Stappenplan Implementatie AVG

Algemene Verordering Gegevensbescherming:

Met deze gids helpen we je op weg om je organisatie aan de AVG te laten voldoen.

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

In deze whitepaper

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming van kracht. Het doel van de AVG, zoals deze kortweg wordt genoemd is het beschermen van natuurlijke personen in verband met de verwerking van hun gegevens. Gevolg van de wetgeving is dat organisaties die persoonsgegevens verwerken en/of opslaan zich aan extra privacy-richtlijnen dienen te houden. Dat betekent dat organisaties meer verplichtingen hebben bij het verwerken van persoonsgegevens. Organisaties die niet aan deze verplichtingen voldoen riskeren hoge boetes.

Ben je benieuwd naar hoe je de zaken in je organisatie zo kunt regelen zodat je voldoet aan de privacywetgeving?
Lees dan snel verder.

Inhoudsopgave

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

De Algemene Verordening Gegevensbescherming per 25 mei 2018

Vanaf 25 mei 2018 geldt in de hele Europese Unie dezelfde privacywetgeving. In Nederland kennen we die wetgeving als Algemene Verordening Gegevensbescherming (AVG). De AVG is ook wel bekend onder Engelse naam: General Data Protection Regulation (GDPR). Met de komst van de AVG-wet is de Wet bescherming persoonsgegevens (Wbp) komen te vervallen.
De AVG-wet is van toepassing op iedere organisatie die persoonsgegevens verwerkt en in de Europese Unie actief is.

Wat is de Algemene Verordering Gegevensbescherming?

Het doel van de Algemene Verordening Gegevensbescherming is het beschermen van natuurlijke personen in verband met de verwerking van hun gegevens. Dankzij de AVG krijg je als persoon dus meer recht en inzage bij de verwerking van persoonsgegevens. De kans dat je persoonsgegevens op straat komen te liggen vanwege een datalek is met de komst van de AVG aanzienlijk verkleind.

Zijn er ook voordelen aan de AVG voor mijn organisatie?

De Algemene Verordening Gegevensbescherming kent vele verplichtingen, maar levert organisaties die operationeel zijn in de Europese Unie ook voordelen op. Een voordeel is dat er in de hele EU nog maar één wet geldt in plaats van tientallen verschillende nationale wetten. Hierdoor heb je als organisatie meer rechtszekerheid, minder administratieve kosten en de garantie dat het speelveld voor iedereen die zaken doet in de EU gelijk is. Een ander voordeel is dat de nieuwe privacywet veel meer is toegespitst op de digitaliserende samenleving.

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

1. De impact van de nieuwe privacywetgeving op je organisatie

Door de komst van de AVG hebben organisaties meer verplichtingen bij het verwerken van persoonsgegevens. Organisaties dienen middels documentatie aan te tonen dat ze de juiste organisatorische en technische maatregelen hebben genomen om aan de wetgeving te voldoen. Dit betekent dat ze met een aantal zaken rekening moeten houden, zoals:

- Het verkrijgen van geldige toestemming van mensen om hun persoonsgegevens te mogen verwerken;
- Bewijzen dat er geldige toestemming is verkregen;
- Ervoor zorgen dat het voor personen net zo makkelijk is om hun toestemming in te trekken als dat deze gegeven is;
- Indien dit voor een organisatie aan de orde is, dan dient er een Data Protection Impact Assessment (DPIA) te worden uitgevoerd.
- Eventueel, het aanstellen van een Functionaris Gegevensbescherming (FG).

2. Stap 1: De privacyverklaring

Met de komst van de AVG kan vrijwel geen enkel bedrijf er meer omheen; de privacyverklaring. Wanneer je via je website persoonsgegevens verzamelt en die vervolgens verwerkt, dan ben je verplicht om een privacyverklaring op te stellen. Een dergelijke verklaring is een gedragscode waarin staat beschreven wat er met de gegevens van personen die verzameld zijn via de website gaat gebeuren. Het uitgangspunt van de AVG is transparantie. In de privacywet van 2018 zijn de regels met betrekking tot de privacyverklaring aangescherpt en daarom zullen veel bedrijven de privacyverklaring die was opgesteld voor de Wet bescherming persoonsgegevens (Wbp) moeten herzien om opnieuw aan de regels te kunnen voldoen.

