerker. In

sommige gevallen is een PUO ook een Verwerkingsverantwoordelijke, maar alleen voor zover de PUO zelf het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerkingsverantwoordelijke: De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4, AVG). Het fonds is de verwerkingsverantwoordelijke.

Verwerking van persoonsgegevens: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 4, AVG).

Artikel 2 Identificeren datalek

Met Verbonden personen en derde (PUO) is afgesproken om zonder onnodige vertraging, doch uiterlijk binnen 48 uur nadat Verbonden personen of derde (PUO) een (mogelijk) datalek heeft geconstateerd, de Uitvoerende Bestuursleden, direct of via bestuursondersteuning, hiervan in kennis te stellen. De Uitvoerende Bestuursleden, direct of via bestuursondersteuning, stellen de Functionaris Gegevensbescherming (hierna 'FG') direct op de hoogte van de melding.

Daarnaast informeert de Verbonden persoon of derde (PUO) het fonds zo mogelijk niet later dan 48 uur nadat het (mogelijk) Datalek is geconstateerd accuraat over:

a. de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van Persoonsgegevens en (kring van) de betrokkenen;
b. de maatregelen die de derde (PUO) heeft getroffen of voorstelt te treffen om de (negatieve) gevolgen van de inbreuk te beperken en te verhelpen.
c. desgevraagd aanvullende gegevens die het fonds nodig heeft om een eventuele melding bij de toezichthouder te kunnen verrichten.

Artikel 3 Beoordeling datalek ja/nee

Op basis van de verkregen informatie en bij vermoeden van een datalek wordt door de Uitvoerende Bestuursleden, direct of via bestuursondersteuning, met inachtneming van de wettelijke termijn van 72 uur voor melding aan de AP, zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een Datalek, hierbij wordt tevens advies van de FG ingewonnen. De beoordeling of er sprake is van een incident, dat gemeld moet worden aan de AP komt tot stand met behulp van de WP29 guidelines on data breach notification (6 februari 2018). Tevens wordt beoordeeld of er per direct maatregelen genomen moeten worden om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen en/of de AP.

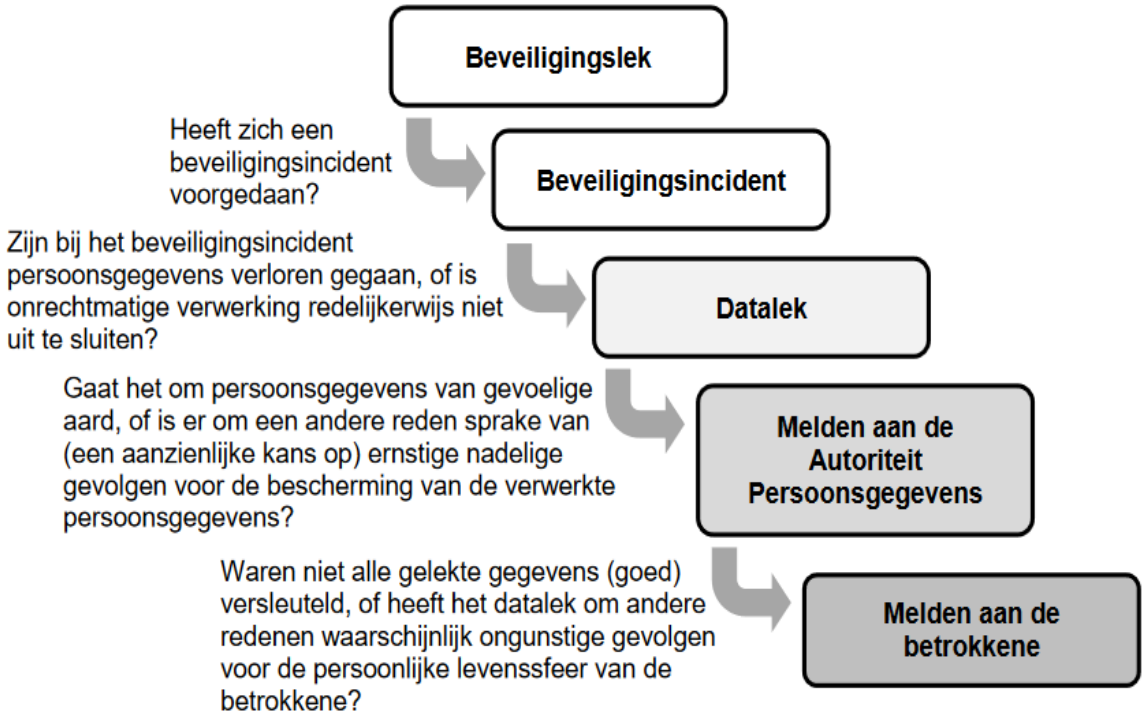
Artikel 4 Melden aan de Autoriteit Persoonsgegevens

