De praktijk

Onze maatschappij wordt steeds verder gedigitaliseerd

De huidige privacywetgeving (Wet Bescherming Persoonsgegevens) voldoet niet meer aan de eisen van onze steeds digitaler wordende samenleving. Er moest nieuwe regelgeving komen die tegemoet komt aan de snelle voortgang van technologische ontwikkelingen. Met dit doel voor ogen is de GDPR ontwikkeld (General Data Protection Regulation). In Nederland heeft deze wet de naam AVG gekregen: de Algemene Verordening Gegevensbescherming.
De AVG is op 25 mei 2016 in werking getreden maar pas vanaf 25 mei 2018 echt van toepassing. We bevinden ons nu dus in een overgangsfase, die gebruikt kan worden ter voorbereiding op de AVG. Op dit moment (2017) is dus nog gewoon de WBP
(Wet Bescherming Persoonsgegevens) van toepassing maar de AVG is wel al actief.

Oude gewoonten zijn hardnekkig

Mensen zijn gewoontedieren; ook als het gaat om het vastleggen van gegevens. Vaak werken we privé al met Microsoft Office, dat ook erg handig lijkt voor het verwerken van gegevens van je cliënten. Het gebeurt dan ook vaak dat counsellors de dossiers van cliënten maken en opslaan in Excel of Word. Dit lijkt handig omdat je deze bestanden makkelijk kunt uitwisselen; bijna iedereen werkt er immers mee. Dus als je cliënt aan het einde van het counselling traject vraagt om een kopie van zijn dossier dan is het zeer eenvoudig om dit via een email attachment naar hem of haar te sturen.

Het Microsoft Officepakket is echter niet bedoeld en niet geschikt voor deze taken. Vooral de beveiliging van de bestanden is daarvoor onvoldoende. Je doet er veel beter aan om je dossiers op te bouwen in een programma dat daarvoor speciaal ontwikkeld is. De software van Intramed is daar een goed voorbeeld van. Maar dit bedrijf is niet het enige; er zijn een aantal ondernemingen die prima software bieden voor het vastleggen van cliëntgegevens. Naast de veiligheid van dergelijke pakketten is ook het gemak een groot voordeel: je hoeft niet zelf aan de slag te gaan met Excel om een systeem te ontwikkelen dat aan je eisen voldoet. Daarbij hoef je je meestal ook niet druk te maken over backups; die functionaliteit zit in de meeste gevallen standaard in deze softwarepakketten ingebouwd.

Wat het versturen van dossiers en andere cliëntgegevens over het internet betreft: stuur dit soort gegevens ***nooit*** onversleuteld! Het sturen van privacygevoelige gegevens via E-mail is sowieso een zeer slecht idee. E-mail is slecht beveiligd; iemand met wat geavanceerdere kennis van computers kan een attachment vrij eenvoudig onderscheppen, met alle gevolgen van dien. Wil je toch privacygevoelige gegevens digitaal versturen, zorg dan dat ze versleuteld zijn. Dit kan met de diensten van Zivver, te vinden op https://www.zivver.com/nl/

Het belang van goede wachtwoorden

Tegenwoordig kun je belangrijke bestanden, websites of dossiers prima beveiligen met een wachtwoord. Het grote probleem bij het gebruik van wachtwoorden, is dat veel mensen een makkelijk te raden wachtwoord gebruiken. Ze kiezen hun eigen geboortedatum of de naam van hun favoriete huisdier als wachtwoord en denken daarmee hun belangrijke gegevens veilig te hebben opgeslagen. Maar het moge duidelijk zijn dat mensen die jou een beetje kennen een dergelijk wachtwoord binnen een paar minuten kunnen achterhalen. Doe dit daarom niet en maak gebruik van een lastig te achterhalen wachtwoord door het als volgt samen te stellen:

