Zicht
risico- en
verzekeringsadviseurs

Zijn uw verzekeringen AVG-proof?

In deze whitepaper staat een korte uitleg over de inhoud van de aangescherpte privacywetgeving, maar we staan vooral stil bij de gevolgen voor uw verzekerbare risico's. Want ook daar moet u iets voor regelen.

VERZEKERING • BEDRIJFSRISICO • HYPOTHEEK • PENSIOEN

gelukkig geregeld!

Inhoud

Aanleiding

Privacy wordt voor ieder bedrijf een steeds belangrijker onderwerp. Per 25 mei 2018 is de AVG (Algemene Verordening Gegevensbescherming), ook wel bekend als GDPR (General Data Protection Regulation), van kracht in de gehele EU. Hiermee vervalt de huidige privacywetgeving. Deze zogenaamde AVG/GDPR-regelgeving moet de privacy van uw klanten en medewerkers beschermen en hen meer inzicht geven in waarom, hoe, waar en hoelang hun gegevens bewaard worden. Als uw bedrijf niet aan deze nieuwe eisen voldoet, dan kunt u een hoge boete krijgen: maximaal € 20 miljoen of 4% van de omzet. Hoe groot of hoe klein uw bedrijf ook is, het geldt ook voor u! Het is in het belang van zowel uw klanten als uw medewerkers dat u de juiste maatregelen treft. Niet alleen vanwege de financiële consequenties.

U bent hier ongetwijfeld al druk mee bezig. En u krijgt waarschijnlijk van diverse partijen ook de nodige informatie over acties die u moet nemen om de privacy van de data waar u over beschikt te kunnen waarborgen.

We geven in deze whitepaper een korte uitleg over de inhoud van de aangescherpte privacywetgeving, maar staan vooral stil bij de gevolgen voor uw verzekerbare risico's. Want ook daar moet u iets voor regelen. Want zijn uw verzekeringen AVG-proof?

1. AVG in een notendop

Bijna dagelijks zijn er berichten in het nieuws dat er privacygevoelige klantgegevens van bedrijven gehackt worden of op een andere manier op straat komen te liggen. Dit kan natuurlijk heel vervelende gevolgen voor de betreffende klanten hebben. Maar ook voor uw bedrijf.

Waarom AVG?

In Europa was al een privacywet van toepassing, alleen is deze met de Algemene Verordening Gegevensbescherming (AVG) aangescherpt. Zo zorgt de AVG onder meer voor:

- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor organisaties;
- stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

De verordening is dus aangescherpt om klanten en medewerkers nog beter te beschermen.

Voor wie is de AVG van toepassing?

Deze Europese privacywetgeving is voor alle Europese bedrijven en organisaties van toepassing die persoonsgegevens verwerken van klanten, personeel of andere personen. Vrijwel alle ondernemers krijgen ermee te maken, ook zzp'ers en klein mkb. Door bijvoorbeeld het versturen van een offerte, factuur of (digitale) nieuwsbrief legt u namelijk al persoonsgegevens vast. Dat geldt ook voor het bijhouden van afspraken met klanten, contactgegevens van klanten (zoals adres, e-mailadres of telefoonnummers) of personeelsinformatie.

Ook stichtingen en verenigingen en internationale bedrijven die zaken doen binnen de EU moeten zich houden aan de AVG.

Door de AVG heeft u verantwoordingsplicht. U moet kunnen aantonen dat u de juiste organisatorische en technische maatregelen heeft genomen om aan de AVG te voldoen.

In 10 stappen voorbereid op de AVG

De Autoriteit Persoonsgegevens (AP) houdt in Nederland toezicht op de naleving van de AVG. Het is belangrijk dat u als bedrijf vaststelt wat u moet doen om aan de AVG-regelgeving te voldoen. Om u hierbij te helpen heeft AP een 10 stappenplan opgesteld waardoor u snel overzicht krijgt op een aantal belangrijke AVG-thema's waar u zich op moet voorbereiden. De volledige stappen kunt u hier lezen.

Hulp nodig?

Hieronder staan een aantal partijen/websites waar u terecht kunt voor meer algemene informatie over de AVG of handige checklists.

