**Privacy- en beveiligingsbeleid**

**Bescherming persoonsgegevens**

***Inleiding***
Tussen alle informatie die cliënten ter beschikking stellen aan ons kantoor om de aan ons gegunde opdrachten uit te kunnen voeren, zitten ook persoonsgegevens. Die informatie betreft ofwel direct een natuurlijk persoon, of is naar deze persoon te herleiden. Naast voor de hand liggende gegevens, zoals naam, adres, geboortedatum en -plaats en BSN-nummer is er nog veel meer informatie naar een persoon te herleiden, zoals telefoonnummers, ziektekostenverzekeringsnummers, kentekengegevens en zelfs IP-adressen. Dat een gegeven soms niet altijd direct exact naar één persoon te herleiden is, maar naar een kleine groep van mensen, maakt daarbij niet uit. Op basis van twee persoonsgegevens (bijvoorbeeld adres en leeftijd) is de informatie immers mogelijk alsnog naar één persoon te herleiden. Als kantoor hebben wij de verantwoordelijkheid en (dus) de plicht om zorgvuldig met deze gegevens om te gaan, in overeenstemming met de Algemene Verordening Gegevensbescherming, de AVG. De belangrijkste uitgangspunten hierbij zijn:

1. De persoonsgegevens worden uitsluitend (en niet uitgebreider dan nodig) opgevraagd en gebruikt voor de uitvoering van de betreffende opdracht die wij van de cliënt(en) hebben gekregen.
2. Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk.
3. De betrokken persoon, of degene die primair voor hem of haar verantwoordelijk is (bijvoorbeeld een werkgever die zijn personeelsgegevens aan ons doorgeeft – volgens de AVG gedefinieerd als de ‘verwerkingsverantwoordelijke’), krijgt op verzoek inzage in de vastgelegde persoonsgegevens en kan eisen dat deze worden verbeterd of verwijderd.
4. We dragen zorg voor de geheimhouding van de verkregen persoonsgegevens. Dat geldt voor alle medewerkers van ons kantoor, maar ook voor derden die toegang (kunnen) hebben tot deze gegevens, zoals leveranciers van online softwareapplicaties, maar ook aan onze systeembeheerder, ingeschakelde deskundigen, stagiaires, enzovoorts. Met de betreffende personen en/of organisaties regelen we dit in contracten (zie o.a. de modellen ‘verwerkersovereenkomst’ en ‘geheimhoudingsverklaring leveranciers’), arbeidsovereenkomsten en/of de door medewerkers en andere verbonden personen te tekenen verklaring fundamentele beginselen. Onze beveiligingsmaatregelen voor het pand en de beveiliging rond onze ICT-structuur hebben mede tot doel de vertrouwelijkheid van de persoonsgegevens te beschermen.
5. In het verlengde van het voorgaande: indien het nodig is dat wij op onze beurt derden inschakelen, doen wij uitsluitend een beroep op verwerkers die afdoende garanties bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen. Op die manier voldoet de verwerking aan de vereisten van deze verordening en wordt de bescherming van de rechten van de betrokkene gewaarborgd.

Uiteraard geldt de geheimhouding niet indien wij op grond van de wet- of regelgeving verplicht zijn om anders te handelen. Bijvoorbeeld indien we een bindend verzoek of opdracht hiertoe ontvangen hebben van een daartoe bevoegde instantie. Als we volgens de regelgeving de betreffende cliënt hiervan op de hoogte mogen stellen, zullen we dat (zo spoedig mogelijk) doen.

***Verwerkingsregister***
Allerlei aspecten rond de diverse persoonsgegevens die onze organisatie verwerkt, worden door ons vastgelegd in een ‘verwerkingsregister van persoonsgegevens’. Hierin is in kaart gebracht welke categorieën persoonsgegevens van verschillende categorieën van betrokkenen die wij verwerken om diverse redenen/ voor diverse doelen. Doordat wij door middel van dit verwerkingsregister een goed beeld hebben van de vastleggingen/verwerkingen van alle persoonsgegevens, hebben wij ook helder welke risico's er rond de bescherming van die persoonsgegevens bestaan. Daardoor kan duidelijk worden bepaald en gemonitord of de technische en organisatorische maatregelen (nog) afdoende zijn c.q. of er nog aanvullend maatregelen moeten worden getroffen. Secundair doel van het verwerkingsregister is dat aan belanghebbenden (betrokkenen, verwerkingsverantwoordelijken, toezichthouders, etc.) verantwoording kan worden afgelegd over het adequaat omgaan met persoonsgegevens.

***Verwerkersovereenkomst en privacyverklaring***
In situaties waarin wij zijn aan te merken als verwerker, zullen wij onze verantwoordelijkheden naar de verwerkingsverantwoordelijke bevestigen c.q. met de verwerkingsverantwoordelijke overeenkomen via een verwerkersovereenkomst.
Voor situaties waarin wij zijn aan te merken als verwerkingsverantwoordelijke hebben we de kern van ons beleid en de voorschriften vanuit de AVG waaraan wij ons houden, vastgelegd in een privacyverklaring. Deze verklaring is beschikbaar via onze website.

**Melding incident persoonsgegevens (datalek)**

Van een datalek is sprake als er een inbreuk is op de beveiliging van persoonsgegevens. Het gaat dan om toegang tot – of vernietiging, wijziging of het vrijkomen van – persoonsgegevens zonder dat dit de bedoeling was. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook de onrechtmatige verwerking van gegevens. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming hadden moeten bieden. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker. Maar ook een e-mail aan een verkeerde persoon, of een e-mail aan een groep personen, waarbij ten onrechte de geadresseerden zichtbaar (dus niet in de Bcc-balk) zijn opgenomen.