- minstens 10 tekens lang maar liefst meer
- gebruik hoofdletters, kleine letters en cijfers
- voeg bijzondere tekens toe zoals bijvoorbeeld & % $ #.
- verander wachtwoorden regelmatig
- gebruik voor elke toepassing / website een ander wachtwoord

Vooral dit laatste is iets wat maar weinig wordt gedaan. Veel mensen gebruiken één wachtwoord voor alle websites waarop ze zich registreren en kiezen ook voor de toegang tot gegevens op hun computer geen ander wachtwoord. Dit omdat ze anders een enorme hoeveelheid wachtwoorden moet onthouden; iets wat in de praktijk bijna niet te doen is. Logisch, zou je denken. Maar er zijn handige applicaties die hierbij kunnen helpen: de zogenaamde password managers. Een password manager is een klein programma dat je in je webbrowser kunt installeren.
Na de installatie vul je één keer op elke benodigde plek je inloggegevens in en de software ‘onthoudt’ deze vervolgens voor je. Zodra je een volgende keer weer dezelfde website bezoekt, worden de inloggegevens volledig automatisch ingevuld. Als je wachtwoorden wilt aanpassen dan kan dat natuurlijk: je hoeft dan alleen nog maar het zogenaamde master wachtwoord te onthouden.
Een goede passwordmanager is LastPass; te vinden op https://www.lastpass.com/nl De gratis versie is beschikbaar in het Nederlands en zal in de meeste gevallen goed voldoen.
De oplettende lezer zal nu opmerken: “Ja, maar als die gegevens online opgeslagen worden dan kunnen er ook problemen ontstaan als zo’n bedrijf gehackt wordt.” Dat is waar, maar de kans dat je problemen krijgt als je heel simpele wachtwoorden of overal dezelfde wachtwoorden gebruikt, is vele malen groter dan de kans dat logingegevens op straat komen te liggen via een password manager. Deze bedrijven beveiligen de gegevens zeer goed omdat het immers hun broodwinning is: ze kunnen zich niet veroorloven daar slordig mee om te springen. Toch blijft het oppassen geblazen; niet alle bedrijven die dergelijke software aanbieden zijn bonafide. Maak daarom gebruik van de grote merken zoals LastPass, KeyPass of Dashlane (deze laatste is wel een stuk duurder).

Wachtwoorden in apparaten

We maken van steeds meer apparaten gebruik die zijn aangesloten op het internet. Denk aan je mobiele telefoon, je laptop en het apparaat dat het mogelijk maakt om draadloos te internetten: je router. Vooral die router kan een groot gevaar vormen als het gaat om privacy. De router maakt zich namelijk bekend door het laten zien van een SSID (Server Set IDentifier). Dit is de naam van je netwerk. Je hebt vast wel eens op je telefoon gezien dat er diverse netwerken in je buurt zijn. Zo'n naam van een netwerk noemen we dus een SSID. Deze gegevens zijn vanaf de fabriek ingevoerd. Standaard wordt daar door de fabriek ook een wachtwoord bij gezet. Door het invullen van de SSID en het wachtwoord op je telefoon kun je verbinding maken met het netwerk. Meestal staan die gegevens op een sticker op het apparaat. Verander het standaard wachtwoord want mensen die kwaad willen kennen dergelijke in de fabriek ingestelde wachtwoorden. Je moet je goed realiseren dat als iemand de wachtwoorden van je router kent, hij/zij alle apparaten die van die router gebruik maken, kan bedienen en manipuleren. Als jij dus bijvoorbeeld thuis op je mobiele telefoon internet gebruikt en iemand in je buurt kent het wachtwoord van je router dan kan hij via dat apparaat in je mobiele telefoon komen; zeker als je geen wachtwoorden op je telefoon hebt ingesteld. Een sterk, moeilijk te raden wachtwoord voor je router is dus van enorm groot belang. Bij de meeste routers kun je de instellingen aanpassen via een website met een adres dat er ongeveer zo uitziet: http://167.673.983.7 (deze cijfers zijn in dit voorbeeld willekeurig gekozen uit veiligheidsoverwegingen). Hou er rekening mee dat als je de wachtwoorden in de router aanpast, deze ook aangepast moeten worden in alle apparaten die draadloos zijn aangesloten op de router.

Een router is de poort naar je draadloze internet apparatuur; een goede beveiliging is cruciaal

De mobiele telefoon

De mobiele telefoon is niet meer weg te denken uit onze maatschappij. Dat is ook wel logisch, want behalve dat je er makkelijk mensen mee kunt bereiken op diverse manieren (denk aan Whatsapp, SMS, email) heb je in feite een heel kantoor op zak. Je kunt documenten bewerken en versturen, overleg plegen met meerdere mensen tegelijk via bijvoorbeeld Skype, of even snel je social media accounts checken. Je kunt zelfs als je over de juiste software beschikt en bijvoorbeeld ambulant werkt, onderweg de gegevens checken van een cliënt die je gaat bezoeken.
De huidige mobiele telefoons zijn niets minder dan complete computers. Je moet er dan ook op die manier mee omgaan als het gaat om de bescherming van gegevens. Uitgebreide mogelijkheden kunnen ook grote gevaren betekenen. Het is daarom goed om je telefoon niet aan anderen uit te lenen. Als je werknemers hebt, laat hen nooit met hun mobiele telefoon van jouw wifi netwerk gebruikmaken.
Een ander belangrijk punt: wees enorm voorzichtig met de zogenaamde wifi spots. Dit is een service die door een aantal mobiele providers wordt aangeboden. Die wifi spots kun je beschouwen als een soort openbaar wifi netwerk. Je kunt via zo'n netwerk op je mobieltje internet gebruiken zonder dat de databundel wordt aangesproken. Je werkt dan immers via een wifi verbinding en dan is je databundel dus op dat moment overbodig. Daarnaast bieden veel bedrijven (zeker in de horeca) ook gratis wifi aan als je bij hen naar binnen loopt. Dit lijkt handig en goedkoop, maar het kan je peperduur te staan komen. Dit soort openbare netwerken is namelijk in veel gevallen niet of slecht beveiligd. Daar komt bij dat ze vaak erg traag zijn waardoor je online weinig mogelijkheden hebt. Maak alleen van een dergelijk netwerk gebruik voor simpele dingen als je mail checken. Gebruik het echt ***nooit*** voor bankzaken of het benaderen van je praktijk / cliëntgegevens. Persoonlijk gebruik ik ze nooit: de huidige databundels die je tegenwoordig bij je telefoon abonnement krijgt zijn dermate groot dat de noodzaak om dergelijke onveilige netwerken onderweg te gebruiken gering is.

IoT
Koelkasten, wasmachines, babyfoons, TV's, audio-apparatuur: steeds meer apparaten die we dagelijks gebruiken hebben een verbinding met het internet. Deze ontwikkeling wordt IoT genoemd: Internet of Things. Dit biedt nieuwe mogelijkheden, zoals bijvoorbeeld een koelkast die je via internet een waarschuwing geeft op je mobiele telefoon, precies op het moment dat jij in je auto zit en niet ver verwijderd bent van een supermarkt, zodat je meteen even een nieuw pak melk kunt kopen.
Er zijn tal van andere handige toepassingen te bedenken als de apparaten die je dagelijks gebruikt zijn aangesloten op het internet. Maar er schuilt ook een gevaar in. De fabrikanten van dergelijke 'slimme' apparaten besteden doorgaans zeer weinig aandacht aan de beveiliging van dergelijke apparatuur. Vaak kun je het voorgeprogrammeerde wachtwoord niet eens wijzigen.
Let er bij het kopen van 'slimme' apparatuur op dat je het wachtwoord zelf kunt aanpassen. Kan dit niet, koop het apparaat dan liever niet.