- De Autoriteit Persoonsgegevens gaat streng toezien op de naleving van de AVG. Dan moet ook duidelijk zijn waar u op moet letten en wat u moet doen. Op deze pagina leest u hier uitgebreid informatie over.
- Ook op de site van de Kamer van Koophandel staat algemene informatie, inclusief een 10-stappenplan voor de voorbereiding en veel gestelde vragen.
- ESET helpt ondernemers, groot en klein, vooral met het technische aspect rond de AVG. En dan in het bijzonder de IT-beveiliging. Denk daarbij onder andere aan oplossingen voor encryptie, toegangsbeveiliging door middel van tweefactor authenticatie en het bieden van bescherming tegen kwaadaardige software.
  Voor de organisatorische en beleidsmatige vraagstukken werken ze nauw samen met privacy specialisten van DPO Consultancy en Mazars.
- Privacy en compliance vormen een grote uitdaging voor veel bedrijven. DPO Consultancy helpt u met de begeleiding naar een veiligere en meer privacy bewuste omgeving. Zowel online als offline. Hun team van onafhankelijke Data Protection Officers (DPO's) en Privacy Implementatie Managers, wordt ingezet om u volledig privacy-compliant te laten werken.
- DAS Rechtsbijstand heeft de DAS Privacy Protect in het leven geroepen om bedrijven de zorgen van de Functionaris voor de Gegevensbescherming uit handen te nemen. Ook kunt u op de website terecht voor een infographic met belangrijke aandachtspunten en de Privacy Scan waarmee u in 5 minuten ziet welke acties u vóór 25 mei 2018 nog moet nemen.
- Het Nederlands Cyber Collectief is een overkoepelend verbond van de cybersector. Als MKB'er kunt u op hun website terecht voor handige hulpmiddelen, preventieve tips, een gratis informatielijn en noodhulp.

Het is essentieel dat u als bedrijf de juiste maatregelen neemt om te voldoen aan de aangescherpte regelgeving. Beleidsmatig, organisatorisch, technisch en softwarematig. Maar zijn uw verzekerbare risico's daarmee ook 'AVG-proof'?

U kunt alles goed geregeld hebben, maar dat betekent niet dat u niet geconfronteerd kunt worden met bijvoorbeeld het lekken van privacygevoelige gegevens. Denk bijvoorbeeld aan uw computer die gehackt wordt of een medewerker die een klantenbestand naar een verkeerd e-mailadres stuurt. Dan kunt u aansprakelijk gesteld worden en loopt u cyber- en datarisico's.

2. Wat gebeurt er als ik nog niet klaar ben voor de AVG?

De huidige privacyrichtlijnen zijn al vanaf 1995 van kracht en in 2001 opgenomen in de Wet Bescherming Persoonsgegevens. In het voorjaar van 2016 is de aangescherpte verordening al in werking getreden, maar op 25 mei 2018 gaat de AVG écht in en moeten bedrijven aan de nieuwe privacyregels voldoen. Bedrijven en instellingen hebben dus bijna twee jaar de tijd gehad om zich hierop voor te bereiden. Dit is een arbeidsintensief traject.

De Autoriteit Persoonsgegevens gaat erop toezien dat ook uw bedrijf aan de regels voldoet. Dit kan op het moment dat u wordt getroffen door een data-inbreuk, maar dat hoeft niet. Zij kunnen ook een reglementair onderzoek uitvoeren zonder specifieke aanleiding.

Wat gebeurt er dan als blijkt dat u nog niet voldoet aan alle richtlijnen?

Boetes en sancties

De Autoriteit Persoonsgegevens kan:

- een administratieve boete opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet.
- uw bedrijf berispen, verbieden om verwerkingen uit te voeren of straffen door certificeringen in te trekken.
- de gegevensstromen naar derde landen of internationale organisaties laten opschorten.
- een bestuurlijke boete onder dwangsom opleggen.

Privacy-aansprakelijkheid

Als u de 10 stappen niet heeft gezet, is de kans groter dat uw bedrijf getroffen wordt door een data-inbreuk. Dit kan zijn door een DDoS-aanval, een hack of andere data- en cybercriminaliteit. Maar denk ook aan het versturen van gegevens naar een verkeerd e-mailadres of het verliezen van een USB-stick of laptop. U kunt in zo'n geval door de persoon van wie gegevens op straat liggen aansprakelijk gesteld worden. In hoofdstuk 5 kunt u een voorbeeld hiervan lezen.

