Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Prins Clauslaan 60, 2595 AJ Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

KNGF

Postbus 248
3800 AE AMERSFOORT

Datum
15 maart 2016

Ons kenmerk
Z2016-204

Contactpersoon

Onderwerp
Beveiliging contactformulier op websites fysiotherapeuten

Geachte ,

Naar aanleiding van vragen van een aantal van uw leden constateert de Autoriteit Persoonsgegevens (AP) dat er bij fysiotherapeuten onduidelijkheid bestaat over de wijze waarop websites, die een contactformulier bevatten, moeten worden beveiligd. De vraag is met name in welke gevallen daarbij gebruik moet worden gemaakt van een beveiligde verbinding (https).

Beveiliging is een belangrijk aandachtspunt van de AP. Wij hebben er daarom voor gekozen de KNGF als overkoepelende vereniging van fysiotherapeuten in te lichten over hoe de AP de beveiligingsnormen uit de Wet bescherming persoonsgegevens (Wbp) in dit geval toepast.

Dit is als volgt:

Bij het bouwen van een website voor een fysiotherapiepraktijk dient rekening te worden gehouden met de NEN 7512:2015 norm en de NCSC ICT-Beveiligingsrichtlijnen voor webapplicaties (2015).

Indien via een contactformulier op de website bijzondere persoonsgegevens – waaronder gezondheidsgegevens en bsn – worden verwerkt, dient de gehele webapplicatie via https te worden aangeboden.

Indien uitsluitend andersoortige gegevens worden verwerkt dan moet de organisatie zelf op basis van een risicoanalyse en classificatieschema vaststellen of de webapplicatie via https wordt aangeboden.

De AP zou het op prijs stellen, indien u uw leden hiervan – en ook van de toelichting hieronder - op de hoogte wilt stellen.

Toelichting

Artikel 13 Wbp vereist dat de verantwoordelijke 'passende' beveiligingsmaatregelen treft teneinde persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Bij de bepaling van hetgeen in dit geval als 'passende technische en organisatorische maatregelen' in de zin van artikel 13 Wbp moet worden beschouwd zijn de NEN 7512 norm en de ICT-Beveiligingsrichtlijnen voor webapplicaties als beveiligingsstandaarden gebruikt.

Norm NEN 7512:2015

De NEN 7512 norm heeft betrekking op de elektronische communicatie in de zorg, tussen zorgverleners en zorginstellingen onderling en met patiënten en cliënten, met zorgverzekeraars en andere partijen die bij de zorg betrokken zijn. In deze norm worden minimumeisen gesteld met betrekking tot de bron van de gegevens, het transportkanaal en de ontvanger van de gegevens.[1]

NEN 7512:2015 geeft aan dat uitsluitend indien communicatie niet vertrouwelijk is[2] [3], er geen versleuteling nodig is. NEN 7512:2015 specificeert niet wanneer sprake is van vertrouwelijke communicatie.

Norm ICT-Beveiligingsrichtlijnen voor webapplicaties

De ICT-Beveiligingsrichtlijnen voor webapplicaties [4] (verder:IBW) geeft aan dat "gevoelige (vertrouwelijke) gegevens [moeten] worden beschermd door gebruik van cryptografische technieken in de […] communicatie. Welke gegevens gevoelig of vertrouwelijk zijn, moet door de organisatie op basis van een risicoanalyse […] en classificatieschema […] worden vastgesteld."[5]

In de IBW wordt ook een nadere uitleg gegeven hoe de communicatie moet worden versleuteld. Als de webapplicatie een contactformulier bevat, dient de gehele webapplicatie via https te worden aangeboden. [6]

(Nadere) normering AP

AP gaat er bij de toepassing van artikel 13 Wbp vanuit dat een verantwoordelijke in de zorg deze beide algemeen geaccepteerde beveiligingsstandaarden toepast.[7]

[1] NEN 7512:2015, p. 5.
[2] Of via een gegarandeerd exclusief communicatiekanaal loopt – maar hiervan is in casu geen sprake.
[3] NEN 7512:2015, p. 24.
[4] NCSC, 2015.
[5] IBW Verdieping, p. 28. Zie ook IBW Richtlijnen, p. 18 (Beveiligingsrichtlijn U/WA.05, maatregel 05).
[6] IBW Verdieping, p. 29, maatregel 05 (Versleutel communicatie)
[7] CBP Richtsnoeren beveiliging persoonsgegevens, 2013, p. 4, 13, 14, 16.

AP gaat er daarnaast van uit dat in ieder geval bijzondere persoonsgegevens – waaronder gezondheidsgegevens en bsn – vertrouwelijk zijn. Voor andersoortige gegevens geldt dat de organisatie zelf de vertrouwelijkheid van de verwerkte gegevens dient vast te stellen zoals aangegeven in de IBW.

Conclusie

Bij het bouwen van een website voor een fysiotherapiepraktijk dient rekening te worden gehouden met de NEN 7512:2015 norm en de NCSC ICT-Beveiligingsrichtlijnen voor webapplicaties (2015).

Indien via een contactformulier op de website bijzondere persoonsgegevens – waaronder gezondheidsgegevens en bsn – worden verwerkt, dient de gehele webapplicatie via https te worden aangeboden.

Indien uitsluitend andersoortige gegevens worden verwerkt dan moet de organisatie zelf op basis van een risicoanalyse en classificatieschema vaststellen of de webapplicatie via https wordt aangeboden.

Hoogachtend,

Autoriteit Persoonsgegevens,
Voor deze,

Mr. W.B.M. Tomesen
Vicevoorzitter