

Melding van Inbreuken

Deze procedure voorziet in een gestructureerde wijze voor het melden van Inbreuken in het kader van de wetgeving inzake bescherming persoonsgegevens.

Introductie

Stichting Pensioenfonds Aon Groep Nederland (het Fonds) voert pensioenregelingen voor de (gewezen) werknemers van Aon Groep Nederland uit. De uitvoering van pensioenregelingen leidt tot Verwerking van Persoonsgegevens. Het Fonds is Verwerkingsverantwoordelijke.

Het Fonds) heeft voor de uitvoering van de pensioenregelingen de volgende activiteiten uitbesteed aan RiskCo Administrations B.V (RiskCo):

- Het administreren van door het fonds uitgevoerde pensioenregelingen. Deze uitbesteding omvat de volgende componenten:
 - deelnemers- en aansprakenadministratie;
 - uitkeringsadministratie;
 - financiële administratie.

Met RiskCo is naast de dienstverleningsovereenkomst een verwerkersovereenkomst gesloten die voldoet aan de Wet.

Definities

AP: Autoriteit Persoonsgegevens

Betrokkene: een geïdentificeerde of identificeerbare natuurlijk persoon op wie de Persoonsgegevens betrekking hebben.

Persoonsgegevens: de informatie als omschreven in artikel 4 sub 1 van de Wet.

Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, het verlies, de wijziging of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens (artikel 4 lid 12 van de Wet).

Medewerker: de natuurlijke persoon die werkzaam is bij het Fonds, al dan niet op basis van een arbeidsovereenkomst.

Wet: Verordening (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van Persoonsgegevens en de op basis van die Verordening ingevoerde lagere regelgeving.

Verwerker: de verwerker als bedoeld in artikel 4 lid 8 van de Wet.

Verwerking: de verwerking als bedoeld in artikel 4 lid 2 van de Wet.

Verwerkingsverantwoordelijke: de verwerkingsverantwoordelijke als bedoeld in artikel 4 lid 7 van de Wet.

De meldingsplicht aan de AP

Indien een Inbreuk heeft plaatsgevonden moet de Verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen melden aan de AP, tenzij het niet waarschijnlijk is dat de Inbreuk in verband met Persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Dit betekent dat de Verwerkingsverantwoordelijk zelf beoordeelt of een melding van een Inbreuk moet leiden tot een melding aan de AP.

De mededeling van een Inbreuk aan de Betrokkene(n).

Wanneer de Inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen moet de Verwerkingsverantwoordelijke de Betrokkene de Inbreuk onverwijld mededelen, tenzij zich één van de uitzonderingen als omschreven in artikel 34 lid 3 van de Wet van toepassing is. Deze uitzonderingen zijn:

1. de Verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de Persoonsgegevens waarop Inbreuk in verband met Persoonsgegevens betrekking heeft, met name die welke de Persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
2. de Verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van Betrokkene(n) zich waarschijnlijk niet meer zal voordoen;
3. de mededeling onevenredige inspanningen vergen. In plaats daarvan komt dan een openbare mededeling of een soortgelijke maatregel waarbij Betrokkene(n) even doeltreffend word(t)(en) geïnformeerd.

Documentatie van Inbreuken

De Verwerkingsverantwoordelijke documenteert alle Inbreuken, met inbegrip van de feiten omtrent de Inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie moet de AP in staat stellen de naleving van de meldplicht te controleren.

Doel

Deze procedure beschrijft hoe te handelen indien er sprake is van een Inbreuk. De meldplicht is eveneens van toepassing, als de Inbreuk bij een derde is ontstaan, bijvoorbeeld een (sub) Verwerker die ten behoeve van een Verwerkingsverantwoordelijke Persoonsgegevens verwerkt.

Inbreuken ontstaan bij contractuele Verwerkers

1. In de verwerkersovereenkomst met Verwerkers wordt vastgelegd dat Verwerker de Verwerkingsverantwoordelijke onmiddellijk, doch uiterlijk binnen 48 uur, na constatering in kennis stelt van een Inbreuk. Deze kennisgeving zal Verwerker per e-mail richten aan de Contactpersoon Privacy van Verwerkingsverantwoordelijke.
2. De in lid 1 genoemde kennisgeving bevat in ieder geval:
 - a. datum en tijd van de Inbreuk en de detectie daarvan;
 - b. aantal Betrokkenen;
 - c. de Persoonsgegevens waarop de Inbreuk betrekking heeft;
 - d. de oorzaak van de Inbreuk op de Persoonsgegevens (bijvoorbeeld verlies, diefstal, verminking, hacken);
 - e. de mogelijke gevolgen en risico's voor Betrokkene(n);
 - f. de maatregelen die zijn genomen of worden genomen om de Inbreuk te voorkomen.
3. De Contactpersoon Privacy beslist binnen 48 uur na de kennisgeving door verwerker of melding van de Inbreuk leidt tot een melding aan de AP.
4. Een melding aan de AP geschiedt met het in Bijlage 1 beschreven formulier.

5. Tegelijkertijd met de melding aan de AP beoordeelt de Contactpersoon Privacy of aan Betrokkene(n) mededeling wordt gedaan van de Inbreuk. Een melding aan Betrokkene(n) bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de Inbreuk in verband met Persoonsgegevens en bevat ten minste de volgende gegevens en maatregelen:
 - a. de naam en de contactgegevens van de Contactpersoon Privacy waar meer informatie kan worden verkregen;
 - b. de waarschijnlijke gevolgen van de inbreuk in verband met de persoonsgegevens;
 - c. de maatregelen die de Verwerkingsverantwoordelijke heeft voorgesteld of genomen om de Inbreuk in verband met persoonsgegevens aan te pakken waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele gevolgen daarvan

Melding Inbreuk door derden, anderen dan contractuele (sub)Verwerkers van Verwerkingsverantwoordelijke aan de laatste.

1. Indien de Contactpersoon Privacy een mededeling van een derde ontvangt verstrekt hij onverwijld aan de melder het formulier van Bijlage 2.
2. Na ontvangst van het in lid 1 genoemde formulier handelt de Contactpersoon Privacy conform het hiervoor onder de artikelen 1 tot en met 5 gestelde.

Deze procedure en Bijlage 2 worden op de site van de Verwerkingsverantwoordelijke geplaatst.