Negatieve aandacht

De sociale media is vandaag de dag niet meer weg te denken. Het is heel gemakkelijk om met weinig inspanning veel mensen te bereiken. Als iemand tevreden is, is dat natuurlijk fijn. Maar als een klant klachten heeft niet. Het gevaar is dus dat er na een data-inbreuk negatieve aandacht aan uw bedrijf gegeven wordt waardoor u reputatieschade oploopt. De kosten kunnen dan enorm oplopen om uw reputatie weer te herstellen.

3. AVG-proof, maar hoe zit het met de verzekerbare risico's?

Op 25 mei 2018 is de AVG van kracht en dan heeft u de 10 stappen keurig doorgevoerd. U heeft beleidsmatig, organisatorisch, technisch en softwarematig maatregelen getroffen. U bent dus AVG-proof en er kan u niets meer gebeuren. Toch?

Wat zijn uw belangrijkste risico's?

Als u alle AVG-maatregelen heeft getroffen, heeft u helaas nog niet de zekerheid dat er geen privacygevoelige gegevens van uw klanten of medewerkers op straat komen te liggen. Denk hierbij aan de volgende gegevens.

Persoonsgegevens
Gegevens aan de hand waarvan personen kunnen worden geïdentificeerd. Denk hierbij aan NAWT-gegevens, e-mailadres, BSN-nummer, rijbewijsnummer, bankrekeninggegevens, gebruikersnamen en wachtwoorden van online accounts, medische gegevens en zorgverzekeringsinformatie.

Beschermde gegevens genoten gezondheidszorg
Gegevens over de verlening en betaling van gezondheidszorg aan de hand waarvan personen kunnen worden geïdentificeerd.

Betaalkaart-gegevens
Gegevens van betaalpassen en creditcards.

Wat zijn de risico's die u loopt als deze gegevens door een data-inbreuk buiten uw organisatie bekend worden?

- **Bedrijfsaansprakelijkheid**. U kunt als bedrijf aansprakelijk gesteld worden voor schade die u, uw werknemers, tijdelijke krachten of vrijwilligers veroorzaken bij de uitvoering van werkzaamheden. Of die uw eigendommen veroorzaken aan derden. Dit kan materiële of letselschade zijn.
- **Beroepsaansprakelijkheid**. U kunt als bedrijf aansprakelijk gesteld worden voor de vermogensschade die u, uw werknemers of tijdelijke krachten veroorzaken door het geven van bijvoorbeeld een verkeerd advies of ontwerp. Maar ook voor financiële schade die ontstaat door het niet nakomen van een gemaakte afspraak.
- **Bestuurdersaansprakelijkheid**. U kunt aansprakelijk gesteld worden voor de handelingen die u als bestuurder van bijvoorbeeld een bv heeft verricht.
- U kunt **imagoschade** oplopen doordat in de publiciteit komt dat u niet zorgvuldig om bent gegaan met de gegevens van uw klanten.
- U kunt **bedrijfsschade** oplopen doordat uw bedrijf stil ligt.
- De Autoriteit Persoonsgegevens kan u een **bestuurlijke boete** opleggen als u de data-inbreuk niet of niet tijdig meldt.
- Tot slot kunt u te maken krijgen met **kosten** voor bijvoorbeeld forensisch onderzoek, juridisch advies, het herstellen van gegevens en het inzetten van een pr-bureau.

Hoe kunt u uw risico's beperken?

Wat kunt u doen om de risico's zo veel mogelijk te beperken?

1. **Voldoen aan de AVG-regelgeving**
   Als u voldoet aan de AVG-regelgeving dan heeft u de basis op orde. U heeft dan alleen niet de zekerheid dat er geen privacygevoelige gegevens in handen van derden komen.

2. **Preventiemaatregelen treffen**
   Om uw privacy-beveiliging in kaart te brengen, hebben we een checklist gemaakt met vragen die u zich minimaal moet stellen.

Vraag	Ja	Nee
Is privacy- en gegevensbescherming integraal opgenomen in de bedrijfscultuur? M.a.w. zijn uw medewerkers bewust van de risico's?		
Heeft u beleid opgesteld over het openen van privé e-mail op het bedrijfsnetwerk/de computers?		
Heeft u een wachtwoordbeleid waarbij medewerkers regelmatig hun wachtwoord moeten wijzigen en moeten kiezen voor sterke wachtwoorden?		
Is er één persoon eindverantwoordelijk voor de beveiliging en gegevensbescherming?		
Is uw software altijd up-to-date? Installeert u direct de nieuwste versies?		
Heeft u waterdichte contracten met uw leveranciers en relaties?		
Beperkt u het aantal verzamelde en bewaarde persoonsgegevens en vertrouwelijke informatie tot het strikt noodzakelijke minimum?		
Maakt u onderscheid in de verzamelde en opgeslagen informatietypen/soorten?		
Heeft u inzicht in de gevolgen voor uw bedrijf als data verdwenen zijn?		
Weet u wat u moet doen als er een datalek binnen uw bedrijf plaatsvindt?		
Evalueert en actualiseert u de bestaande veiligheidsmaatregelen, -plannen en -procedures?		
Maakt u een back-up van uw data en test u deze regelmatig?		

