Herziene editie

MKB accountant

Nieuwe privacywetgeving in 2018

Wat te doen als mkb-accountant?

NBA

De tekst van deze brochure is een samenvatting van het NEMACC-rapport "*Informatiebeveiliging & Privacybescherming, Een aanpak waarmee de MKB-accountant kan voldoen aan de verscherpte eisen van informatiebeveiliging en privacy-bescherming*", december 2017.

De brochure is tot stand gekomen met medewerking van NEMACC, het mkb-kenniscentrum waarin NBA en de Erasmus Universiteit Rotterdam hun expertise bundelen.

Status

Deze publicatie is samengesteld voor leden en derden. De publicatie heeft geen status in het kader van de beroepsuitoefening. Er kan worden verwezen naar publicaties die een dergelijke status wel hebben. Overal waar in deze publicatie 'hij' staat wordt 'hij/zij' bedoeld.

Inhoudsopgave


F5
F6
F7
F8
F9
Ü
Ä
N
J
Gr

1 | Waarom informatiebeveiliging/ privacybescherming?

Cybercrime vormt in de huidige tijd een toenemend risico. Ook voor de mkb-accountant kan dit serieuze gevolgen hebben; voor zijn bedrijfsvoering en voor zijn reputatie als professioneel dienstverlener. De vraag is niet of hij wordt gehackt, maar wanneer en of zijn organisatie dan in staat is de schade te voorkomen of te beperken.

Het risico op cybercrime geldt niet alleen voor de bescherming van de eigen bedrijfsgegevens, maar ook voor die van klanten. Deze klantgegevens kunnen economisch gezien een grote waarde vertegenwoordigen. Bescherming van klantgegevens is dan ook een essentiële voorwaarde voor de 'Licence to Operate' van een mkb-accountant.

Los van het toenemende risico van cybercrime stelt ook de nieuwe Europese privacywetgeving strengere eisen aan privacybescherming. De toezichthouder, de Autoriteit Persoonsgegevens (AP), heeft al aangekondigd dat rekening moet worden gehouden met strikt toezicht. Om mkb-accountants te helpen bij de invoering van deze nieuwe regels is deze brochure opgesteld. Ook kan de mkb-accountant de informatie uit deze brochure gebruiken bij zijn advisering aan mkb-ondernemers. Ook zij krijgen te maken met de nieuwe wet.

Deze brochure bevat informatie op hoofdlijnen. Het uitgebreide rapport '*Informatiebeveiliging & Privacybescherming*'[1] biedt mkb-accountants meer concrete handvatten die zij kunnen gebruiken bij het op niveau brengen van de eigen informatiebeveiliging en privacybescherming.

1.1 Nieuwe privacywet vanaf 25 mei 2018

Op 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dit betekent in de praktijk dat de AP overgaat tot handhaven. Personen die menen schade te hebben geleden als gevolg van schending van hun privacy, kunnen zich dan op de AVG beroepen. Tot 25 mei 2018 geldt in Nederland nog steeds de Wet bescherming persoonsgegevens (Wbp) uit 2001 en de Meldplicht datalekken, die 1 januari 2016 van kracht is geworden.

De AVG versterkt de positie van mensen van wie persoonsgegevens worden verwerkt (betrokkenen). Zij krijgen nieuwe privacyrechten en bestaande rechten worden sterker. De AVG stelt hoge eisen aan de beveiliging van persoonsgegevens. Van organisaties wordt verwacht dat zij kunnen aantonen dat de beveiliging effectief is. De AVG bepaalt verder dat verwerking van persoonsgegevens alleen mag worden uitbesteed aan een verwerker die afdoende garanties biedt voor de beveiliging ervan.

Dit betekent bijvoorbeeld dat klanten (opdrachtgevers) alleen zaken mogen doen met mkb-accountants die zo'n garantie kunnen afgeven. En op hun beurt mogen mkb-accountants alleen verwerkingen uitbesteden aan partijen die ook een dergelijke garantie kunnen afgeven. Bovendien moet de uitbesteding van de verwerking van persoonsgegevens zijn geregeld in een overeenkomst en verwerkers hebben de plicht het nakomen van de vastgelegde verplichtingen aan te tonen.

1 Een aanpak waarmee de mkb-accountant kan voldoen aan de verscherpte eisen van informatiebeveiliging en de nieuwe privacywet (AVG)", november 2017,

De nieuwe wetgeving geeft de AP de bevoegdheid hoge boetes op te leggen[2]. Een datalek kan grote gevolgen hebben, ook voor de reputatie of de waarde van een onderneming.

