

PRIVACY-BELEID, BIJLAGE ICT INCLUSIEF PROTOCOL DATALEKKEN

20 oktober 2020



Stichting Welzijn Westerwolde (hierna Welzijn Westerwolde) verzamelt en verwerkt naast specifieke informatie voor cliënten, ook specifieke informatie middels haar ICT. Deze persoonsgegevens worden vastgelegd in daarvoor bestemde dossiers. De persoonsgegevens worden verwerkt conform de Algemene Verordening Gegevensbescherming, de AVG. De gegevens worden beveiligd en vertrouwelijk behandeld.

Wat doen wij met uw IP-adres, bezoekgegevens en cookies?

Iedereen die internet gebruikt heeft een IP-adres, ook als u internet met uw mobiele telefoon. Zonder IP-adres kunt u niet internetten. Welzijn Westerwolde houdt IP-adressen bij om u te behoeden voor internetfraude.

Website

Iedereen die internet gebruikt, heeft een IP-adres. Ook wanneer het internet gebruikt/bezocht wordt met een mobiele telefoon of tablet. Als u onze website bezoekt, registreren we uw IP-adres, bezoekgegevens en cookies. Hieronder leest u waarvoor wij deze gegevens gebruiken.

Wat doen we met bezoekgegevens?

Op onze website worden algemene bezoekgegevens bijgehouden, zoals de meest bezochte pagina's. Met deze informatie kunnen wij onze website optimaliseren, meer gerichte informatie op de website plaatsen en onze dienstverlening verder verbeteren. We registreren ook hoe bezoekers door onze website klikken. Deze gegevens worden alleen intern opgeslagen en verwerkt. Ze worden gebruikt voor statistische analyses van bezoekgedrag en voor fraudebestrijding.

Wat doen we met cookies?

We maken op onze website gebruik van cookies. Een cookie is een eenvoudig klein bestandje dat met pagina's van onze website wordt meegestuurd en door uw browser op uw harde schijf van uw computer wordt opgeslagen.

Via onze website wordt een cookie geplaatst van het Amerikaanse bedrijf Google, als deel van de 'Analytics' dienst. Wij gebruiken deze dienst om bij te houden en rapportages te krijgen over hoe onze bezoekers de website gebruiken. Google kan deze informatie aan derden verschaffen indien Google hiertoe wettelijk wordt verplicht of voor zover derden de informatie namens Google verwerken. Wij hebben hier geen invloed op. De informatie die Google verzamelt wordt zoveel mogelijk geanonimiseerd. Uw IP-adres wordt nadrukkelijk niet meegegeven. De informatie wordt overgebracht naar en door Google opgeslagen op servers in de Verenigde Staten.

Contactformulier

Op onze website staat een contactformulier. Als u hiervan gebruik maakt wordt u gevraagd uw naam en e-mailadres te verstrekken. Daarnaast kun u uw telefoonnummer geven. Deze persoonsgegevens hebben wij nodig om contact met u op te kunnen nemen. Deze gegevens worden bewaard zolang als nodig is voor de volledige beantwoording en afhandeling van de met het contactformulier verzonden vraag.

Beeldmateriaal op onze (social) media

Doel voor het plaatsen van foto's en filmpjes door Welzijn Westerwolde is altijd om het publiek te informeren. Op deze wijze wordt bijvoorbeeld een evenement of activiteit onder de aandacht gebracht. Als een organisatie foto's of video's op (social) media wil plaatsen geldt de privacywet. Dit betekent dat er toestemming nodig is van de mensen die op de foto's of filmpjes staan om ze te mogen publiceren. Welzijn Westerwolde zal, wanneer er foto's worden gemaakt in haar gebouwen

of tijdens haar activiteiten, de aanwezigen informeren en vragen om expliciete toestemming voor publicatie.

Protocol datalekken

Vanaf 1 januari 2016 geldt de meldplicht datalekken. Dit houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra er een ernstig datalek is. In een aantal gevallen moet het datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Het niet (tijdig) nakomen van de meldplicht kan leiden tot hoge boetes en imagoschade voor de organisatie. Daarom dient een (vermoeden van) een datalek altijd serieus genomen te worden en zorgvuldig te worden afgehandeld.

Waar is dit protocol voor bedoeld?

In dit protocol staat hoe omgegaan moet worden met (een vermoeden van) een datalek binnen Welzijn Westerwolde. Ook wordt aangegeven hoe beoordeeld kan worden of er sprake is van een datalek en of dit gemeld moet worden aan de Autoriteit Persoonsgegevens en aan de betrokkene(n).

Wat is een datalek?

Er is sprake van een datalek als zich een *beveiligingsincident* heeft voorgedaan, waarbij er persoonsgegevens verloren zijn gegaan, of waarbij onrechtmatige verwerking niet redelijkerwijs kan worden uitgesloten.

Voorbeelden van beveiligingsincidenten zijn:

- Kwijtraken of diefstal van laptop, telefoon of USB stick
- Kwijtraken van cliëntgegevens op papier
- Doorgeven van persoonsgegevens aan iemand die dit niet had moeten ontvangen (bv. sturen van gegevens naar de verkeerde cliënt)
- Inbraak in computersysteem door een hacker
- Toegang door onbevoegden tot persoonsgegevens op niet goed beveiligde computers en telefoons.
- Kwijtraken van wachtwoorden die toegang geven tot een gegevensbestand.

Niet ieder beveiligingsincident is dus een datalek. Als er alleen sprake is van een zwakke plek in de beveiliging, dan is er sprake van een beveiligingslek.

Meldplicht

Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Daarbij spelen de aard van de gegevens een belangrijke rol.

