Privacy- en beveiligingsbeleid

Inleiding

Ons bedrijf slaat persoonsgegevens van cliënten op. Dat kunnen de gegevens van een ondernemer/eigenaar zijn, of bij een vennootschap de bestuurder daarvan; in voorkomende gevallen kunnen het ook gegevens zijn van andere bij de cliënt werkzame medewerkers.

De betrokken personen mogen erop vertrouwen dat ons bedrijf zorgvuldig en vertrouwelijk met hun persoonsgegevens omgaat. De wet- en regelgeving, met de name de Algemene Verordening Gegevensbescherming (AVG), verplicht ons ook daartoe.

Dit beleid beschrijft hoe binnen ons bedrijf met privacy wordt omgegaan. Doel van dit beleid is om de organisatorische en technische maatregelen te nemen die in redelijkheid van ons verwacht mogen worden om te waarborgen dat zorgvuldig met de vastgelegde persoonsgegevens wordt omgegaan. De leiding van het bedrijf/ kantoor is verantwoordelijk voor het opstellen van het beleid en voor het toezien op de naleving ervan. Van alle medewerkers wordt verwacht dat zij in lijn met dit beleid integer, vertrouwelijk en overigens zorgvuldig met de persoonsgegevens omgaan.

Grondslag en doel

Persoonsgegevens worden voornamelijk verzameld en vastgelegd voor de facturering en/of het goed uitvoeren van de werkzaamheden die wij in opdracht van onze cliënten uitvoeren en verder voor de naleving van eventuele wettelijke verplichtingen. Zie daarnaast ook het kopje ‘Website’ hierna.

Het kan ook zijn dat wij specifiek toestemming hebben van betrokkene(n) om gegevens te bewaren, bijvoorbeeld een potentiële cliënt waar nog geen cliëntrelatie mee bestaat, maar wiens gegevens wij van deze potentiële cliënt met het oog op eventuele toekomstige opdrachten gedurende een bepaalde periode mogen bewaren;

Tot slot kunnen wij persoonsgegevens langer dan strikt noodzakelijk bewaren indien dat wenselijk is in verband met onze aansprakelijkheidspositie (een zogenaamd ‘gerechtvaardigd belang’).

Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan nodig is. Het gedurende een bepaalde periode bewaren van persoonsgegevens kan nodig zijn om ontvangen opdracht(en) /werkzaamheden goed te kunnen uitvoeren en/of om wettelijke verplichtingen te kunnen naleven (bijvoorbeeld in verband met de fiscale bewaarplicht).

Bij reguliere/vaste cliënten blijven de contactgegevens en gegevens relevant voor de facturering in ons relatiebeheersysteem staan, zolang het de verwachting is dat zij vaker diensten of producten bij ons zullen afnemen.

Tot slot bewaren wij persoonsgegevens van ex-cliënten voor zover en voor zo lang dat nodig is in verband met onze mogelijke aansprakelijkheidspositie.

Rechten van betrokkenen

Op verzoek zullen wij een betrokkene inzage geven in de persoonsgegevens die we van hem/haar vastleggen. In alle gevallen kunnen personen van ons vragen om onjuiste gegevens te corrigeren of de gegevens te verwijderen. Behoudens eventueel wettelijke verplichtingen zullen we dat dan ook op zo kort mogelijke termijn doen.

Beveiliging

Wij hebben, rekening houdend met de gesignaleerde mogelijke risico's, passende technische maatregelen getroffen om de verwerkingen van persoonsgegevens te beveiligen. De software en data zijn beveiligd via firewalls en beschermingssoftware en ook de (SSL-beschermde) website voldoet aan de geldende eisen.

Ook organisatorisch hebben wij passende maatregelen genomen. 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.

De toegang van medewerkers tot verschillende programmatuur c.q. gegevens is afgestemd op hun functies, taken en verantwoordelijkheden.

Elke nacht wordt er een back-up gemaakt van de bestanden. Om veiligheidsredenen is de verdere bewaarprocedure rond de back-up vertrouwelijk.

Ons bedrijf heeft een servicecontract afgesloten met QSIT ICT Dienstverlening..

Melding incident persoonsgegevens (datalek)

Ondanks de getroffen maatregelen kan het gebeuren dat er zich een incident voordoet rond de vastgelegde persoonsgegevens. Een datalek zal 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 zal daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor zijn of haar persoonlijke levenssfeer.

Uiteraard wordt een dergelijk incident grondig geëvalueerd en worden indien mogelijk nadere maatregelen genomen die herhaling van het incident zo goed mogelijk voorkomen.

Wij informeren onze medewerkers zodat zij enerzijds een inbreuk in verband met persoonsgegevens kunnen herkennen en anderzijds weten wat zij in de betreffende omstandigheden moeten doen.

Wij leggen alle inbreuken in verband met persoonsgegevens vast in een intern register.

Inschakelen derden

Wij geven persoonsgegevens uitsluitend door aan (betrouwbaar te achten) derden wanneer dat wettelijke verplicht is, of omdat dit in het kader van de uitvoering van de aan ons opgedragen werkzaamheden noodzakelijk is en verder bijvoorbeeld indien dit nodig is voor onze bedrijfsvoering. Met dergelijke derden worden schriftelijke afspraken gemaakt, waarin wordt overeengekomen dat ook deze derden zich houden aan de wet- en regelgeving.

In geen geval zullen wij de gegevens voor commerciële doeleinden aan derden verstrekken en ook niet aan ‘goede doelen.’

Wanneer wij persoonsgegevens verwerken in een online omgeving zullen wij ook met de betreffende softwareleverancier de nodige afspraken maken. Onder meer zullen wij vaststellen dat de betreffende partij de persoonsgegevens niet naar landen buiten de Europese Unie doorgeeft als die landen niet een privacybeschermingsniveau bieden dat minimaal gelijk is aan het niveau in Nederland.

Website

Op onze website houden wij gegevens bij over de bezoekersaantallen. Verder kunnen bezoekers van onze website als ze een vraag hebben via het betreffende formulier contactgegevens achterlaten. Wij zullen de opgegeven contactgegevens uitsluitend gebruiken om contact op te kunnen nemen met de betreffende bezoeker. Ontvangers van de nieuwsbrief kunnen overigens altijd, via de ‘unsubscribe-knop’ onderaan de nieuwsbrief of door “reply” van de nieuwsbrief aangeven de nieuwsbrief niet meer te willen ontvangen.

Onze website is voorzien van een SSL-certificaat en verder beveiligd met actuele software.

Onze privacyverklaring is ook in te zien en eventueel te downloaden via de website.

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 betrokkenen 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. Zo kan duidelijk worden bepaald en gemonitord of de technische en organisatorische maatregelen (nog) afdoende zijn c.q. of er nog aanvullende 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.