De omvang van uw organisatie is niet van belang voor de toepasselijkheid van de AVG. Bepalend is of een organisatie persoonsgegevens verwerkt. De wijze waarop een kantoor invulling geeft aan de wettelijke verplichtingen, kan wel per kantoor verschillen. Dit is onder meer afhankelijk van de omvang, de organisatie en de aard van de dienstverlening. Het is uiteindelijk aan de organisatie zelf welke keuzes worden gemaakt.

1.2 Welke risico's loopt een mkb-accountant?

Kenmerken van een mkb-kantoor

Om het risico van cybercrime en de impact van de nieuwe privacywetgeving in hun context te kunnen plaatsen, worden in deze paragraaf de specifieke kenmerken en risico's van mkb-kantoren behandeld.

Dienstverlening

Veel mkb-kantoren bieden diverse diensten aan en hierbij worden vaak veel bedrijfs- en persoonsgegevens gebruikt. Ook maken mkb-kantoren vaak gebruik van meerdere computerprogramma's, vaak in combinatie met mobiele apparatuur (laptop, tablet, smartphone). Een aantal van deze programma's wordt ook door hun klanten gebruikt.

Dienstverlening door mkb-kantoren

- administratieve dienstverlening (bijvoorbeeld het bijhouden van de bedrijfs- en personeelsadministratie en salarisverwerking);
- fiscale en juridische dienstverlening;
- advisering en het samenstellen en controleren van jaarrekeningen;
- ondersteuning bij pensioenen, overnames, fusies, bedrijfsopvolging, waardebepaling, financiering, estate planning, subsidies, etc.

De verschillende dienstverlening in combinatie met het gebruik van een grote hoeveelheid gegevens in een vaak complex IT-landschap, brengt risico's met zich mee. Hierdoor is een mkb-kantoor kwetsbaar voor verlies of misbruik van data, verstoring van de bedrijfsvoering en voor non-compliance met de privacywetgeving.

Kenmerken leidend tot een verhoogd risico op verlies of misbruik data en verstoring bedrijfsvoering

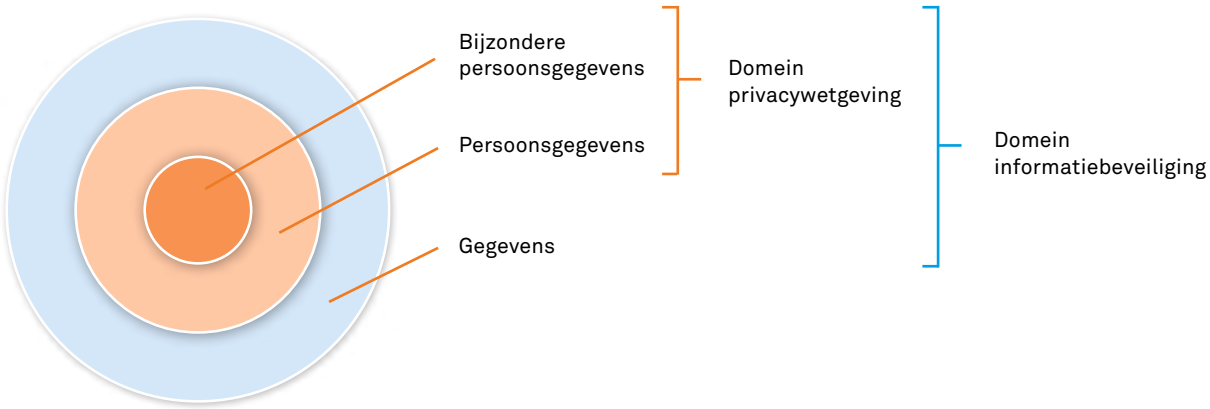
- beperkte kennis van IT en privacy en beperkte personele capaciteit;
- het gebruik van een veelheid aan data, waaronder (bijzondere) persoonsgegevens;
- communicatie met klanten via meerdere kanalen;
- gebruik van diensten van derde partijen, waardoor het risico bestaat dat onbevoegden toegang hebben tot data;
- gebruik van publieke diensten voor de uitwisseling, opslag van data (WeTransfer, Dropbox, Google Drive of OneDrive);
- gemengd gebruik van de applicaties, waardoor de accountant vaak geen zicht heeft op welke gegevens door de klant in zijn IT-omgeving worden geplaatst of verwerkt en waarvoor hij qua beveiliging medeverantwoordelijk wordt;
- afwezigheid van een geïntegreerde vorm van toegangsbeveiliging;
- gebruikmaken van mobiele apparatuur;
- een e-mailbox en website, die onvoldoende zijn beveiligd;
- een complexe IT-infrastructuur.

2 De AP kan organisaties sancties opleggen van maximaal 20 miljoen euro of 4% van de wereldwijde omzet, afhankelijk van welk bedrag het hoogste is.

Gebruik van persoonsgegevens

Een mkb-accountant maakt bij de uitvoering van zijn werkzaamheden veelvuldig gebruik van de gegevens van zijn klanten. Voorbeelden zijn: grootboektransacties, debiteuren- en crediteurengegevens, banktransacties, declaraties, personeels- en salarisgegevens, fiscale gegevens, maar ook claims en rechtszaken, notulen en verslagen, correspondentie, e-mailverkeer en berichten op sociale media.

De privacywetgeving richt zich juist op organisaties die persoonsgegevens verwerken, dus ook op mkb-accountants en hun klanten. Verwerken betekent hier: verzamelen, vastleggen, ordenen, structureren, raadplegen, verstrekken, bewerken, verwerken of vernietigen. Kortom “alle” activiteiten rond persoonsgegevens. Bij elke vorm van verwerking kan inbreuk op de privacy optreden.



Afbeelding 1: Welke gegevens vallen onder de privacywetgeving

Wat zijn persoonsgegevens?

Een persoonsgegeven is elk gegeven over een natuurlijk persoon (de betrokkene). Voorbeelden zijn:

- naam, adres, geboortedatum, titulatuur, geslacht, medische gegevens, overtredingen, veroordelingen;
- e-mailadres, telefoonnummers, inhoud van e-mails, surfgedrag, werkgever, functie, personeelsnummer, loopbaan, opleidingen, competenties;
- antwoorden, klachten, meningen, publicaties;
- gebruikersnamen, wachtwoorden, IP-adressen.

Anonieme gegevens

Gegevens zijn geen persoonsgegevens als deze zijn geanonimiseerd. Anoniem betekent dat maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen aan de hand van deze gegevens redelijkerwijs is uitgesloten.

Bijzondere persoonsgegevens

Een deel van de persoonsgegevens wordt gezien als bijzondere persoonsgegevens. Gebruik en verwerking hiervan mag alleen onder strikte voorwaarden. Voorbeelden van bijzondere gegevens zijn:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuiging;
- lidmaatschap van een vakbond;
- gezondheid;
- seksueel gedrag en seksuele gerichtheid.
- lichamelijke kenmerken (genetische of biometrische gegevens).

Persoonsgegevens van gevoelige aard

- Gegevens over de financiële of economische situatie van de betrokkene
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene
- Gebruikersnamen, wachtwoorden en andere inloggegevens
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude

Oorzaken verlies of misbruik data en verstoring bedrijfsvoering

'Bekende' oorzaken die leiden tot verlies of misbruik van gegevens zijn: het verlies van een gegevensdrager (laptop, USB-stick), de verzending van gegevens naar het verkeerde (e-mail)adres of de gevolgen van het 'meewerken' aan pishing mails. Uit gesprekken met accountantskantoren bleek dat accountants soms ook onverwacht en onbedoeld worden geconfronteerd met gegevens die niet door de eigen organisatie voor hun werkzaamheden worden gebruikt, maar bijvoorbeeld door hun klanten of adviseurs.

Zo bleek een klant medische informatie van medewerkers bij te houden in het salarissysteem dat door het accountantskantoor wordt gebruikt en dat online toegankelijk en beschikbaar is voor klanten. Dit zijn bijzondere persoonsgegevens die niet door de accountant of de klant mogen worden verwerkt. Tenzij hiervoor een wettelijke grondslag bestaat.

In een ander geval werd een accountantskantoor betrokken in een mailwisseling tussen zijn klant en juridische adviseurs over persoonlijke zaken. Hier ging het om fiscale aangelegenheden en juridische geschillen.

Waarom het soms mis gaat met de verwerking van persoonsgegevens?

- gebrek aan kennis en capaciteit;
- te ruime of niet actuele bevoegdheden (autorisaties);
- menselijk (afwijkend) gedrag;
- combinatie van zakelijk en privé;
- basisbeveiliging niet op orde (geen sterke wachtwoorden gebruikt, beveiligingssoftware onregelmatig geüpdatet, geen back-up);
- onvoldoende beveiligde IoT-apparatuur;
- complexe configuraties van hardwarecomponenten, software-oplossingen, en een diversiteit aan koppelingen.

Datalekken in 2016 (Bron: AP)

In 2016 heeft de AP 5.849 meldingen ontvangen. In het derde kwartaal van 2017 stond de teller al op 7.364. Op de volgende pagina staat een overzicht van type datalekken, belangrijkste gegevens die gelekt zijn en de belangrijkste sectoren waarin het gebeurt.

Type datalekken	%
Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger	46%
Apparaat, gegevensdrager e/o papier kwijtgeraakt of gestolen	14%
Brief of postpakket kwijtgeraakt of geopend retour ontvangen	10%
Hacking, malware e/o phishing	6%
Persoonsgegevens per ongeluk gepubliceerd	4%
Persoonsgegevens van verkeerde klant getoond in klantportaal	4%
Persoonsgegevens nog aanwezig op afgedankt apparaat	<1%
Persoonsgegevens bij oud papier gezet	<1%
Overige	14%
Belangrijkste sectoren	**%**
Gezondheid en welzijn	29%
Openbaar bestuur	20%
Financiële dienstverlening	20%
Belangrijkste gegevens	
Naam- en adresgegevens, geboortedatum, telefoon, BSN, financiële en gezondheidsgegevens	

2 | De belangrijkste verplichtingen van de AVG

2.1 Eisen aan en verantwoordelijkheden bij de verwerking van persoonsgegevens

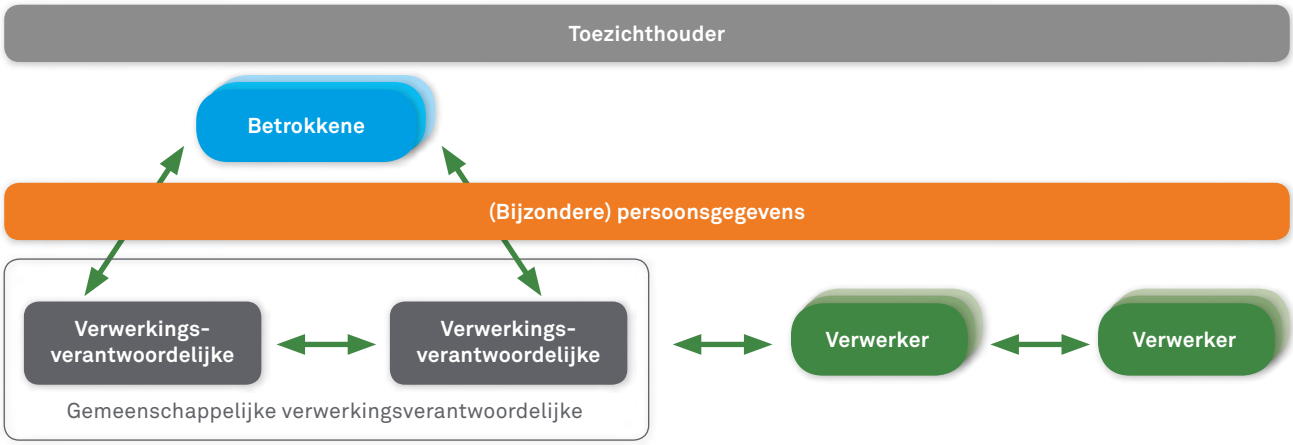
De AVG stelt zware eisen aan de verwerking van persoonsgegevens. Dit ter bescherming van natuurlijke personen (betrokkene). De toezichthouder AP ziet toe op de naleving.

Organisaties mogen niet zomaar persoonsgegevens verwerken dan wel verzamelen, hiervoor moet wel een gegronde reden (rechtmatige grondslag) zijn. De belangrijkste grondslagen om gegevens te mogen verwerken, zijn:

- toestemming van de betrokkene: door middel van een duidelijke actieve handeling; een schriftelijke, elektronische of mondelinge verklaring;
- uitvoering van een overeenkomst: waarbij de betrokkene partij is;
- voldoen aan een wettelijke verplichting; bijvoorbeeld het uitvoeren van een klantenonderzoek i.v.m. Wwft.

Verschillende rollen en verantwoordelijkheden in de keten

Voor de verwerking in de keten zijn verschillende partijen verantwoordelijk: de verwerkingsverantwoordelijke, de verwerker en de eventuele subverwerker. De verwerkingsverantwoordelijke is een natuurlijke persoon of rechtspersoon die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit kan de mkb-accountant zijn die als werkgever de wettelijk vereiste gegevens verzameld van zijn werknemers. De verwerker is de natuurlijke persoon of rechtspersoon die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Bijvoorbeeld het verwerken van salarissen en het bijhouden van administraties. De subverwerker is de natuurlijke persoon of rechtspersoon die in opdracht van de verwerker persoonsgegevens verwerkt.