Zorg dat je privacyverklaring op orde is

Door het opstellen van een privacyverklaring laat je als bedrijf zien dat je voldoet aan de eisen van de Algemene Verordening Gegevensbescherming. Hierdoor weet een persoon dat zijn gegevens in veilige handen zijn bij jou en wat jij met zijn of haar gegevens gaat doen. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de AVG en kan sancties opleggen bij overtreding van de wet. Dat kan bijvoorbeeld zo zijn wanneer je als organisatie niet binnen 72 uur een datalek bij de Autoriteit Persoonsgegevens meldt. Het is dus van belang dat je privacyverklaring op orde is. Het onjuist informeren van personen omtrent de verwerking van de persoonsgegevens kan leiden tot boetes die kunnen oplopen tot 20 miljoen euro of 4% van de wereldwijde omzet. Een doemscenario waar geen enkele ondernemer natuurlijk op zit te wachten.

Deze 8 punten mag je niet missen in jouw privacyverklaring

Wanneer je aan de slag gaat met je privacyverklaring, zorg er dan in ieder geval voor dat je de volgende acht punten daarin opneemt;

1. De identiteit en de contactgegevens van degene die verantwoordelijk is voor de opslag van de data.

2. De doelen van de gegevensverzameling (bijvoorbeeld e-mailadressen voor het versturen van e-mails aan personen met informatie over producten en diensten, aanbiedingen, acties, reviews en klanttevredenheidsonderzoeken) en de genomen veiligheidsmaatregelen.

3. De bewaartermijn van de gegevens.

4. De rechten van de betrokken personen. Zo hebben personen recht op inzage en correctie, evenals recht op verwijdering van de persoonsgegevens.

5. Belanghebbenden hebben het recht een klacht in te dienen bij een toezichthouder, zoals de Autoriteit Persoonsgegevens (AP). Dit dient duidelijk vermeld te zijn in de privacyverklaring.

6. De ontvangers van de gegevens en de tussenpartijen die inzage krijgen in de persoonsgegevens dienen te worden vermeld.

7. Indien profiling (het maken van profielen op basis van verkregen gegevens) van toepassing is voor je bedrijf, dient dit apart vermeld te worden.

8. Verstrekking van gegevens aan derden, zoals andere landen. Indien de servers van je bedrijf in een ander land staan, dan is het zaak dat je dit vermeldt. Geef hierbij aan of het land adequaat is verklaard.

Wat staat er precies in een privacyverklaring?

De belangrijkste regel binnen de AVG is dat je transparant bent over de verwerking van de persoonsgegevens. Je moet dus uitleggen waarvoor je bedrijf de gegevens opvraagt of vervangt en wat je organisatie met die gegevens doet. Binnen de AVG wordt dit de ‘doeleinden’ van gegevensverzameling genoemd. Het is de bedoeling dat deze doeleinden duidelijk gespecificeerd worden en ook duidelijk worden omschreven in de privacyverlkaring.

Volgens de nieuwe privacywet zijn er ook gegevens die je niet mag verwerken/opslaan. Dit worden de bijzondere persoonsgegevens genoemd. De volgende gegevens mag je nooit verwerken en/of opslaan in je database, tenzij hier een uitzondering voor is gemaakt in de wet:

- Ras
- Politieke voorkeur
- Gezondheid
- Gegevens over iemands seksueel leven
- Lidmaatschap vakbond
- Strafrechtelijk verleden

Ook het Burgerservicenummer (BSN) valt onder de bijzondere persoonsgegevens, omdat het een uniek en herleidbaar nummer is.

3. Stap 2: Bewaartermijn persoonsgegevens

De Algemene Verordening Gegevensbescherming verplicht organisaties om maatregelen te nemen waarmee de veiligheid van persoonsgegevens wordt geborgd. Met de komst van de AVG krijgen personen meer mogelijkheden om voor zichzelf op te komen bij het verwerken van hun gegevens. Maar wat zijn eigenlijk de richtlijnen omtrent de bewaartermijn van persoonsgegevens? Hoelang mag je als organisatie gegevens bewaren?

Het antwoord op de vraag hoelang de bewaartermijn persoonsgegevens in de AVG-wet is, is vrij simpel: de AVG geeft geen concrete bewaartermijn voor persoonsgegevens aan. In de wet wordt wel gesproken over opslagbeperking. Dat houdt in dat persoonsgegevens zolang bewaard mogen worden als dat nodig is voor het doel waarvoor ze verzameld zijn. Daarop zijn een aantal uitzonderingen:

- Wanneer gegevens geanonimiseerd worden, dan is het onder bepaalde voorwaarden wel mogelijk om ze langer te bewaren.
- Opslag mag wanneer sprake is van archivering voor algemeen belang, wetenschappelijk onderzoek of statistische/ historische doeleinden.
- Persoonsgegevens bewaren mag als dit door wetgeving wordt voorgeschreven.
  De Belastingwet schrijft bijvoorbeeld een bewaartermijn van 7 jaar voor.