De Uitvoerende Bestuursleden doen de tijdige (onverwijld, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek) elektronische melding bij de AP volgens het online meldingsformulier van de AP. Zij fungeren als contactpersoon inzake communicatie naar de AP. Dit geldt ook in geval nog niet duidelijk is of het Incident een Datalek is. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het Incident de melding aan te vullen dan wel in te trekken. Indien de concrete situatie zich daartoe leent, zullen de Uitvoerende Bestuursleden aan de derde (PUO)

vragen de melding aan de Autoriteit Persoonsgegevens te doen en hen op de hoogte te houden van de melding[3]. De Verwerkingsverantwoordelijke (veelal de PUO) moet zelf ook een melding doen aan de AP.

Artikel 5 Beoordeling of datalek gemeld dient te worden aan betrokkene(n)

De Uitvoerend Bestuursleden stellen samen met de Functionaris Gegevensbescherming van SBZ Pensioen en op basis van informatie van de PUO vast of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat. Zij maken hierbij gebruik van de WP29 guidelines on data breach notification en het advies van de FG van het fonds. Een schematische weergave van deze guideline is onderstaand opgenomen.



Artikel 6 Oorzaken en verbetermaatregelen

De Verbonden persoon of derde (PUO) is verplicht bij constatering van een Datalek, in goed overleg met het fonds, voor eigen rekening en risico alle noodzakelijke maatregelen te nemen om het Datalek te dichten en de schade die hieruit voortvloeit of kan vloeien te beperken. De Verbonden persoon of derde (PUO) zal het fonds volledig op de hoogte houden en blijven houden van de ontwikkelingen met betrekking tot een Datalek en de genomen of te nemen maatregelen om de gevolgen hiervan te beperken en herhaling te voorkomen.

De Uitvoerende Bestuursleden zullen aan de hand van de ontvangen informatie beoordelen of het noodzakelijk is aan de Verbonden persoon of derde (PUO) te vragen bepaalde aanvullende beveiligingsmaatregelen te treffen. De Uitvoerende Bestuursleden bewaken voortgang ten aanzien van eventuele aanvullende beveiligingsmaatregelen.

Artikel 7 Registratie

Uitvoerende Bestuursleden, direct of via bestuursondersteuning en de FG van het fonds houden een register bij van alle (beveiligings)incidenten en Datalekken binnen het fonds. De derde (PUO) houdt tevens een registratie bij van ieder Datalek bij de derde (PUO) en verstrekt deze op verzoek aan het fonds.

[3] Deze clausule geldt alleen voor verwerkers: zij zijn verplicht het fonds zonder onredelijke vertraging op te hoogte te stellen van ieder (vermoedelijk) Datalek. Dat is opgenomen in verwerkersovereenkomsten.

Indien de Uitvoerende Bestuursleden van mening zijn dat er sprake is van een Datalek dan brengen zij de voorzitter van de Audit- Risk- en Compliance commissie daarvan achteraf per e-mail op de hoogte.

Artikel 8 Rapportage

Als de aard van het Datalek dit naar de mening van de Uitvoerende Bestuursleden en/of Functionaris Gegevensbescherming nodig maakt, zullen zij over deze incidenten rapporteren aan het Bestuur.

Artikel 9 Overig

Deze regeling is vastgesteld door het Bestuur op 7 juni 2024 en treedt in werking op 7 juni 2024.

Deze regeling wordt ten minste een keer in de drie jaar geëvalueerd en geactualiseerd via de Audit-, Risk- en Compliancecommissie, tenzij tussentijds sprake is van belangrijke wijzigingen. Dan wordt deze procedure onverwijld aangepast.

Zeist, 7 juni 2024.

Ties Tiessen
Onafhankelijk voorzitter

Edwin Schokker
Uitvoerend bestuurslid