AVG-paraplu OPTIEKadviseurs®

Op 25 mei 2018 wordt de wet Algemene Verordening Gegevensbescherming van kracht. Deze nieuwe wetgeving heeft sterke gevolgen voor u als zelfstandig optiekondernemer, want opticiens vallen in deze wetgeving onder de verzwaarde groep omdat er medische persoonsgegevens verwerkt worden bij optiekwinkels. Dus zorg dat u AVG-proof bent, want de boetes op overtreden van deze wet zijn hoog.

Omdat wij bij OPTIEKadviseurs® begrijpen dat u al druk genoeg bent met het werk in en aan uw winkel hebben wij in samenwerking met onze partners een AVG paraplu ontwikkeld om u te ondersteunen bij het AVG-proof maken van uw onderneming.

We hebben een aantal benodigde zaken die wij u in pakketvorm kunnen aanbieden en die u praktisch ondersteunen in uw AVG traject.

U kunt zelf vrij bepalen van welke pakketten u gebruik wilt maken en u doet hierbij rechtstreeks zaken met de betrokken aanbieders.

Omdat er nog een aantal AVG zaken zijn die nog niet geheel duidelijk liggen, en deze wellicht nog in de praktijk getoetst en aangepast zullen worden, zult u van de aanbieders nog updates kunnen verwachten in de loop van het jaar. Daarnaast zullen een aantal documenten speciaal voor uw onderneming aangepast worden.

Alle opdrachten en facturen lopen rechtstreeks via de genoemde bedrijven en niet via OPTIEKadviseurs®.

U kunt de pakketten bestellen via: www.optiekadviseurs.nl/avg-bestel

Indien u nog vragen heeft:
OPTIEKadviseurs®
Bert Smelik
info@optiekadviseurs.nl
030-6042627

AVG pakketten van De Raadgevers

De Raadgevers ondersteunen u in uw AVG traject

Zelf doen?

OPTIEKadviseur De Raadgevers heeft een uitgebreid **'doe-het-zelf' AVG pakket** ontwikkeld waarmee u stapsgewijs door uw AVG handelingen geleid wordt. In dit pakket zit het **stappenplan**, de benodigde formulieren én heeft u rechtstreeks toegang tot een persoonlijke telefonische begeleiding bij de implementatie van het pakket in uw onderneming.

Ook zullen uw Algemene Voorwaarden op maat, en AVG-proof, gemaakt worden. U ontvangt alle formulieren digitaal en verwerkbaar zodat u het kunt aanpassen voor uw eigen bedrijf.

De kosten voor dit 'doe-het-zelf' pakket bedragen éénmalig **€ 495,00** (ex btw en per vestiging).

Volledig ontzorgen?

Wilt u het professioneel aanpakken en u permanent én op locatie laten ondersteunen op AVG gebied?

Dan biedt De Raadgevers u het volledige '**Optiek AVG PPO'** pakket. Dit pakket is additioneel op het 'doe-het-zelf' pakket en biedt u de volgende service.

- U heeft een vaste externe Privacy Protection Officer die u niet alleen ondersteunt bij het AVG proof maken van uw bedrijf, deze externe medewerker zal u ook duurzaam ondersteunen bij uw AVG verantwoordelijkheden. Dus indien er zich AVG zaken voordoen kunt u direct een beroep doen op uw eigen externe PPO. Daarnaast zal uw externe PPO elk jaar een audit verrichten in uw bedrijf om te controleren of alles nog AVG up-to-date is.

De kosten voor dit 'Optiek AVG PPO pakket' lopen via een maandelijks abonnement met een bedrag van **€ 49,50** per maand. (ex btw, per vestiging en minimaal 12 maanden)

de Raadgevers
helpt ondernemen

Uw eigen externe Privacy Protection Officer (PPO) voor Opticiens

Wilt u ontzorgd worden bij het regelen van AVG in uw bedrijf en hierbij professioneel begeleid worden?
Dan biedt De Raadgevers u uw eigen PPO op abonnement basis:

De voordelen van een externe Privacy Protection Officer

* Altijd iemand met actuele juridische kennis en inzicht op het gebied van privacywetgeving
* Een kritische blik van buitenaf op de bedrijfsvoering op het gebied van privacy
* Vrijheid om de verantwoordelijke aan te kunnen spreken
* De vrijheid om medewerkers aan te spreken over de werkwijze die ze hanteren

Het abonnement
Het abonnement van de externe PPO omvat het volgende in:

* Medewerkers meenemen in het privacy-compliant werken
* Dienen als vraagbaak voor diverse privacy vragen
* Periodieke check op AVG compliance, aanpassing van de processen en AVG documenten binnen de organisatie
* Optreden als PPO van het bedrijf naar derden, met oog op voorkoming van mogelijke juridische gevolgen
* Vast aanspreekpunt van de organisatie bij de Autoriteit Persoonsgegevens

Wat doet u zelf?
Er zijn uiteraard ook dingen die u zelf doet:

* U houdt zich bezig met de dagelijkse gang van zaken met betrekking tot privacy-controle
* U houdt de regie over hetgeen u uitbesteed.

De kosten
De Raadgevers bedrijfsjuristen biedt u een eigen externe PPO aan voor een maandelijks bedrag van € 49,50 (ex btw, minimaal 12 mnd)

Vragen?
Heeft u vragen over de externe Privacy Protection Officer?
Mailt u dan naar optiek@deraadgevers.nl of belt u 088-1331133
Uw contactpersoon is Mr. Marjon Joosten

De Raadgevers is partner van OPTIEKadviseurs®

Cyberrisico Verzekering voor zelfstandige opticiens van Multisafe

Cyberrisico is een actueel onderwerp, ook voor zelfstandige optiekondernemers. Want helaas maken cybercriminelen ook slachtoffers onder zelfstandige ondernemingen.

Wat zijn uw risico's op dit gebied en hoe bent u hierop voorbereid? Wij van Multisafe brengen uw risico's graag voor u in kaart en adviseren u bij de benodigde stappen. Deze individuele risicoanalyse is een intensief en tijdrovend proces, maar door de samenwerking met OPTIEKadviseurs® beschikken we echter over veel basis informatie die de risico's op dit gebied voor opticiens goed in kaart brengt.

Op grond van deze analyse hebben we een pasklare verzekeringsoplossing kunnen filteren uit verschillende producten die worden aangeboden. Hierdoor besparen wij u de tijd en kosten van een individuele inventarisatie, welke al snel zo'n € 800,- kost.

In samenwerking met OPTIEKadviseurs® hebben wij een Cyberrisico Verzekering kunnen opstellen voor de zelfstandige opticiens met een netto premie van **€ 590,00** per jaar, per vestiging. Hiermee heeft u al een goede dekking.

Wat wordt er gedekt met deze Cyberrisico Verzekering?

- Schadekosten cybercriminaliteit
- Begeleidingskosten voor oplossen IT-schade door Hacking en Ransomware
- Reputatieschade
- Omzetderving

U kunt deze risico verzekering eenvoudig regelen met OPTIEKadviseur Lex van Loon van Multisafe.

Multisafe
Lex van Loon
a.vanloon@multisafe.nl
030-2212777

Wilt u nog een stapje verder gaan en toch een uitgebreide risico analyse specifiek voor uw onderneming? Neem dan ook contact met ons op, wij leveren ook maatwerk hierin.

Multisafe is partner van OPTIEKadviseurs®

multisafe
register makelaar in assurantiën

Cyber risico's.

Met betrekking tot cyberrisks geven wij onderstaande informatie ter overweging. Het is nogal wat, een aantal zaken zult u herkennen, een aantal zaken is wellicht nieuw. Wij adviseren iedere onderneming waar met data e/o persoonsgegevens wordt gewerkt om over deze risico's na te denken en vast te stellen of deze risico's al dan niet zelf gedragen kunnen worden.

Wat zijn cyberrisks?
Verbond van Verzekeraars: "Het financiële nadeel dat een verzekerde oploopt door of via computer- en/of ICT systemen, zonder dat er sprake is van materiële schade."

Oorzaken (cijfers 2015):
Schadelijke- of criminele aanvallen 46,5%
Nalatigheid 29%
Falen IT-systeem 24,5%

Wereldwijd heeft de geschatte opbrengst van cybercrime 1,5 maal de omvang van de opbrengst uit drugscriminaliteit (anno 2015).