Met de komst van de privacywet in 2018 hebben personen veel meer rechten. Zo is er het recht op vergetelheid waarbij personen aan organisaties mogen vragen hun persoonsgegevens te laten verwijderen. Ook is er het recht op dataportabiliteit. Dat houdt in dat mensen (onder bepaalde voorwaarden) het recht hebben om hun persoonsgegevens vanuit een organisatie in een standaardformaat te ontvangen.

Bewaartermijn AVG afhankelijk van procesdoeleinden

De privacywetgeving schrijft voor dat organisaties die persoonsgegevens verwerken dienen vast te leggen hoelang zij de gegevens bewaren en voor welke doeleinden. Er is dus geen eenduidige bewaartermijn, maar bij ieder proces moet worden bekeken wat de kortst mogelijke tijd is voor de opslag van de gegevens. Wanneer kunnen gegevens vernietigd worden zonder dat het ten koste gaat van het proces? Ook dienen organisaties gegevens actueel te houden gedurende de bewaartermijn en moeten deze indien mogelijk geanonimiseerd worden.

Organisaties moeten steeds de belangen afwegen tussen het doel waarvoor de gegevens worden verwerkt en de mogelijke gevolgen voor de betrokkene.

Stel je als organisatie de volgende vragen om een onderbouwde bewaartermijn te kunnen bepalen:

- Hoelang is de opslag van gegevens daadwerkelijk nodig?
- Welke gegevens zijn er nodig?
- Kunnen er passende organisatorische en technische methodes worden toegepast om de gegevens veilig op te slaan?
- Wat zijn de gevolgen van de betrokkenen als er een datalek ontsstaat?
- Wat is de impact op de persoonlijke levenssfeer van de betrokkene als de data gelekt wordt?

4. Stap 3: De verwerkersovereenkomst

Wanneer je als organisatie de verwerking van persoonsgegevens uitbesteedt aan een externe partij dan is het vanuit de privacywetgeving verplicht om afspraken te maken over de verwerking van de gegevens. Deze afspraken moeten schriftelijk worden vastgelegd. Het document waarin de afspraken staan beschreven wordt een ‘verwerkersovereenkomst’ genoemd.

Wanneer dien je een verwerkersovereenkomst op te stellen?

De AVG schrijft voor dat er een verwerkersovereenkomst moet zijn als:

- Jouw organisatie persoonsgegevens voor iemand verwerkt
- Je persoonsgegevens aan een derde ter beschikking stelt (subverwerkersovereenkomst)

Een verwerkersovereenkomst is niet altijd noodzakelijk een apart document. Het kan ook zo zijn dat de afspraken tussen partijen vastgelegd worden in een hoofdovereenkomst, algemene voorwaarden of een Service Level Agreement. Hoe dan ook, het is cruciaal om onder de AVG een verwerkersovereenkomst te hebben.

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Wie is de verwerkingsverantwoordelijke en wie is de verwerker?

In een verwerkersovereenkomst staat beschreven wie verantwoordelijk is bij de verwerking van persoonsgegevens als daarvoor een ander bedrijf wordt ingeschakeld. In een dergelijke overeenkomst wordt gesproken over een verantwoordelijke en een verwerker.

De verwerker is degene die in opdracht van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Een voorbeeld is een bedrijf dat persoonsgegevens verzamelt ten behoeve van de salarisadministratie. Dit is de verantwoordelijke. Wanneer de gegevens worden verwerkt door een salarisadministratiekantoor dan is dat de verwerker.

De verwerkings-verantwoordelijke is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Wat staat er in een verwerkersovereenkomst AVG?

In een verwerkersovereenkomst dient te worden opgenomen:

- Wat het doel van de verwerking is
- Wat de manier/methode van verwerking is (met welke middelen)
- De locatie van de data
- Geheimhouding
- Afspraken over eventuele onderaannemers/derden
- Beveiligingsmaatregelen
- De duur van de verwerking
- Afspraken over audits
- Afspraken over aansprakelijkheid

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Data mag enkel worden opgeslagen en verwerkt voor de doeleinden die zijn opgenomen in de overeenkomst. Zodra het doel bereikt is en de overeenkomst is afgelopen, wat gebeurt er dan met de gegevens? Wie vernietigt ze of worden deze teruggestuurd? Het is van belang om dat in de verwerkersovereenkomst op te nemen. Daarnaast is het belangrijk dat partijen met elkaar in een overeenkomst vastleggen hoe er wordt omgegaan met datalekken. Wie meldt de datalekken en wie vergoedt de eventuele schade?