Opslag van gegevens

In de wijze van opslag van gegevens is de laatste jaren veel veranderd door de digitalisering, maar uiteraard ook de snelle ontwikkeling van het internet. Er zullen nog maar weinig bedrijven of instellingen zijn die uitsluitend werken met papieren dossiers of cliënt kaarten. Het opslaan van gegevens gaat steeds makkelijker en sneller. We kunnen daarbij kiezen uit een keur aan opslagmedia. Een van de meest populaire opslagmedia is tegenwoordig de USB-stick. Klein, goedkoop en je kunt er enorm veel op opslaan. De kleine afmetingen zorgen er helaas ook voor dat ze makkelijk zoekraken. Het gevaar van het verliezen van privacygevoelige gegevens ligt dan op de loer. Wees er dus heel voorzichtig mee en maak het liefst gebruik van sticks met data encryptie: op een dergelijke stick worden de gegevens versleuteld opgeslagen zodat ze bij onverhoopt verlies niet voor iedereen toegankelijk zijn.
Als een USB-stick qua opslagcapaciteit niet groot genoeg is kun je je toevlucht nemen tot een externe USB-drive. Dit is een harde schijf die je makkelijk kunt aansluiten op je computer. Ze zijn voor een zacht prijsje te koop en als je wat meer te besteden hebt kun je ze ook krijgen met enorm grote opslagcapaciteiten.

USB drives zijn snel, betaalbaar en kunnen enorme hoeveelheden gegevens bevatten

Gegevens delen met anderen

Maar hoe handig is het als je met een heel team van die ene harde schijf gebruik kunt maken? NAS staat voor Network Attached Storage. Als je gegevens met anderen wilt delen, is een NAS enorm handig maar voorzichtigheid is geboden. Simpel gezegd is het een harde schijf die op je computernetwerk is aangesloten waardoor de gegevens die erop staan toegankelijk zijn voor alle computers in het netwerk en in principe zelfs vanaf elke plek ter wereld waar een internetverbinding beschikbaar is. Je kunt op een NAS precies instellen welke gegevens iemand wel of niet mag inzien zodat niet alles voor iedereen toegankelijk is of slechts beperkt toegankelijk. NAS-systemen kunnen net als gewone harde schijven beschikken over een forse opslagcapaciteit. Die is meestal zelfs vele malen groter dan een gewone externe USB drive omdat voor de meeste exemplaren geldt dat er meerdere harde schijven in zitten.

Houd er rekening mee dat een NAS systeem in beginsel *niet* bedoeld is als backup systeem. Het is bedoeld om gegevens met meerdere computers te delen of om muziek en video te streamen naar diverse apparaten. Persoonsgegevens zet je bij voorkeur niet op een NAS systeem. Doe je dit toch, zorg er dan voor dat de gegevens goed beveiligd zijn door middel van encryptie (hierover later meer). Schakel daarnaast de optie om het NAS systeem buiten het eigen netwerk te benaderen (bijvoorbeeld via je mobiele telefoon als je onderweg bent) uit. Maar het is ondanks deze goede voorzorgsmaatregelen toch een risicovollere optie dan een standaard USB-drive.

Een NAS systeem met ruimte voor 4 harde schijven

Online opslag

Wil je liever geen fysieke apparatuur aanschaffen voor de opslag van gegevens dan kun je kiezen voor online opslag. Microsoft OneDrive en Google Drive zijn bekende voorbeelden van opslagmethoden in de cloud. Je betaalt een paar euro per maand en kunt vervolgens honderden gigabytes aan gegevens in de cloud opslaan.