Aandachtspunten:

Systeeminbraak, gevolg van inbraak op systemen of data:
- De kosten van forensisch onderzoek
- De kosten van informeren gedupeerden, betaalkaartbedrijven en toezichthouders
- De kosten voor het opzetten van een callcenter / informatievoorziening
- Vergoeding en ondersteuning van PR specialist om reputatieschade te herstellen
- Kosten van juridisch verweer bij schadeclaim toezichthouder of betaalkaartbedrijf
- Civielrechtelijke boetes / schadevergoeding (verzekerbaar voor zover toegestaan)
- Vergoeding van kosten voor herstel of vervanging bij schade aan website, programma's of elektronische gegevens
- Inschakeling beveiligingsexpert om identiteit hacker te achterhalen
- Vergoeding losgeld in geval van chantage na inbraak op uw systemen
- Inkomstenderving als gevolg van hacking op uw computersystemen

Privacy, gevolgen van gestolen privacygevoelige gegevens (ook als de info elders is opgeslagen blijft de houder verantwoordelijk):
- kosten van onderzoek door bijvoorbeeld justitie of creditcardmaatschappijen
- claims van individuele personen
- boetes opgelegd door toezichthouders, of andere verplichte vergoedingen.

Digitale aansprakelijkheid:
Als de website of e-mail onbedoeld het auteursrecht schendt, laster verspreidt of een virus bevat.

Hacking (schade, veroorzaakt door hackers):
- reparatie, vervanging of herstel van websites, programma's of data
- kosten van gestolen software of data
- kosten van onderzoek en advies in systeembeveiliging
- kosten van forensisch onderzoek naar de oorzaak van een hacking

multisafe
register makelaar in assurantiën

Afpersing:
Schade als gevolg van criminelen die de website of data gijzelen. Zogeheten ransomware, een chantagemethode op internet door middel van malware, is via het Deep Web eenvoudig verkrijgbaar. Ook worden op dat verborgen stuk Internet opdrachten uitgezet om data te gijzelen.

Omzetverlies door cyberaanvallen:
als een DDos-actie of andere aanval op de computersystemen leidt tot omzetverlies, bijvoorbeeld door uitval van een webwinkel.

Datalek:
Melden van een datalek is vanaf 1 januari 2016 verplicht. Een datalek is een inbreuk op de beveiliging waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Hieronder valt niet alleen het vrijkomen (lekken) van persoonsgegevens, maar ook vernietiging daarvan en andere vormen van onrechtmatige verwerking. Voorbeelden: een kwijtgeraakte USB-stick met persoonsgegevens, een verloren of gestolen laptop of een hack van een databestand met persoonsgegevens.

Hiervoor is regelmatig het woord onderzoek gebruikt. Naast de meldplicht is er ook de onderzoekplicht. Forensisch onderzoek naar de oorzaak is specialistisch werk waar tarieven voor gevraagd worden van € 800 per uur.

Welke risico's loopt u?
Als u bevestigend antwoordt op één of meer van de volgende vragen, dan bedreigen cyberrisico's de continuïteit van uw onderneming.

Soort data
Verwerkt u medische, persoonlijke of financiële gegevens van klanten, personeel of patiënten? Denk aan creditcard- of bankgegevens, persoonlijke gezondheidsinformatie of toegangsgegevens (inlogcodes).

Concurrentiepositie
Bezit u vertrouwelijke documenten of geheime informatie over (innovatieve) werkwijzen? Hierbij kunt u denken aan handelsgeheimen of intellectuele eigendommen. Verlies van dergelijke informatie kan de concurrentiepositie van uw klant schaden.

Productieproces
Bent u voor uw productieproces in hoge mate afhankelijk van ICT systemen? Denk aan computergestuurde apparaten of machines, een website of webshop.

Omzet afhankelijkheid
Bent u voor uw omzet in hoge mate afhankelijk van ICT systemen? Bijvoorbeeld computergestuurde apparaten of machines, een website of webshop.

Gegijzeld

Als ze zaterdagochtend 4 november nog wat werk wil doen laat haar laptop het afweten. Het lukt niet om verbinding te krijgen met de server van haar bedrijf. Om het geplande werk toch af te kunnen maken besluit ze naar kantoor te rijden. Ook daar lukt het niet in te loggen op het netwerk, totdat er uiteindelijk een boodschap op het scherm verschijnt: “Uw bestanden zijn versleuteld, betaal $ 4.000,- om weer toegang te krijgen”.