Het verschil tussen een verwerkersovereenkomst en een bewerkersovereenkomst

De verwerkersovereenkomst zoals deze in de nieuwe privacywet staat beschreven is eigenlijk de bewerkersovereenkomst zoals die stond omschreven in de 'oude' Wet bescherming persoonsgegevens (Wbp). De eisen in de AVG zijn strikter dan in de Wbp. In de AVG zijn bijvoorbeeld nieuwe eisen opgesteld m.b.t. het inschakelen van subverwerkers (onderleveranciers): Er dient expliciet toestemming gegeven worden voor het inschakelen van subverwerkers. Waar in de Wbp sprake was van een bewerker heet dat nu een verwerker.

Het is zaak dat je als organisatie nagaat van welke verwerkers je organisatie gebruik maakt, zodat je hiermee een verwerkersovereenkomst af kunt sluiten. Ook is het van belang om te bekijken of je zelf verwerker bent van gegevens en zo ja, met welke partij er dan een verwerkersovereenkomst afgesloten dient te worden.

5. Stap 4: Ben op de hoogte van de meldplicht datalekken

De meldplicht datalekken geldt sinds 1 januari 2016. Wanneer zich een datalek voordoet hebben bedrijven en overheden de plicht dit direct te melden bij de Autoriteit Persoonsgegevens (AP). In sommige gevallen dient ook een melding te worden gedaan bij de directbetrokkenen (de personen van wie de gelekte persoonsgegevens zijn).

Wat is een datalek?

Een datalek ontstaat wanneer persoonsgegevens bij een organisatie:

- toegankelijk worden,
- vernietigd worden,
- gewijzigd worden,
- of geheel vrijkomen

zonder dat hiervoor toestemming is gegeven door de eigenaar van de persoonsgegevens. Het onrechtmatig gebruik van iemands persoonsgegevens kan ernstige schade veroorzaken, zoals bijvoorbeeld imagoschade. Voorbeelden van een datalek zijn een gestolen laptop of een hack van je bedrijfsgegevens.

Melden van een datalek in je eigen organisatie

Wanneer je vermoedt dat er sprake is van een datalek binnen je organisatie, dan is het van belang om na te gaan of het lek leidt of kan leiden tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. De beleidsregels van de Autoriteit Persoonsgegevens kunnen je helpen om te bepalen of er sprake is van ernstige nadelige gevolgen. Indien je hebt vastgesteld dat het om een datalek gaat, dien je het datalek te melden bij het meldloket datalekken.

Vermoeden van een datalek bij een andere organisatie

Indien je het vermoeden hebt dat er sprake is van een datalek bij een andere organisatie kun je dit ook melden bij de Autoriteit Persoonsgegevens door middel van het sturen van een tip. Het is belangrijk dat je hierbij eerst contact opneemt met de betreffende organisatie om hen hiervan op de hoogte te stellen. Wel zo netjes natuurlijk! De Autoriteit Persoonsgegevens zal de tip onderzoeken en nagaan of het lek al gemeld is door de organisatie zelf. Zo niet, dan neemt de AP contact op met de betreffende organisatie.

AUTORITEIT
PERSOONSGEGEVENS

6. Stap 5: Heb je een functionaris gegevensbescherming nodig?

Met de komst van de Algemene Verordening Gegevensbescherming (AVG) komt ook de term Functionaris Gegevensbescherming (FG) om de hoek kijken. Een FG houdt binnen een organisatie toezicht op de toepassing en de naleving van de AVG. Niet iedere organisatie is echter verplicht om een Functionaris Gegevensbescherming aan te stellen.

Wanneer heb je een Functionaris Gegevensbescherming nodig?

Om aan de privacywet te voldoen is een aantal organisaties verplicht om een Functionaris Gegevensbescherming aan te stellen. De FG houdt intern toezicht op het naleven van de AVG-wet- en regelgeving en adviseert de organisatie hierover. Binnen de organisatie moet iedereen weten wie de FG is en hoe deze te bereiken is.