Alle bovengenoemde opslagmedia hebben gemeen dat ze enorm handig zijn en veel gegevens kunnen bevatten. Maar voorzichtigheid blijft geboden, zeker als je een NAS-systeem of online opslag gebruikt. Data die op het internet belanden kunnen in principe niet verwijderd worden omdat iemand ze heel snel kan kopiëren. Daarom is het opslaan van persoonsgegevens in de cloud bepaald niet ongevaarlijk. Grote bedrijven zoals Google en Microsoft doen er alles aan om hun systemen zo veilig mogelijk te maken maar ook zij kunnen niet garanderen dat er nooit iets misgaat. Zij hebben wel meerdere backup systemen en ze maken gebruik van zeer krachtige beveiligingssystemen maar goed opletten wat je doet blijft belangrijk. Daarom is het aan te raden om persoonsgegevens offline te bewaren op een goed beveiligde externe USB drive, die je ***niet*** permanent op een computer hebt aangesloten.

Houd je gegevens binnen de Europese Economische Ruimte (EER)

Als je besluit om persoonsgegevens online op te slaan dan moet je je goed realiseren dat bijzondere persoonsgegevens niet buiten de Europese Economische Ruimte (EER) mogen komen. De EER bestaat uit alle lidstaten van de EU + Noorwegen, IJsland en Liechtenstein. Hoewel dit strikt genomen alleen voor bijzondere persoonsgegevens geldt, is het verstandig dit voor alle persoonsgegevens te laten gelden; dus ook geen andere persoonsgegevens buiten de EER op te slaan.

E-mail

Hotmail of Gmail?

Indien je Hotmail of Gmail gebruikt voor de communicatie met je cliënten, dan is het goed om nu al te weten dat je actie zult moeten ondernemen.
Veel mensen realiseren het zich niet maar E-mail is per definitie onveilig. Het maakt daarbij niet uit van welke provider je e-mail gebruikt: de onveiligheid ligt aan de basis van e-mail: dit staat los van de provider.
Daarnaast bevat e-mail vaak bijlages die - net als de e-mails zelf - opgeslagen worden op servers. Als die e-mails en/of daaraan gekoppelde bijlagen persoonsgegevens bevatten mogen ze dus ook niet buiten de EER opgeslagen worden. Dit is belangrijk omdat veel mensen gebruik maken van een Hotmail of Gmail adres.

Google is ver in het voldoen aan de AVG. Zo hebben zij onder andere in Delfzijl datacenters gebouwd om te kunnen voldoen aan de eis dat de data op Europees grondgebied bewaard dient te worden. Ook hebben zij inmiddels de mogelijkheid om een bewerkersovereenkomst met Google te tekenen. Voor meer informatie kun je terecht op deze website, waar gedetailleerd beschreven staat hoe Google voldoet aan de AVG. Je zult op deze pagina veelvuldig de afkorting GDPR tegenkomen: dit is de internationale naam voor de AVG (General Data Protection Regulation). https://www.google.com/intl/nl/cloud/security/gdpr/

Let wel dat je zelf actie richting Google dient te ondernemen en dat dit verplicht is.

Van Hotmail is de status zeer onduidelijk. Al jaren voert eigenaar Microsoft een sterfhuis beleid uit. Wel zegt Microsoft ondersteuning toe m.b.t. Outlook accounts. Ook Microsoft heeft een site over de AVG Deze is te vinden via de volgende link:

https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx

Echter: Hotmail wordt, voor zover nu is te overzien, niet meegenomen in de AVG compliance door Microsoft. Reden genoeg om te adviseren een Hotmail adres niet meer te gebruiken voor zakelijk e-mail verkeer.

Gmail zal dan het eerste alternatief zijn maar ook diverse andere hostingbedrijven hebben goedkope en goede oplossingen. Ik noem bv. https://www.transip.nl/webhosting/emailonly/

Bron NFG Nieuwsflits nr. 209

Een e-mail bericht naar meerdere personen tegelijk sturen

Soms moet je een e-mail naar meerdere personen tegelijk sturen. In dat geval is het goed om niet alle adressen in het vakje “Aan:” van je mailprogramma te zetten. Alle mensen waar je het bericht naar toe stuurt kunnen dan namelijk elkaars adressen zien en dat is niet altijd wenselijk. Zeker niet als zo’n bericht naar heel veel mensen wordt gestuurd die elkaar misschien ook nog niet eens kennen. Het gevaar van spam ligt dan op de loer. Doe dit dus niet.
Het is veel beter om de adressen allemaal te zetten in het vakje BCC. Dit staat voor Blind Carbon Copy, en betekent dat de ontvangers niet van elkaar weten dat ze het betreffende bericht krijgen. De ontvangers kunnen ook elkaar adressen niet zien.
Sommige mailprogramma’s eisen dat er bij “Aan:” iets staat; het vakje mag bij zo’n programma dus niet leeg blijven. Als jij van zo’n programma gebruik maakt, zet daar dan een adres van jezelf in.

Data encryptie

Hoewel het zoals hierboven al gezegd niet aan te raden is persoonsgegevens online op te slaan gebeurt dit in de praktijk toch vaak. Als je dit doet, zorg dan dat de gegevens goed beveiligd zijn, bijvoorbeeld door deze te versleutelen. Dit wordt ook wel data encryptie genoemd. De gegevens worden dan volgens een computer algoritme onleesbaar gemaakt alvorens ze opgeslagen worden. Deze versleuteling is zo sterk dat zelfs de krachtigste computers enorm veel tijd nodig hebben om de coderingen te ontcijferen. Voor kwaadwilligen is het daardoor niet meer interessant die gegevens te stelen.

Vragen over encryptie

Het versleutelen van bestanden is broodnodig om bestanden en devices veilig te houden. Dat geldt zeker in het huidige tijdperk, waarin cyber criminaliteit welig tiert en internet criminelen steeds nieuwe manieren ontwikkelen om gevoelige gegevens van derden te pakken te krijgen. De AVG speelt hier op in door Europese burgers te dwingen hun data goed te beschermen. Door gebruik te maken van data-encryptie, voorkom je dat derden over je schouder meekijken als je wachtwoorden intikt of andere gevoelige informatie digitaal opslaat of verstuurt. Maar wat is encryptie precies?

Wat is encryptie?

Versleuteling of encryptie is de techniek waarbij je gegevens tijdelijk onleesbaar maakt als je ze opslaat of verstuurt. Het is dus een manier om gevoelige informatie te beveiligen tegen kwaadwillende derden zoals hackers en cybercriminelen. Om de versleutelde gegevens weer leesbaar te maken, is een sleutel nodig. Dit is meestal een uitgebreide reeks van cijfers en letters. Zonder de sleutel kom je dus niet aan de beveiligde data. Het ver- en ontsleutelen van gegevens wordt uitgevoerd door een complex algoritme. Tegenwoordig merk je in de praktijk nog maar weinig van dit decryptie proces door de enorme rekenkracht van de moderne computers. Er zijn op de huidige markt diverse programma's beschikbaar waarmee je bestanden, hardware en apparaten zoals je computer of mobiel kunt versleutelen. Een overzicht van enkele van deze programma's:

BitLocker: dit is een programma van Microsoft dat vanaf Windows 7 in de Enterprise versies van het besturingssysteem zit. BitLocker versleutelt de hele harde schijf van je computer en kan worden aangezet door naar de verkenner te gaan en met de rechtermuisknop op de map C: te klikken. De Home versie, die op veel computers standaard is geïnstalleerd, beschikt ***niet*** over BitLocker.

Apple FileVault: dit programma geeft je de mogelijkheid om jouw iMac of MacBook te versleutelen. Het programma werkt grotendeels hetzelfde als de Windows tegenhanger. Het belangrijkste verschil is dat de sleutel van de Apple FileVault wordt opgeslagen op een iCloud-account.