In het algemeen geldt:

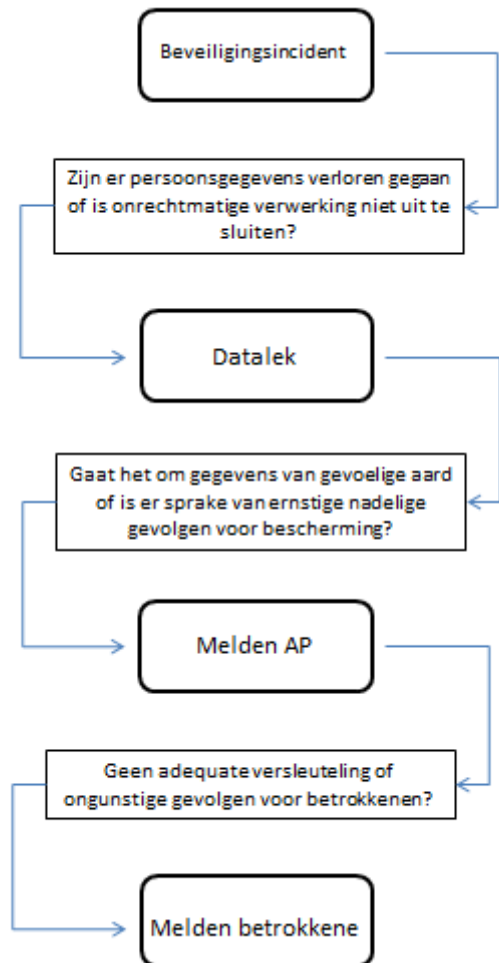
- Hoe gevoeliger de gegevens, hoe eerder er een meldplicht is
- Hoe groter het aantal getroffen mensen, hoe eerder er moet worden gemeld.

Meldplicht aan betrokkene

Het datalek moet ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Bij cliëntgegevens gaat het vaak om persoonsgegevens van gevoelige aard. Daarom kunnen we er in principe vanuit gaan dat wanneer bij een datalek van cliëntgegevens een melding gedaan moet worden aan de Autoriteit Persoonsgegevens, er ook melding gedaan moet worden aan de betrokkene.

Ook gegevens van medewerkers en organisatiegegevens kunnen gevolgen hebben voor de persoonlijk levenssfeer van betrokkenen. Een zorgvuldige afweging is belangrijk. Als de gegevens voldoende beschermd zijn (bijvoorbeeld versleuteld) zodat niet te achterhalen is om wiens gegevens het gaat dan hoeft dit niet aan de betrokkene te worden gemeld.

Onderstaand schema geeft de afwegingen weer die gemaakt moeten worden om te bepalen of een incident gemeld moet worden aan de Autoriteit Persoonsgegevens en aan de betrokkene



Procedure

1. De medewerker die het beveiligingsincident signaleert informeert zijn/haar leidinggevende hierover (bij afwezigheid leidinggevende doet medewerker rechtstreeks melding bij de functionaris gegevensbescherming).
2. Medewerker of leidinggevende meldt bij de functionaris gegevensbescherming.
3. De functionaris gegevensbescherming inventariseert of er acute maatregelen nodig zijn om het lek te dichten en/of de gevolgen te beperken.
4. De functionaris gegevensbescherming maakt de afweging of er daadwerkelijk sprake is van datalek aan de hand van de Beleidsregels voor toepassing van art. 34a Wbp.
5. Indien er geen sprake is van een datalek wordt de procedure beëindigd en maatregelen getroffen.
6. Indien er wel sprake is van een datalek stelt de functionaris gegevensbescherming een commissie samen, waarbij de samenstelling afhankelijk is van het soort datalek en de ernst van het datalek.
7. De functionaris gegevensbescherming meldt het datalek (voorlopig) digitaal binnen 72 uur via het meldloket van de Autoriteit Persoonsgegevens.
8. De commissie analyseert het datalek en legt in een plan van aanpak vast welke maatregelen er

genomen worden en wie op welke wijze geïnformeerd worden.

9. Het plan van aanpak wordt uitgevoerd.

10. Indien er sprake is van een voorlopige melding bij de Autoriteit Persoonsgegevens, vult de functionaris gegevensbescherming de melding aan zodra bekend is welke maatregelen genomen zijn en welke personen geïnformeerd zijn.

11. De functionaris gegevensbescherming monitort de voortgang van de uitvoering van het plan van aanpak: in elk geval na 4 of 8 weken check uitvoering.

12. De functionaris gegevensbescherming informeert de commissie en betrokkenen over de uitgevoerde maatregelen en afhandeling van het datalek.

13. De commissie evalueert het incident; welke verbetermaatregelen zijn nodig om een volgend beveiligingsincident te voorkomen?

14. Opname van melding in meldingsregister door functionaris gegevensbescherming (bewaartermijn 3 jaar).

Klachten en Vragen

Mocht je een klacht of vraag hebben over de verwerking van je persoonsgegevens ten aanzien van onze ICT dan vragen wij je hierover direct contact met ons op te nemen. Komen wij er samen niet uit dan vinden wij dit natuurlijk erg vervelend. Je hebt altijd het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, dit is de toezichthoudende autoriteit op het gebied van privacybescherming.

Contactgegevens:

Stichting Welzijn Westerwolde:

Dr. Bekenkampstraat 37

9561 RD Ter Apel

avg@welzijnwesterwolde.nl

Telefoon 0599-582460

Autoriteit Persoonsgegevens:

Bereikbaar via website www.autoriteitspersoonsgegevens.nl

Of telefonisch via 088-1805250