Artikel 37 van de AVG-wet schrijft voor dat een FG in drie situaties verplicht is:

- Bij overheden en publieke organisaties: deze zijn altijd verplicht een FG aan te stellen, ongeacht het type gegevens dat ze verwerken. Denk aan rijksoverheid, gemeente, provincie, maar ook zorg- en onderwijsinstellingen.
- Observatie: organisaties die vanuit de kernactiviteiten op grote schaal individuen volgen. Denk bijvoorbeeld aan profilering van mensen voor het maken van risico inschattingen en monitoring van iemands gezondheid via wearables.
- Bijzondere persoonsgegevens: een FG is verplicht als er op grote schaal bijzondere persoonsgegevens worden verwerkt en dit een kernactiviteit is. Denk aan gegevens over iemand zijn gezondheid, politieke opvattingen of strafrechtelijk verleden.

Het volstaat om slechts één FG aan te stellen wanneer een organisatie meerdere vestigingen heeft.

Houd er wel rekening mee dat een FG meer kennis en ondersteuning nodig heeft als er in een organisatie grote hoeveelheden gevoelige gegevens verwerkt worden.

Taken Functionaris Gegevensbescherming

Een Functionaris Gegevensbescherming dient een onafhankelijke positie binnen een organisatie te hebben en mag geen instructies krijgen over zijn FG taken.
Deze personen zijn uitgesloten om een FG functie te vervullen:

- Bestuursvoorzitter
- Operationeel directeur
- Financieel directeur
- Medisch directeur
- Hoofd van de marketingafdeling
- Hoofd van personeelszaken
- Hoofd van de ICT-afdeling

Om zijn werk goed te kunnen doen is het zaak dat de FG ondersteund wordt vanuit het management en voldoende tijd, scholing, budget, resources en faciliteiten tot zijn beschikking krijgt.

CertificeringsAdvies NEDERLAND advies, opleiding & outsourcing

De kennis en vaardigheden van een Functionaris Gegevensbescherming:

- Bovengemiddelde kennis van nationale en Europese privacy wet- en regelgeving voor gegevensbescherming;
- Begrip van de gegevensverwerkingen die de organisatie uitvoert;
- Begrip van IT en informatiebeveiliging;
- Kennis van de organisatie en sector waarin deze actief is;
- Vaardigheden om binnen organisatie een cultuur van gegevensbescherming te ontwikkelen.

Een Functionaris Gegevensbescherming is niet aansprakelijk bij overtredingen van de privacywet. De naleving van de privacywet is de verantwoordelijkheid van de organisatie.

Een vrijwillige FG en/of een externe FG

Je kunt er als organisatie ook voor kiezen om vrijwillig een Functionaris Gegevensbescherming aan te stellen. Dat kan bijvoorbeeld verstandig zijn voor organisaties die overheidstaken uitvoeren, zoals bijvoorbeeld een woningcorporatie. Uiteraard kun je er als organisatie ook voor kiezen om in plaats van een FG een werknemer aan te stellen of adviseur in te huren die zich met de privacywetgeving gaat bezighouden. De werkzaamheden van een Functionaris Gegevensbescherming mogen ook door een extern persoon worden uitgevoerd. Outsourcen van een FG bescherming heeft zo zijn voordelen. Zo is de onafhankelijkheid beter geborgd. Daarnaast heeft een externe FG ervaringen opgedaan bij meerdere bedrijven en daarnaast toegang tot een netwerk van FG's waardoor het werk sneller en efficiënter uitgevoerd kan worden.

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

7. Stap 6: Het uitvoeren van de DPIA

Data Protection Impact Assessment (DPIA)

Met de komst van de AVG kan het zo zijn dat je als organisatie verplicht bent om een zogenaamde Data Protection Impact Assessment (DPIA) uit te voeren. Door dit te doen kun je vooraf de privacyrisico's van gegevensverwerking in kaart brengen. Vervolgens kun je als organisatie maatregelen nemen om de risico's te verkleinen of zelfs uit te sluiten.

Voor wie is de DPIA verplicht?
Wanneer je als organisatie gegevens verwerkt waaraan een hoog privacyrisico zit, dan dien je een DPIA uit te voeren. Of jouw organisatie hiervoor in aanmerking komt, bepaal je zelf. Uiteraard zijn er wel richtlijnen opgesteld om te beoordelen of je gegevensverwerking een hoog privacyrisico loopt of niet. De richtlijnen zijn terug te vinden op de website van de Autoriteit Persoonsgegevens (AP).