Onze adviseurs hebben in 2017 veel met klanten gesproken over cyberrisico’s. Daarom delen we hier het verhaal van Iris Kuster, eigenaar van Acc-CENT Accountants & Belastingadviseurs. Zij kreeg het afgelopen jaar te maken kregen met een scenario waar je alleen over leest in de krant: een gijzeling van (computer)servers.

Wie is Acc-CENT?

Acc-CENT is een klein, flexibel kantoor dat ondernemers in het MKB adviseert en ondersteunt met persoonlijke en directe diensten op het brede terrein van het ondernemerschap. Dat doen we met een compleet dienstenpakket, snel, met korte lijnen en op een kostenbewuste manier. Zo voeren wij bijvoorbeeld salarisadministraties uit, helpen wij bij het samenstellen van financiële rapportages, en adviseren wij ondernemingen en ondernemers ook privé omtrent belastingen. We zijn dus voortdurend bezig met heel vertrouwelijke data.

Was Acc-CENT al bekend met het fenomeen cyberrisico?

Uiteraard, voorbeelden zijn er genoeg. Op het nieuws, in de krant en op televisie kun je met regelmaat horen wat er gebeurt. Wij maakten echter de inschatting dat wij niet echt een interessante partij zouden zijn voor een hacker. En belangrijker nog, wij hadden de boel best goed op orde. Met z’n allen gingen we sowieso al zorgvuldig om met data van relaties, er draait voortdurend actueel onderhouden software om virussen en malware buiten te houden, en ons systeembeheer hebben wij bewust uitbesteed aan een professionele partij.

Wat is er uiteindelijk gebeurd?

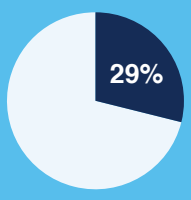
Na de constatering is onze systeembeheerder direct aan de slag gegaan. Hij constateerde dat via een open poort op de server die ooit was gebruikt voor externe besturing was ingelogd op onze server. Alle bestanden waren versleuteld en werden daardoor ontoegankelijk. Er werd ons verzocht om $ 4.000,- te betalen in ruil voor de sleutel waarmee onze gehele administratie weer beschikbaar zou komen. Een ordinaire gijzeling dus.

Wat waren de gevolgen?

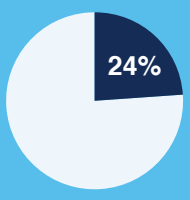
Wij konden nergens meer bij, niemand kon werken. In eerste instantie leek het dan ook alsof $ 4.000,- een aantrekkelijk bedrag was om het probleem op te lossen. Maar daar wilden we niet aan meewerken. Het was bovendien maar de vraag of we daadwerkelijk een sleutel zouden krijgen, en of daarmee alles opgelost zou zijn.
Uiteindelijk hebben wij een volledige herinstallatie gedaan van onze gehele administratie. Alle software

Van alle bedrijven

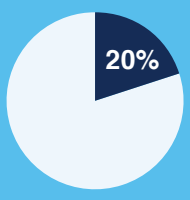
is 29% op frequente basis onderhevig aan een cyber aanval



loopt 24% van de slachtoffers schade en dataverlies op



ondervindt 20% van de slachtoffers een inkomsten- of reputatieverlies



Bron: Norton Symatec Security Survey

Meest voorkomende cyber risico's in het MKB:

- Gehackte telefooncentrale;
- Phising e-mails;
- Politievirus / Lockyransomware;
- DDOS-aanval;
- Kwijtraken laptop of USB stick;
- Datadiefstal.

is opnieuw geïnstalleerd en alle data zijn vanuit de laatste veilige back-up opnieuw ingelezen. Een klus waar we bijna een week met meerdere mensen mee bezig zijn geweest.
Gelukkig hebben een aantal medewerkers extern door kunnen werken omdat we sinds 1 januari 2017 ook software in de cloud gebruiken. Onze systeembeheerder heeft echter flink wat uren gedraaid. En ik ben zelf ook nog lang bezig geweest met het herstel van alle data.
Heel vervelend allemaal, maar we maakten ons de grootste zorgen over de data. We hebben daar direct overleg over gevoerd met de Autoriteit Persoonsgegevens maar tot onze grote opluchting is er geen sprake geweest van een datalek.

De beveiliging was al op een hoog niveau, zijn er desondanks toch nog andere maatregelen getroffen?