Naast de bovengenoemde encryptie programma's zijn er ook nog diverse opties van derde partijen beschikbaar. Populaire en deugdelijke voorbeelden zijn VeraCrypt (gratis basisversie, gebruiksvriendelijk en dankzij hashing technieken erg goed bestand tegen grootschalige aanvallen), CryptoExpert 8 (een sterk, op Windows toegesneden programma dat meerdere vormen van encryptie combineert) en DiskCryptor.

Je website

De meeste mensen zullen het zich niet meteen realiseren maar op een website worden gegevens opgeslagen. Wie heeft er nooit zo'n irritante cookie-melding weggeklikt? Een cookie is een stukje code dat veel mogelijkheden biedt. Het kan bijvoorbeeld ervoor zorgen dat je 'herkend' wordt zodat je bij een volgende bezoek een aanbieding krijgt die voor jou geschikt is. Je hebt vast wel eens gemerkt dat als je naar een product op zoek was en je even later naar een totaal andere website ging, er advertenties op die pagina stonden van producten waar je net nog naar op zoek was. Dit wordt gedaan door het installeren van een cookie op jouw computer.
Maar ook de website van jouw praktijk slaat gegevens op. Denk maar eens aan het contactformulier dat een bezoeker van je site kan invullen. Deze gegevens bevatten persoonsgegevens en vallen daarom ook onder de AVG.

Een SSL-certificaat

Naast dat invulformulier, gaan er ook andere gegevens van jouw computer naar je site, en omgekeerd. Dat kunnen de gegevens zijn die ingevuld worden op je webformulier, maar ook wachtwoorden bijvoorbeeld. Deze uitwisseling van gegevens kan door kwaadwillenden onderschept en misbruikt worden. Je kunt dit een stuk minder interessant maken door een SSL-certificaat op je site te installeren. SSL staat voor Secured Socket Layer en houdt in dat alle gegevens van en naar je site versleuteld worden. Het is zeer sterk aan te raden een dergelijk certificaat te installeren. Voor de kosten hoef je het niet te laten want dit kan al vanaf enkele tientjes per jaar. Je webdesigner en / of hosting provider (het bedrijf dat je site online houdt) kunnen je hier verder over informeren. Websites die beschikken over een certificaat kun je herkennen aan het groene sleutel symbool voor het adres. Het adres zelf ziet er ook iets anders uit. Het adres van een website zonder certificaat ziet er zo uit: http://mijnbedrijf.nl Als er een certificaat is geïnstalleerd dan komt er een 's' achter http. Het adres is dan dus https://mijnbedrijf.nl. Die 's' staat voor 'secure'.
Naast het veiligheidsaspect, is een SSL-certificaat vanaf januari 2017 ook van belang voor de vindbaarheid van je website. Google heeft als belangrijkste doel zo goed mogelijke zoekresultaten te produceren en stelt daarom steeds strengere eisen aan je website. Vanaf nu zal Google een website als onveilig gaan aanmerken als deze niet beschikt over een SSL-certificaat.

Disclaimer

- *De tekst in dit document is met de grootst mogelijke zorg samengesteld. De tekst is informatief en in eerste instantie voor het MKB bedoeld en pretendeert niet volledig te zijn. Voor sommige - vooral grote - organisaties zullen maatregelen noodzakelijk zijn die in deze tekst niet worden genoemd.*
- *De AVG is recente wetgeving; er is nog niet zo veel jurisprudentie over. Mogelijk dat er in de toekomst wijzigingen in de AVG wetgeving aangebracht worden n.a.v. jurisprudentie.*
- *Laat documenten die voor de AVG worden gemaakt (o.a. verwerkingsregister, DPIA) altijd controleren door een jurist met kennis van de AVG.*
- *Jotiko en/of eigenaar Jo Tummers kunnen niet aansprakelijk gesteld worden voor mogelijke onvolkomenheden in de tekst en de mogelijk daaruit voortvloeiende gevolgen.*