5 tips om op een snelle en pragmatische wijze een DPIA op te stellen

1

Start op tijd

Het is aan te raden om zo snel mogelijk te starten met de uitvoering van een DPIA. Zelfs wanneer nog niet alle details over de gegevensverwerking in de organisatie bekend zijn. Door zo snel mogelijk te starten met de DPIA kunnen de privacyregels al in de ontwerpfase worden meegenomen. De DPIA is een doorlopend proces dat regelmatig gecontroleerd dient te worden op wijzigingen van de risico's. Indien dat het geval is dient de DPIA aangepast te worden. Als organisatie hoef je een DPIA niet zelf uit te voeren, maar draag je wel de verantwoording.

2

Betrek de Functionaris gegevensbescherming

Wanneer je als organisatie verplicht een Functionaris Gegevensbescherming aan hebt moeten stellen, dan moet deze altijd om advies gevraagd te worden bij de uitvoer van een DPIA. In het DPIA-rapport dient beschreven te worden welke adviezen wel en niet zijn verwerkt. Wanneer een advies niet verwerkt is, dan dient de reden daarvan duidelijk te worden beschreven.

3

Beschrijf de doeleinden

Beschrijf systematisch de doeleinden waarvoor je organisatie de verwerking van bepaalde gegevens uitvoert. Ook dien je het gerechtvaardigd belang hierin op te nemen.

4

Beoordeel de noodzaak van de verwerkingen

Neem de beoordeling van de noodzaak en proportionaliteit van de verwerkingen op in de DPIA. Dat wil zeggen dat je dient te beschrijven of het verwerken van persoonsgegevens op de manier zoals jouw organisatie dat doet noodzakelijk is. Dit wordt ook wel de grondslag van de verwerking genoemd. Vraag jezelf daarbij af of de mogelijke privacy schending in verhouding staat tot het doel waarvoor je gegevens verzamelt.

5

Beschrijf de preventiemaatregelen

Stel als bedrijf regels op om de veiligheidsrisico's tot een minimum te beperken. Zorg dat je daarbij de risico's in kaart brengt te daaraan de bijbehorende maatregelen koppelt om de risico's te voorkomen.

Van ISO 27001 naar Algemene Verordening Gegevensbescherming

Voor vrijwel iedere organisatie zijn informatie en kennis een belangrijk bezit. Het is dan ook van cruciaal belang dat je informatie goed wordt beveiligd. Enerzijds omdat je niet wilt dat je concurrent met je bezit aan de haal gaat, maar anderzijds ook omdat je niet wilt dat persoonsgegevens door een datalek op straat komen te liggen. Privacy en informatiebeveiliging gaan daarom vaak hand in hand. Een uitstekende manier om de veiligheid van kennis en informatie te borgen is door de implementatie van een ISO 27001 managementsysteem.

Het is alleen niet zo dat wanneer je ISO 27001 gecertificeerd bent, je dan ook voldoet aan de AVG. Het managementsysteem is echter wel een goed hulpmiddel. Wanneer je als organisatie de regels van de AVG borgt in een kwaliteitsmanagementsysteem op basis van ISO 27001, dan sla je twee vliegen in één klap. Je kiest immers voor een integrale benadering van alle informatie die in je organisatie aanwezig is. Het helpt je om invulling te geven aan zowel technologische als organisatorische maatregelen voor een passende bescherming van persoonsgegevens.

Wil je meer informatie over de mogelijkheden omtrent de AVG en het implementeren van een ISO 27001 managementsysteem in je organisatie? Neem dan gerust contact met ons op. Wij hanteren een aanpak waarbij we niet de norm, maar jouw organisatie als uitgangspunt nemen. Op pragmatische wijze analyseren wij processen en optimaliseren deze conform ISO 27001 richtlijnen. Zo behalen we samen met jou en je collega's het beste resultaat.

CERTIFICERINGSADVIES NEDERLAND

JOUW PARTNER IN CERTIFICEREN

Heb je vragen over de AVG of Informatiebeveiliging? Of wil je aan de slag met het stap voor stap dichten van de laatste gaten van de informatiebeveiliging van je organisatie? Neem dan contact op met CertificeringsAdvies Nederland.

Deze whitepaper is geschreven door CertificeringsAdvies Nederland. Als Partner In Certificeren helpen wij organisaties met advies, opleiding en outsourcing binnen de thema's Kwaliteit, Arbo en Veiligheid, Milieu en MVO, Informatiebeveiliging en Voedselveiligheid.

CertificeringsAdvies Nederland werkt onder andere voor: