Beveiligingsbeleid Wilgenrijk

Versie 2.0, dd. 16.05.2018

Wij nemen de bescherming van uw gegevens serieus en nemen passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als u het idee hebt dat uw gegevens toch niet goed beveiligd zijn of er zijn aanwijzingen van misbruik, neem dan contact op via privacy@wilgenrijk.nl of via telefoonnummer 088 122 8866

Wilgenrijk heeft een informatiebeveiligingsbeleid opgesteld en de hierin beschreven maatregelen aantoonbaar toegepast. Dit beleid wordt regelmatig getoetst en geüpdatet. Wilgenrijk neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens adequaat te beveiligen en beveiligd te houden tegen verlies of enige vorm van onzorgvuldig, ondeskundig of onrechtmatige gebruik of verwerking, waarbij rekening wordt gehouden met de stand van de techniek.

Andere Verwerkers

Het beveiligingsbeleid van Wilgenrijk en de verwerkers die voor ons persoonsgegevens verwerken is gericht op een veilige omgeving voor de persoonsgegevens. Waar we diensten van derden gebruiken om gegevens te verwerken zijn verwerkersovereenkomsten afgesloten en worden er onderzoeken gedaan om een hoog niveau van beveiliging te garanderen voor uw gegevens. De verwerkers en de uitkomsten van deze onderzoeken worden deze expliciet beschreven en bekend gemaakt bij de Autoriteit Persoonsgegevens wanneer daar door de Autoriteit Persoonsgegevens naar wordt gevraagd.

Personeel

Wilgenrijk heeft aantoonbaar bevoegd en bekwaam personeel. Zowel bevoegd en bekwaam voor het verwerken van de gegevens als voor het beveiligen en beschermen van de gegevens. De personeelsleden zijn via een schriftelijke overeenkomst verplicht tot geheimhouding van alle informatie. Toegang tot persoonsgegevens is beperkt op basis van het need-to-know principe. Alleen wanneer toegang tot persoonsgegevens daadwerkelijk benodigd is voor het uitvoeren van de werkzaamheden wordt deze toegang ook gegeven. Zodra de bevoegdheden van personen veranderen, wordt de toegang tot gegevens hierop aangepast.

Beveiliging

Wij zorgen ervoor dat persoonsgegevens worden verwerkt in een fysiek beveiligde omgeving, met passende bescherming tegen dreigingen van buitenaf. Wanneer medewerkers of derden van ons toegang op afstand (bijvoorbeeld telewerken via internet) kunnen krijgen tot persoonsgegevens, is deze toegang afgeschermd met een versleutelde verbinding. Wanneer persoonsgegevens worden verwerkt op mobiele apparatuur, waaronder tablets, laptops en/of smartphones, dan zijn deze apparaten versleuteld (encrypted).

We hebben de volgende maatregelen genomen om uw persoonsgegevens te beveiligen:

- Servers en apparaten van onze medewerkers zijn uitgerust met actuele beveiligingssoftware, zoals een virusscanner en firewall.
- We versturen uw gegevens alleen via beveiligde internetverbindingen (TLS, voorheen SSL). Dit kunt u zien aan de adresbalk 'https' en het hangslotje.
- Alleen werknemers waarvoor het noodzakelijk is uw gegevens in te zien, hebben toegang tot uw persoonsgegevens.
- Toegang tot persoonsgegevens vanaf mobiele apparaten is ingeperkt en wordt actief gemonitord.
- Alle medewerkers van Wilgenrijk die toegang hebben tot persoonsgegevens zijn getraind in het zorgvuldig omgaan met uw gegevens.
- DKIM en SPF zijn internetstandaarden die wij gebruiken om te voorkomen dat u uit onze naam e-mails ontvangt die virussen bevatten, spam zijn of bedoeld zijn om persoonlijke (inlog)gegevens te bemachtigen.
- Onze organisatie is zo ingericht dat laptops, USB's en andere dragers van persoonsgegevens nooit onbemand achtergelaten worden of door een onbevoegde kan worden gebruikt.
- Door middel van een *clean desk policy* en het op de juiste wijze vernietigen van oude documenten zullen er geen persoonsgegevens rondslingeren.

Verwerkingsregister en privacy impact assessment

Wij houden een verwerkingsregister bij waarin alle verwerkingen die met persoonsgegevens te maken hebben, worden genoteerd. Hierin is in kaart gebracht welke categorieën persoonsgegevens we verwerken en voor welke doeleinden. Door het verwerkingsregister hebben we een goed beeld van alle verwerkingen, maar ook van welke risico's er rondom de bescherming van de persoonsgegevens bestaan. Zo kan duidelijk worden bepaald en gemonitord of de technische en organisatorische maatregelen voldoende zijn of er nog aanvullende maatregelen moeten worden getroffen. Een bijkomstigheid van het verwerkingsregister is dat aan belanghebbenden, zoals u of de Autoriteit Persoonsgegevens, gemakkelijker verantwoording kan worden afgelegd over het veilig omgaan met persoonsgegevens.

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, 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;
- 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 wordt in alle gevallen geregistreerd in het datalek register van Wilgenrijk dat inzichtelijk is voor de Autoriteit Persoonsgegevens. 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.

Vragen of Feedback
We controleren regelmatig of we aan dit beveiligingsbeleid voldoen. Als u vragen heeft over dit beveiligingsbeleid, kunt u contact met ons opnemen via emailadres privacy@wilgenrijk.nl of telefoonnummer 088-122 88 66.

Klacht indienen
Als u vindt dat wij u niet op de juiste manier helpen, dan heeft u het recht om een klacht in te dienen bij de toezichthouder. Deze heet de Autoriteit Persoonsgegevens. op www.autoriteitspersoongegevens.nl leest u hoe u een klacht moet indienen.