De ernst van een datalek hangt af van:
- de omvang van het lek (het aantal betrokken personen en/of aantal gegevens);
- de aard van de erbij betrokken gegevens (een leeftijd is normaal gesproken minder ernstig dan bijvoorbeeld een BSN-nummer, een foto of gezondheidsgegevens);
- de kans dat een lek ook daadwerkelijk tot schade zal leiden (een onbeveiligde USB-stick in de trein laten liggen is ernstiger dan een beveiligde USB-stick per ongeluk over de rand van een veerboot laten vallen).

Een datalek moet in bepaalde gevallen worden gemeld aan de Autoriteit Persoonsgegevens. Dit is aan de orde wanneer het lek leidt of kan leiden tot een aanzienlijke (kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor zijn of haar persoonlijke levenssfeer.

***Verantwoordelijke versus bewerker***
De ‘verwerkingsverantwoordelijke voor de betreffende persoonsgegevens’ moet een dergelijke melding doen. In sommige gevallen is *Kantoornaam* echter niet aan te merken als verantwoordelijke voor de gegevens, maar als ‘verwerker’. In voorkomende gevallen zullen we de omstandigheden rond het datalek zo snel mogelijk moeten doorgeven aan de verwerkingsverantwoordelijke voor de gegevens (vrijwel altijd een van onze cliënten), zodat deze – indien nodig – kan overgaan tot een melding.
*Kantoornaam* is wel *verwerkingsverantwoordelijke* voor de persoonsgegevens, namelijk in het geval dat we een bepaalde invloed hebben op wat we precies met de gegevens doen, bijvoorbeeld bij de samenstelling van jaarrekeningen of rond adviesdiensten. In andere gevallen is *Kantoornaam* alleen *verwerker* van de personeelsgegevens. Bij het verzorgen van een salarisadministratie bijvoorbeeld heeft *Kantoornaam* een precies gedefinieerde opdracht. De uitvoering ervan ligt op basis van de opdracht en wet- en regelgeving al op voorhand vrijwel geheel vast. Dit geldt meestal ook rond het verzorgen van administraties en aangiften omzetbelasting.
In geval van twijfel wie de verwerkingsverantwoordelijke voor de persoonsgegevens is, is het zaak om met de opdrachtgever te overleggen over het datalek, de eventuele melding en wie die gaat doen. Uiteindelijk gaat het er om dát de melding indien nodig wordt gedaan en is niet cruciaal wie die melding doet.

Het lek kan zich hebben voorgedaan bij *Kantoornaam*, maar ook bij een partij waaraan *Kantoornaam* toegang heeft gegeven tot de persoonsgegeven. Bijvoorbeeld omdat we een specialist hebben moeten inschakelen, of denk aan de opslag van gegevens in een datacenter. In de betreffende overeenkomst of door middel van een aanvullende subverwerkersovereenkomst is dan

overeengekomen dat de desbetreffende partij ons op de hoogte moet brengen van een eventueel datalek bij hen, zodat *Kantoornaam* – indien en voor zover nodig – verdere actie kan ondernemen.
Binnen onze organisatie moeten alle incidenten rond de beveiliging van persoonsgegevens onmiddellijk worden gemeld aan het bestuur. Omdat een eventuele melding onverwijld en (aan de Autoriteit Persoonsgegevens) zo mogelijk binnen 72 uur moet gebeuren – én omdat het incident schadelijk kan zijn voor personen – moet deze procedure voortvarend en zorgvuldig worden opgepakt.
Leidraad voor de afhandeling van het incident is de ***Checklist Incident persoonsgegevens.***
Daarnaast is er veel informatie te vinden op *www.autoriteitpersoonsgegevens.nl.*

**ICT en beveiliging**

De ICT-structuur van *Kantoornaam* wordt afdoende beveiligd met een firewall en de virusscansoftware wordt up-to-date gehouden.
Elke medewerker heeft een inlogprofiel. Bij het opstarten van een computer moeten de medewerkers een inlognaam en een wachtwoord invoeren. Ook vraagt bepaalde programmatuur om een inlognaam en wachtwoord.
Het bewustzijn bij medewerkers betreffende veilig werken wordt gestimuleerd, zoals het vragen van aandacht voor het niet openen van verdachte e-mails, het niet klikken op verdachte links, bij het langdurig verlaten werkplek uitloggen, enzovoorts.
Elke nacht wordt er een back-up gemaakt van de bestanden. Om veiligheidsredenen is de verdere bewaarprocedure rond de back-up vertrouwelijk.
*Kantoornaam* heeft een servicecontract afgesloten met <*naam systeembeheerder*>.

***Digitale communicatie***
*Deze paragraaf moet u zelf invullen! Mede onder invloed van de AVG zal de komende periode naar verwachting een verschuiving zichtbaar zijn van de relatief onveilige digitale communicatie via standaard e-mailoplossingen en gratis diensten als Wetransfer en Dropbox naar meer geavanceerde en beveiligde oplossing zoals e-mailen met encryptie, werken met specifieke websites en andere applicaties met beveiligde communicatiefuncties en (overigens) het werken met een portalfunctionaliteit. Hoewel er op dit gebied al veel mogelijk is, is veilige digitale communicatie nog een relatief onbekend gebied, zelfs bij sommige ICT-beheerders. Het is zeer wenselijk om op dit gebied advies in te winnen en rond digitale communicatie een veiligheidsbeleid te formuleren/vorm te geven en uiteraard te implementeren.*