Heeft u minimaal één vraag met nee beantwoord, dan is het belangrijk om verder te onderzoeken welke preventiemaatregelen u nog moet treffen.

3. **Verzekeren**
   Welke maatregelen u ook treft, de kans is altijd aanwezig dat privacygegevens in handen van derden komen. Daarom is het belangrijk om te beoordelen of u bepaalde risico's moet verzekeren. Hieronder behandelen we een aantal verzekeringen die u kunt afsluiten om de kosten zo veel mogelijk te beperken. Daarbij geven we aan of deze dekking bieden voor datalekken.

Aansprakelijkheidsverzekering voor bedrijven

De meeste bedrijven hebben een aansprakelijkheidsverzekering voor bedrijven (AVB) afgesloten. Deze verzekering komt tot uitkering als u aansprakelijk gesteld wordt voor schade die u, uw werknemers, tijdelijke krachten of vrijwilligers veroorzaken bij de uitvoering van werkzaamheden. Of die uw eigendommen veroorzaken aan derden. Dit kan materiële of letselschade zijn.

Met een AVB heeft u echter geen dekking in het kader van AVG. Als u een privacy-fout maakt is er in principe geen sprake van materiële- of letselschade. Het privacy-aansprakelijkheidsrisico is dus niet verzekerd.

Beroepsaansprakelijkheidsverzekering

U kunt ook aansprakelijk gesteld worden voor vermogensschade die u, uw werknemers of tijdelijke krachten veroorzaken door het geven van bijvoorbeeld een verkeerd advies of ontwerp. Maar ook voor financiële schade die ontstaat door het niet nakomen van een gemaakte afspraak. In zo'n geval kunt u terugvallen op uw beroepsaansprakelijkheidsverzekering.

Met een beroepsaansprakelijkheidsverzekering heeft u in sommige gevallen dekking in het kader van AVG. Dit is afhankelijk van de polisvoorwaarden en of u iets te verwijten valt. Het privacy-aansprakelijkheidsrisico is dus niet altijd verzekerd.

Data- en cyberrisicoverzekering

Snel en doelgericht reageren op dataverlies, hackers of cyberaanvallen beperkt de schade. Een cyber- en datarisicoverzekering helpt u met de inzet van een team van ervaren professionals. Zij helpen u databases en websites te herstellen, belanghebbenden te informeren en het juridische traject op te starten zodat u zo snel mogelijk verder kunt.

Met de data- en cyberrisicoverzekering bent u zeker van de volgende dekkingen in het kader van privacy-aansprakelijkheid:

- Vergoeding van de juridische kosten tijdens het onderzoek door bijvoorbeeld justitie, creditcardmaatschappijen of als gevolg van schadeclaims van particulieren.
- Als u claims ontvangt van particulieren (aansprakelijkheidsstelling door derden), worden de verweerkosten en eventueel de claim zelf vergoed.
- Bestuurlijke boetes opgelegd door toezichthouders of andere verplichte vergoedingen.

Niet alleen in het kader van privacy is het afsluiten van een data- en cyberrisicoverzekering verstandig. Ook biedt deze verzekering dekking voor de volgende kosten.

Met een data- en cyberrisicoverzekering kunt u in het kader van privacy-aansprakelijkheid in de meeste gevallen terugvallen op de volgende dekkingen:

Hacking

- 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 identiteit van de hacker.
- Kosten van PR-advies voor reputatiebescherming.

Systeeminbraak

- Kosten van forensisch onderzoek.
- Kosten van communicatie met providers, klanten, toezichthouders, justitie, creditmaatschappijen en andere belanghebbenden.
- Kosten voor extra klantondersteuning, bijvoorbeeld via een call center.
- Kosten van crisismanagement, reputatieherstel en PR-campagnes.

4. Wist u dat? Een aantal stellingen

Tijdens gesprekken met bedrijven hebben we meerdere malen gemerkt dat zij de klok hebben horen luiden, maar dat ze toch niet precies wisten hoe het zat. Daarom hebben we hieronder enkele stellingen opgenomen waarvan we het belangrijk vinden dat u hier ook over nadenkt.

Vanaf 25 mei gebeurt er niet zoveel
De AVG is niet nieuw. Vanaf 24 mei 2016 geldt er al een overgangsfase van de Wbp naar de AVG zodat u tijd genoeg heeft om u voor te bereiden. Vanaf 25 mei 2018 krijgt de Autoriteit Persoonsgegevens niet alleen meer bevoegdheden, ook kunnen klanten vanaf dat moment hun rechten uitoefenen. En dat kan een behoorlijke impact hebben. Paniek is niet nodig, snel handelen wel.

Een functionaris voor de gegevensbescherming (FG) is helemaal niet nodig
Voor sommige organisaties is het verplicht een FG aan te stellen. Voor de grote meerderheid is dat niet het geval. Maar het is voor iedere organisatie verstandig een FG aan te stellen. Een FG neemt u namelijk veel werk uit handen; zorgt voor structurele assessments en rapportages, is het aanspreekpunt voor AVG-kwesties én is de schakel met de Autoriteit Persoonsgegevens. Maar het belangrijkste voordeel is dat u richting uw klanten het signaal geeft dat u hun privacy hoog in het vaandel heeft staan.

Ik vraag overal toestemming voor, dus daarmee ben ik safe
Met alleen toestemming vragen voldoet u nog niet aan alle AVG-verplichtingen. Daarnaast is bewustwording bij werknemers van groot belang. Zij werken tenslotte met de gegevens. In de inrichting van uw processen kunt u hier veel ondervangen. Vanuit de wet wordt het zogenaamde Privacy By Design dan ook aangeraden. Hiermee kunt u bij de implementatie rekening houden.

Het uitvoeren van DPIA's geldt niet voor mijn organisatie
Een DPIA (Data Protection Impact Assessment of Gegevensbeschermingseffectbeoordeling) is verplicht onder bepaalde voorwaarden. Niet altijd dus. Een FG kan u advies geven of het voor uw bedrijf noodzakelijk is.

Ik ben niet verantwoordelijk voor data die ik van iemand anders krijg
U mag volgens de wet alleen maar samenwerken met partijen die voldoen aan de AVG-wetgeving. Hierbij geldt een ketenverantwoordelijkheid. Verwerkt uw bedrijf data van andere partijen? Dan moet u ook voldoen aan de wetgeving en dus compliant zijn.

Ik stel gewoon iemand uit mijn organisatie aan als FG
Als u een werknemer aanstelt als functionaris voor de gegevensbescherming, moet u er rekening mee houden dat deze persoon onafhankelijk is en blijft. Deze persoon mag dus niet zijn eigen werk beoordelen. Daarnaast krijgt de FG dezelfde ontslagbescherming als leden van de ondernemingsraad. De FG krijgt dus een aparte positie in uw organisatie.

De FG is verantwoordelijk voor alles rondom privacy
Dit is niet helemaal waar. De AVG gaat over de verwerking van persoonsgegevens. Het gaat dus niet om àlles rondom privacy. De FG verzorgt assessments, rapportages en geeft adviezen over de inrichting van de processen en de verwerking van gegevens. Maar hij is raadgever. Uw bedrijf blijft dus altijd verantwoordelijk en aansprakelijk voor hoe gegevens verwerkt worden.

Met persoonsgegevens worden alleen de NAW-gegevens bedoeld
Als er gesproken wordt over persoonsgegevens, dan gaat het om alle informatie die kunnen herleiden naar een persoon. Naast de NAW-gegevens gaat het dus ook om gegevens die in de context terug te leiden zijn naar een persoon.

Een register van verwerkingen hoef ik niet bij te houden
Niet ieder bedrijf hoeft inderdaad een register van verwerkingen bij te houden. Maar het kan wel heel gemakkelijk zijn als de Autoriteit Persoonsgegevens of klanten om inzage vragen. Dat scheelt u veel werk én u laat zien dat u de AVG zeer serieus neemt.

5. Een voorbeeld

We hebben dit voorbeeld geschreven om uit te leggen waar u als bedrijf mee te maken kunt krijgen. Het gaat over een fictief bouwbedrijf, maar het kan ook uw bedrijf overkomen.

