

Bepalingen en maatregelen AVG

In onderstaand overzicht treft u de belangrijkste bepalingen uit de AVG aan alsmede de acties die Millenaar Adviesgroep B.V. onderneemt om aan deze eisen te voldoen.

Een organisatie die op grootschalige wijze persoonsgegevens verwerkt dient een verwerkingsregister op te stellen.

Millenaar Adviesgroep B.V. stelt een verwerkingsregister op. In dit verwerkingsregister worden de volgende onderdelen opgenomen:

- Het doel c.q. de doelen van verwerking van persoonsgegevens;
- De categorieën van persoonsgegevens die worden bijgehouden;
- De categorieën van betrokkenen waarvan persoonsgegevens worden bijgehouden;
- Of er sprake is van de registratie van bijzondere persoonsgegevens of strafrechtelijke gegevens;
- De (categorieën van) organisaties aan wie wij deze persoonsgegevens verstrekken;
- De bewaartermijn van de persoonsgegevens.

Voor dit verwerkingsregister zullen wij een analyse uitvoeren naar de persoonsgegevens die wij hebben geadmistreerd, van welke personen, wie toegang heeft tot deze persoonsgegevens of wie ze ontvangt.

Een ontvanger is iemand die van een persoon persoonsgegevens ontvangt voor de uitvoering van een overeenkomst. Als er organisaties zijn die persoonsgegevens voor ons verwerken, denk daarbij aan leveranciers van advies- of beheerapplicaties, dan zullen wij zorgen dat in onze overeenkomsten met deze organisaties uw belangen voldoende zijn geborgd.

Om persoonsgegevens te mogen verwerken moet er sprake zijn van rechtmatigheid.

Deze rechtmatigheid kan onder andere bestaan uit:

- Toestemming van de betrokkene;
- Het uitvoeren van een overeenkomst;
- Het voldoen aan een wettelijke plicht.

Millenaar Adviesgroep B.V. werkt met u samen uit hoofde van een opdracht tot dienstverlening inzake advies en/of bemiddeling. Deze opdracht komt, ook al zijn wij deze niet nadrukkelijk schriftelijk overeengekomen, automatisch tot stand op basis van het Burgerlijk Wetboek. Dit betekent dat de rechtmatigheid van onze gegevensverzameling is gebaseerd op het uitvoeren van een overeenkomst.

In sommige gevallen ontleent Millenaar Adviesgroep B.V. de rechtmatigheid van onze gegevensverzameling aan een wettelijke plicht, dit betekent echter niet dat wij zomaar allerlei gegevens van u mogen opvragen. Wij mogen slechts die gegevens opvragen die strikt noodzakelijk zijn voor het doel, waarvoor wij deze gegevens hebben opgevraagd.

De gegevens die u aan ons verstrekt, verstrekt u dan ook uit hoofde van deze overeenkomst tot opdracht. Wij zijn geen verwerker in de zin van de AVG, het is dan ook niet nodig om verwerkersovereenkomst met u aan te gaan, voordat u vertrouwelijke informatie aan ons verstrekt.

Wij maken een analyse van de door ons ingewonnen informatie en de noodzaak daarvan. Beschikken wij over meer informatie dan noodzakelijk, dan zullen wij u om toestemming vragen deze gegevens te mogen bewaren of wij verwijderen deze informatie uit onze administratie. Aangezien het niet mogelijk is om voor de invoering van de AVG onze volledige administratie te doorzoeken, zullen wij de analyse op dossierniveau uitvoeren als wij uw dossier behandelen. Uitzondering hierop zijn de niet noodzakelijk opgeslagen bijzondere persoonsgegevens, hiervoor vragen wij toestemming of deze worden verwijderd.

Met medewerkers die persoonsgegevens verwerken moeten geheimhouding worden overeengekomen.

Omdat vertrouwelijkheid zo belangrijk is hebben wij een analyse gemaakt van welke medewerkers toegang hebben tot welke persoonsgegevens. Wij beoordelen hierbij of deze toegang noodzakelijk is voor de uitvoering van de werkzaamheden van deze medewerkers. Indien deze toegang niet nodig blijkt, dan zullen wij de rechten van deze medewerkers beperken.

Met alle medewerkers binnen onze onderneming is geheimhouding overeengekomen. Deze geheimhouding maakt deel uit van de arbeidsovereenkomst die wij met de medewerkers zijn aangegaan. Daarnaast hebben de medewerkers van ons kantoor een eed of belofte afgelegd waarin zij eveneens verklaren alle informatie die zij in de uitoefening van hun werkzaamheden hebben ontvangen geheim te houden en dat zij te allen tijde in het belang van de klant zullen handelen.

Een organisatie die persoonsgegevens verwerkt moet betrokkenen informeren over deze verwerking, betrokkenen wijzen op hun rechten en de uitoefening van deze rechten faciliteren.

Wij passen de informatie over onze dienstverlening aan, zodat deze voldoet aan de informatieverplichting uit de AVG. Deze informatie verstrekken wij aan klanten voordat wij zaken met elkaar gaan doen. Ook vermelden wij deze informatie op onze website.

Wij hebben interne procedures opgesteld om de betrokkenen te faciliteren bij de uitoefening van hun rechten. Hierbij is het voor ons wel belangrijk om vast te stellen of de persoon die rechten wil uitoefenen ook daadwerkelijk de persoon is waarvan wij persoonsgegevens van verwerken. Hiervoor kunnen wij om identificatie vragen of u vragen om op ons kantoor langs te komen om u te identificeren. Ook in een dergelijk geval is vertrouwelijkheid belangrijk.