Uiteraard, dit willen we niet nog eens meemaken. De relevante virus- en malware software is nog verder uitgebreid en de server is nog verder afgeschermd. Tot op het randje van onwerkbaar zijn zaken beveiligd. Daarnaast hebben we het aantal back-ups nog verder verhoogd, en gaan we nog kritischer om met onze software. Voor de pakketten die het meest intensief worden gebruikt en essentieel zijn voor onze dienstverlening hebben we nog betere maatregelen genomen om in geval van herhaling nog sneller te kunnen herstarten. Allemaal maatregelen om in geval van een herhaling de schade te beperken. Je kunt tenslotte alles beveiligen maar hackers zullen altijd wel weer nieuwe wegen vinden. En uiteraard heb ik het advies voor een cyberverzekering dat al uitgebracht was heel snel opgevolgd.

Wat zou u op het hart willen drukken bij andere ondernemers?

Denk niet dat het je niet zal gebeuren. Niet alleen de grote ondernemingen liggen onder vuur. Hackers proberen gewoon overal binnen te komen. De manieren waarop worden steeds professioneler en inventiever. Het gaat al lang niet meer om een link in een e-mail in slecht Nederlands die niet wordt herkend.
Daarnaast, zorg voor goede procedures die de kans verkleinen en frequente back-ups van je werk zodat je niet afhankelijk bent van een crimineel voor de toegang tot je eigen systemen. En vooral, ga niet in op een voorstel om te betalen. Je weet nooit of je wat krijgt als je betaalt, en wat er daarna nog achterblijft aan geïnstalleerde programma's.

Wat u zegt

'Wij zijn zeer tevreden over de goede snelle en deskundige afwikkeling van onze stormschade. TOP!'

AVG Website Check voor Optiek van eResults

Is uw optiekwebsite al 'AVG-proof'?

En weet u al wat u nog voor 25 mei 2018 moet regelen om aan alle AVG eisen te voldoen met betrekking tot uw website?

OPTIEKadviseurs® ondersteunt u graag hierbij en biedt u in samenwerking met eResults de AVG websitecheck aan.

Bij deze AVG website check lopen de online marketingexperts van eResults uw hele website door op alle benodigde onderdelen. Daarna stellen zij op basis van hun bevindingen een overzichtelijke checklist op waar u zelf, of waar uw websitebouwer, mee aan de slag kan.

Wilt u meer weten? Kijk dan op www.websiteavgproof.nl/avg-optiek

De standaard prijs voor deze AVG check is € 575,- all-in per website

Via uw serviceplatform OPTIEKadviseurs® uw prijs **€ 475,-**

Hoe werkt het?

U regelt deze dienst eenvoudig rechtstreeks met eResults.

Stap 1. Meld uw website aan bij eResults

Dat kan makkelijk en direct via het online formulier (www.websiteavgproof.nl/avg-optiek)

Wilt u liever persoonlijk contact of heeft u vragen, bel dan even: 030 242 0931 (optie 1)

Stap 2. eResults levert de benodigde aanpassingen kant en klaar aan in een duidelijke checklist.

Stap 3. eResults controleert achteraf of alles klopt

Geef aan eResults door zodra alle punten van checklist verwerkt zijn op uw website en zij checken of uw website 100% AVG-proof is.

En mochten er nog vragen hebben tussendoor zijn, dan kunt u altijd bellen naar de helpdesk van eResults.

eResults

Karel Dansen

kareldansen@eresults.nl

030-2420931

WebsiteAvgProof.nl
by eresults

Prijslijst AVG-paraplu OPTIEKadviseurs®

1. AVG pakket De Raadgevers

AVG ‘doe-het-zelf’ pakket éénmalig **€ 495,00**

AVG ‘Optiek AVG PPO pakket’ maandelijks abonnement (min. 12 mnd) van **€ 49,50**

2. Cyberverzekering Multisafe

Deze cyberverzekering netto jaarpremie vanaf **€ 590,00**

3. AVG Website Check voor Optiek

Website Check Optiek per website **€ 475,00**

Alle opdrachten en facturen lopen rechtstreeks via de genoemde bedrijven en niet via OPTIEKadviseurs®. De genoemde bedragen zijn exclusief btw en per vestiging.

Bestellen kan via www.optiekadviseurs.nl/avg-bestel

Indien u nog vragen heeft:

OPTIEKadviseurs®
Bert Smelik
info@optiekadviseurs.nl
030-6042627