Even voorstellen

Joris is eigenaar van bouwbedrijf Vastgoed. Het bedrijf heeft 10 werknemers in dienst en een klantenbestand met 2.000 klanten. De persoonsgegevens van de medewerkers en klanten heeft het bouwbedrijf in een computersysteem opgeslagen. Denk hierbij aan naam- en adresgegevens, e-mailadressen en bankrekeningnummers.

Bouwbedrijf Vastgoed heeft de afgelopen maanden veel tijd besteed aan de AVG. Hiervoor hebben ze als basis het stappenplan van de Autoriteit Persoonsgegevens gevolgd. Zo zijn er instructies 'hoe om te gaan met persoonsgegevens' voor medewerkers gemaakt, is in kaart gebracht welke gegevens van klanten voor welke doelen worden gebruikt en is de naast een goede firewall de back-upprocedure up to date. Het bedrijf is 'AVG-proof'! Goed geregeld dus.

De situatie

Een medewerker heeft een e-mail ontvangen met het verzoek iets via een bepaalde link te bevestigen. Dit blijkt een valse e-mail te zijn geweest. Want nadat op de link geklikt is, is het computersysteem gehackt. Alle bestanden in het systeem zijn niet meer te openen. Joris ontvangt een e-mail van de hacker: 'Uw systeem is gehackt. Betaal 2 bitcoins (ongeveer € 20.000,-) en u heeft weer toegang tot uw gegevens. Betaalt u niet, dan worden deze gegevens op internet geplaatst en zijn dan voor iedereen inzichtelijk.'

Joris heeft nu een paar problemen. Zijn systeem zit 'op slot' en daarmee ligt zijn bedrijf zo goed als administratief plat. Joris heeft gelezen dat hij nu in actie moet komen. Maar wat precies? Wie moet hij inschakelen? Wie moet hij informeren? Moet hij het losgeld betalen? Dat is voor hem even zoeken.

Wat moet Joris doen?

Welke acties moet Joris nu ondernemen?

1. Melden bij Autoriteit Persoonsgegevens

Joris moet datalekken die ernstige nadelige gevolgen hebben voor bescherming van persoonsgegevens direct melden bij de Autoriteit Persoonsgegevens. Dit moet hij binnen 72 uur doen.

Het melden van het datalek bij de Autoriteit Persoonsgegevens alleen is niet genoeg. Joris moet nog meer acties ondernemen.

2. Communiceren

Het is essentieel (en verplicht) dat Joris communiceert over dit datalek. Maar naar welke partijen?

- Naar klanten. Alle klanten moeten op de hoogte worden gebracht. Het is hierbij belangrijk dat een jurist die gespecialiseerd is op dit gebied Joris helpt met het opstellen van de boodschap.
- Naar werknemers. Voor werknemers geldt hetzelfde als voor klanten. Ook zijn werknemers moeten op de hoogte gesteld worden. De jurist kan ook hierbij helpen.

3. Inschakelen van een pr-bureau
Joris moet nadenken of hij het risico van reputatieschade loopt. Als in het nieuws komt dat zijn bedrijf gehackt is en klantgegevens in handen van derden zijn, dan kan dit ernstige gevolgen hebben voor de reputatie en misschien wel het voortbestaan van zijn bedrijf. Een pr-bureau kan hem op dat moment helpen met een goed plan van aanpak.

4. Forensisch onderzoek
Het computersysteem moet worden onderzocht op besmetting door deze hack. Joris weet namelijk niet of en tot welke gegevens de hackers toegang hebben. Om dat goed en succesvol te doen moet Joris een op dit terrein gespecialiseerd bedrijf inschakelen.

5. Keuze maken betalen losgeld
In de e-mail van de hacker staat dat Joris moet betalen om de data weer terug te krijgen. Het betalen van het losgeld is voor het bedrijf geen garantie dat de gegevens weer beschikbaar zijn. Maar ook geen garantie dat de hacker niet nog een keer toeslaat. Meestal is het dus de beste afweging om het losgeld niet te betalen.

6. Mogelijke aansprakelijkheid melden bij verzekeringsmaatschappij
Op het moment dat klanten te maken krijgen met kosten, bestaat het risico dat ze bouwbedrijf Vastgoed aansprakelijk gaan stellen. Joris neemt daarom contact op met zijn verzekeringsmaatschappij om te kijken of dit risico gedekt is bij zijn aansprakelijkheidsverzekering voor bedrijven. Helaas is dit niet het geval, want er is geen sprake van schade aan goederen of lichamelijk letsel.

7. Werkzaamheden inzichtelijk maken
Tijdens het onderzoek moet Joris misschien zijn bedrijf of een deel daarvan sluiten. Waarschijnlijk gaan de bouwwerkzaamheden gewoon door. Daarom moet Joris een inschatting maken welke werkzaamheden hij voorlopig niet meer kan uitvoeren. Stilstand van zijn bedrijf betekent natuurlijk extra kosten.

Conclusie: er komt in een hele korte tijd heel veel op Joris af. Dit kost Joris veel tijd en geld. Het is voor ieder bedrijf verstandig om dit traject in kaart te brengen. Want als een datalek plaatsvindt moeten er meteen een aantal belangrijke acties worden ondernomen.

Joris weet dat hij waarschijnlijk veel kosten moet maken. Hoe hoog deze kosten zijn, of het kosten van zijn eigen bedrijf zijn of bijvoorbeeld kosten die klanten moeten maken, dat is nog niet direct duidelijk. Maar dat deze schade niet verzekerd is op zijn bedrijfsaansprakelijkheidsverzekering is wel een feit.

Wat had Joris kunnen doen?

In bovenstaande situatie moest Joris zelf contact opnemen met verschillende bedrijven die hem bij een datalek kunnen helpen. De jurist, een forensisch onderzoekbedrijf en een pr-bureau. Misschien had Joris al weleens geregeld dat deze bedrijven stand-by staan voor het geval dat hij een datalek krijgt. Maar een optimale situatie is dit niet. Want Joris weet natuurlijk nooit wanneer zo'n incident plaatsvindt en hoeveel tijd het hem gaat kosten.

Joris had ook kunnen overwegen om het risico van datalekken te verzekeren. Dat kan met een data- en cyberrisicoverzekering. Deze verzekering biedt naast vergoeding van kosten ook praktische ondersteuning. Wat had Joris dan moeten doen?

Datalek melden via het noodnummer van de verzekeringsmaatschappij

Met één telefoontje naar de verzekeringsmaatschappij wordt alles in gang gezet:

- Het opstellen van een plan van aanpak.
- De forensische dienst wordt ingeschakeld. Zodat meteen onderzoek kan worden gedaan naar de oorzaak van het lek, maar ook naar het verwijderen van de schadelijke software.
- De jurist wordt ingeschakeld om communicatie naar gedupeerden op te stellen en te onderzoeken welke andere juridische stappen genomen moeten worden.
- Onderzoek of overleg met een pr-bureau om te bepalen of er sprake is van reputatieschade. En welke maatregelen genomen moeten worden.
- Behandelen van eventuele aansprakelijkheden. Zoals aangegeven biedt de aansprakelijkheidsverzekering voor bedrijven geen dekking. Een data- en cyberrisicoverzekering biedt dat wel. Aansprakelijkheidsstellingen worden dan ook in behandeling genomen.
- Eventueel betalen van bestuurlijke boetes als blijkt dat Joris volgens de Autoriteit Persoonsgegevens niet correct heeft gehandeld.

Dit was een fictief voorbeeld van bouwbedrijf Vastgoed. Maar het kan u ook overkomen. We hopen dat u nu een beter beeld heeft van wat een datalek voor uw bedrijf kan betekenen. Al is ieder bedrijf en situatie natuurlijk anders.

Zicht risico- en verzekeringsadviseurs

Over Zicht

Wij helpen u bij het maken van bewuste keuzes over financiële risico's. Bijvoorbeeld door samen goed vooruit te kijken. En door uw wensen en situatie in kaart te brengen. Maar ook door na te denken over verschillende oplossingen.

Dit doen we met persoonlijk advies en financiële producten die aansluiten bij de fase van uw (zakelijk) leven. Daardoor kunt u zich richten op de dingen waar het in uw leven écht om draait. **Dat is gelukkig geregeld!**

Zicht heeft meer dan 100 jaar ervaring met onafhankelijke advisering van bedrijven en particulieren. Vandaag de dag zijn we één van de toonaangevende adviesbedrijven van Nederland en onderdeel van NN Group. Vanuit vestigingen door heel Nederland adviseren onze 500 deskundige medewerkers u graag.

WWW.ZICHTADVISEURS.NL

gelukkig geregeld!

Z.AVG.WP.0318