Als u ons verzoekt om persoonsgegevens van u te verwijderen, dan zullen wij daar gehoor aan geven, tenzij wij deze gegevens nog nodig hebben. Bijvoorbeeld omdat het financiële product de einddatum nog niet heeft bereikt of hier nog uitkeringen op worden verwacht. Wilt u dan toch dat wij deze gegevens verwijderen, dan zullen wij u om een vrijwaring vragen voordat wij tot verwijdering van uw persoonsgegevens overgaan.

Wij werken ook mee aan overdracht van data in geautomatiseerde bestanden. Hiervoor moet het wel mogelijk zijn om deze gegevens gestructureerd en geautomatiseerd over te dragen.

Een organisatie die persoonsgegevens verwerkt moet, rekening houdend met de aard, omvang, de context en het doel van verwerking, maar ook met de waarschijnlijkheid en de ernst van de uiteenlopende risico's, passende technische en organisatorische maatregelen treffen om zorgvuldige verwerking van persoonsgegevens te waarborgen.

Wij stellen een analyse op van de middelen waarop wij persoonsgegevens verwerken. Per verwerkingsmiddel maken wij een analyse van de volgende onderwerpen:

- Welke persoonsgegevens worden hierin/-op geadministreerd;
- Wie heeft toegang tot deze persoonsgegevens;
- Welke beveiligingsmaatregelen zijn getroffen om deze persoonsgegevens te beschermen.

Op basis van deze analyse beoordelen wij of de getroffen maatregelen voldoende zijn of dat wij aanvullende maatregelen moeten treffen..

Daarnaast besteden wij doorlopend aandacht voor de vertrouwelijkheid van uw persoonsgegevens bij onze medewerkers. Onze kernwaarden zijn belangrijk voor ons en maken deel uit van het DNA van onze onderneming.

Datalekken die een risico opleveren voor de rechten en vrijheden van natuurlijke personen moeten zonder onredelijke vertraging (uiterlijk binnen 72 uur na ontdekking hiervan) worden gemeld aan de Autoriteit Persoonsgegevens.

Wij monitoren onze systemen op onrechtmatige toegang tot persoonsgegevens. Indien wij een datalek signaleren, dan zullen wij deze zo spoedig mogelijk repareren. Ook zullen wij nagaan of het risico aanwezig is dat de persoonsgegevens onrechtmatig worden verspreid.

Wij beschikken over een interne procedure voor het melden van datalekken, indien een medewerker per ongeluk persoonsgegevens onrechtmatig verspreid. Een datalek wordt door ons altijd gemeld aan de Autoriteit Persoonsgegevens en eventueel ook aan de Autoriteit Financiële Markten. Een datalek kan ook een incident in de zin van de Wet op het financieel toezicht zijn.

Bij het gebruik van nieuwe technologieën bij de verwerking van persoonsgegevens moet de organisatie bij de ontwikkeling rekening houden met het borgen van de privacyrechten van de betrokkenen (privacy by design).

Wij hebben procedures en instructies opgesteld die waarborgen dat bij de inrichting of het gebruik van nieuwe technologieën wordt getoetst of de rechten van betrokkenen voldoende geborgd zijn.

Indien persoonsgegevens buiten de Europese Unie worden opgeslagen, moet de verwerkingsverantwoordelijke waarborgen verkrijgen dat de belangen van de betrokkenen voldoende zijn geborgd (op hetzelfde niveau als binnen de EU). Dit geldt ook voor de samenwerking met internationale organisaties die buiten de EU werkzaam zijn.

Uit een door ons opgestelde analyse is gebleken dat wij niet met partijen samenwerken die persoonsgegevens buiten de EU opslaan. In onze beoordeling van nieuwe samenwerkingsverbanden met ontvangers of verwerkers, wordt standaard beoordeeld of er sprake kan zijn van het opslaan van persoonsgegevens buiten de EU.

Het administreren van een persoonlijk identificatienummer (BSN) is uitsluitend toegestaan indien hiervoor een wettelijke verplichting geldt.

In veel gevallen zal er voor ons een wettelijke verplichting gelden voor het gebruik van BSN nummers van onze klanten en of andere betrokkenen. Voor het opslaan van deze gegevens in onze administratie zal er in sommige gevallen ook een wettelijke grondslag zijn.

Wij maken een analyse van onze geautomatiseerde systemen op de opslag van BSN nummers en zullen deze -indien ze onrechtmatig voorkomen in onze systemen- collectief verwijderen. Daar waar een collectieve verwijdering niet mogelijk blijkt zullen wij dit bij de behandeling van een betreffend dossier uitvoeren.

Persoonsgegevens mogen niet langer worden bewaard dan strikt noodzakelijk voor het doel, waarvoor deze gegevens zijn ingewonnen.

Wij hebben per categorie persoonsgegevens vastgesteld welke bewaartermijn noodzakelijk is. Deze bewaartermijnen kunnen voorkomen uit wettelijke verplichtingen (Wet op het financieel toezicht, Burgerlijk Wetboek of Belastingwet) of overeenkomsten met verzekeraars waarvoor wij als gevolmachtigd agent optreden.

Op klant- en polisniveau leggen wij de vernietigingsdatum van de persoonsgegevens vast, nadat het contract of de relatie is beëindigd.

Dit memo is gebaseerd op de kennis van 7 februari 2018. Hoewel wij dit memo met de nodige zorgvuldigheid hebben samengesteld, kan dit memo niet worden gezien als een juridisch advies.