AUTORITEIT
PERSOONSGEGEVENS

# Veilig thuiswerken tijdens de coronacrisis

Nieuwsbericht/18 maart 2020

Categorie: Veilig thuiswerken tijdens corona Beveiliging van persoonsgegevens Hoe werk je veilig thuis Zorgverleners en de AVG tijdens de coronacrisis? De Autoriteit Persoonsgegevens (AP) geeft 4 tips om op een veilige manier gewoon aan het werk te blijven.

Nederland blijft doorwerken tijdens de coronacrisis. Wie dat kan, doet dat thuis. Maar let op: voor cybercriminelen is deze crisis een kans om gevoelige data buit te maken. En een foutje is snel gemaakt, waardoor gevoelige gegevens op straat kunnen komen te liggen.

Volg deze tips op en voorkom dat er gegevens over klanten, cliënten, patiënten, burgers of collega's in verkeerde handen vallen.

## 1. Werk in een beveiligde omgeving

Werk uitsluitend in een beveiligde thuiswerkomgeving, als dat mogelijk is. Dus log thuis in op de server van uw organisatie. Zodat u hetzelfde scherm te zien krijgt als op kantoor. Gebruik hiervoor als dat kan apparatuur (laptop of tablet bijvoorbeeld) die uw organisatie u heeft verschaft.

Heeft u geen beveiligde thuiswerkomgeving? Overleg dan met collega's, opdrachtgevers en opdrachtnemers over hoe u veilig werkt.

Wees voorzichtig met het gebruik van cloud-, opslag- of e-maildiensten, zeker wanneer deze gratis zijn. Want het zou kunnen dat zo'n dienst juist gratis is omdat de aanbieder uw gegevens gebruikt voor andere doeleinden. Zoals marketing of verkoop van gegevens aan derden. Ook zou het kunnen dat deze diensten niet goed beveiligd zijn tegen internetcriminelen.

Wees net als altijd extra voorzichtig met bijzondere persoonsgegevens, zoals medische gegevens of gegevens waaruit iemands etnische afkomst, seksuele voorkeur of religie af te leiden is.

## 2. Bescherm gevoelige documenten

Staan gevoelige documenten niet op de server, maar alleen op een usb-stick of op papier? Zorg er dan voor dat ze op de server van uw organisatie komen te staan.

Papieren documenten kunt u op kantoor inscannen om ze daarna op de server te zetten. Of neem, als dit niet kan, de gegevens op een usb-stick mee. Zorg er dan wel voor dat u de gegevens op de usb-stick versleutelt.

Dit geldt bijvoorbeeld voor lijsten met adressen van uw klanten, maar al helemaal voor gevoelige informatie. Bijvoorbeeld over religie, etniciteit of gezondheid. U kunt papieren dossiers of een usb-stick verliezen en in sommige gevallen kunnen ze zelfs worden gestolen.

## 3. Wees voorzichtig met het gebruik van (video)chatdiensten

Maak voor gesprekken waarin u gevoelige gegevens bespreekt bij voorkeur gebruik van de beschikbare veilige communicatiemiddelen. Dat is allereerst de telefoon. Soms hebben organisaties beveiligde opties om te beeldbellen of te chatten.

Zorgorganisaties

Veel zorgorganisaties gebruiken bijvoorbeeld systemen die voldoen aan de strenge normen die er voor de zorg zijn vastgesteld, voor gesprekken met patiënten. Gebruik deze, als ze beschikbaar zijn. Voor meer informatie, zie Beeldbellen tijdens de coronacrisis op de website van de KNMG.

Geen beveiligde opties?

Heeft uw organisatie geen beveiligde opties om te beeldbellen of te chatten? En is het echt noodzakelijk om deze middelen in te zetten? Ga dan bewust om met eventuele alternatieven. Bijvoorbeeld apps als Facebook Messenger, Skype of Whatsapp.

FaceTime en Signal worden over het algemeen als veilig alternatief beschouwd, maar wees zelfs met het gebruik van deze apps voorzichtig. De AP heeft namelijk bij geen van de genoemde apps onderzocht of ze AVG-proof zijn.

Gebruik deze apps tijdens de coronacrisis dus bij hoge uitzondering. Goede zorg gaat in deze crisis boven privacy, maar neem wel belangrijke waarborgen.

Zorg dat u zo min mogelijk gevoelige gegevens bespreekt. Noem bijvoorbeeld geen namen, maar gebruik in plaats daarvan zaken als agendanummering of patiëntennummers.

Breng degene om wie het gaat waar het kan wel op de hoogte van de privacyrisico's bij het bespreken van persoonsgegevens via een consumentenapp. Vraag waar het kan toestemming aan bijvoorbeeld de patiënt met wie u spreekt.

Gebruikt u een chatapp als Signal of Whatsapp? Wis dan in ieder geval na elk gesprek de chathistorie. En denk eraan dat u checkt of de app die u gebruikt uw berichten versleuteld verzendt. Beveilig uw internetverbinding met een sterk wachtwoord.

## 4. Let op phishingmails

Krijgt u e-mailberichten die u niet verwacht of die van een onbekende afzender zijn? Klik dan niet op links in deze e-mailberichten, open geen bijlagen en vul geen gegevens in.

Het is bekend dat cybercriminelen gebruikmaken van de coronacrisis door phishingmails te versturen. Dat zijn nepmails met bijvoorbeeld informatie over het coronavirus. De criminelen proberen hiermee informatie te ontfutselen of malware op uw computer te installeren.

Houd hier de komende tijd rekening mee. Krijgt u zo'n mail binnen? Meld het dan bij de ICT-afdeling van uw organisatie.

Meer weten over beveiliging bij thuiswerken? Kijk bij Voorzorgsmaatregelen thuiswerken op de site van het Nationaal Cyber Security Centrum.