Afbeelding 2: Betrokken partijen en de relatie tot elkaar

LET OP

Niet altijd is sprake van gemeenschappelijke verwerkingsverantwoordelijken indien zich binnen een relatie twee verwerkingsverantwoordelijken bevinden.

Gezamenlijk zijn zij verantwoordelijk voor het beschermen van de privacy en aansprakelijk voor mogelijke schade. Dit heeft mede tot gevolg dat alle partijen in de keten elkaar moeten bevestigen dat zij voldoen aan de wet.

2.2 Passende technische en organisatorische maatregelen

Organisaties moeten volgens de AVG passende technische en organisatorische maatregelen treffen om de persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Privacy by design en Privacy by default

Organisaties moeten bij het ontwerpen van producten en diensten ervoor zorgen dat persoonsgegevens goed worden beschermd (Privacy by design). Ook moeten ze maatregelen treffen om ervoor te zorgen dat alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel dat moet worden bereikt (Privacy by default). De AVG verwacht van organisaties dat zij hiermee bij de inrichting van hun processen en beveiliging rekening houden en een risicoanalyse uitvoeren met betrekking tot de verwerking. Denk aan verwerkingsrisico's, zoals de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot gegevens. De verwerkingsverantwoordelijke moet de naleving van de AVG aan kunnen tonen. Ook voor de mkb-accountant is deze bepaling zéér belangrijk ongeacht zijn rol. Ook in zijn rol als verwerker moet een mkb-accountant kunnen aantonen dat hij de wet naleeft, omdat klanten wettelijk verplicht zijn om schriftelijke garanties van de mkb-accountant te vragen.

2.3 Rechten van de betrokkene

De AVG versterkt de privacy-rechten van mensen. Zo heeft de betrokkene straks recht op:

- Transparante informatie en duidelijke communicatie over de persoonsgegevens die over hem/haar zijn verzameld en worden gebruikt;
- Inzage in zijn persoonsgegevens; welke, aan wie verstrekt, door wie verwerkt en onder welke voorwaarden;
- Rectificatie in het geval van onjuiste persoonsgegevens;
- Beperking van de verwerking, bijvoorbeeld in het geval van onrechtmatigheid, onjuiste gegevens of wanneer gegevens niet meer nodig zijn voor de verwerkingsdoeleinden;
- Vergetelheid; dit betekent dat de verwerkingsverantwoordelijke de persoonsgegevens (op verzoek) verwijdert;
- Overdraagbaarheid van gegevens; dat wil zeggen dat de verwerkingsverantwoordelijke deze op verzoek kan overdragen aan of delen met een andere partij. Sluit aan bij de invoering van de PDS2-regelgeving, waarbij bedrijven zonder bankvergunning toegang krijgen tot betaalgegevens van rekeninghouders;
- Bezwaar tegen gebruik van zijn persoonsgegevens, wanneer deze worden gebruikt voor alleen geautomatiseerde verwerking (profilering) waaraan voor hem rechtsgevolgen zijn verbonden. Denk aan personeelsselectie of het bepalen van iemands kredietwaardigheid. Of voor het gebruik van direct marketing;
- Kennisgeving aan een ontvanger als betrokkene vraagt om rectificatie, beperking of vergetelheid.

Een organisatie (kantoor) dient binnen een maand passend te reageren op een verzoek tot uitoefening van deze rechten door betrokkene.

LET OP

Een verzoek om verwijdering hoeft niet gehonoreerd te worden als er andere wettelijke gronden zijn (bijvoorbeeld bewaarplicht) voor de verwerking van de gegevens.

2.4 Register van verwerkingsactiviteiten

Organisaties met meer dan 250 medewerkers zijn verplicht een register van verwerkingen bij te houden. Een register van verwerkingen is niet verplicht voor organisaties met minder dan 250 medewerkers, tenzij het waarschijnlijk is dat:

- de verwerking een risico inhoudt voor de rechten van betrokkenen;
- de verwerking niet incidenteel is;
- of de verwerking bijzondere persoonsgegevens betreft. Je kunt hierbij denken aan grootschalige verwerking van salarissen waarbij ook bijzondere persoonsgegevens worden gebruikt, zoals loonbeslag.

De praktijk wijst uit dat iedere organisatie een aantal niet incidentele verwerkingen heeft. Deze moet u opnemen in het register. Denkt u bijvoorbeeld aan een salarisverwerking of debiteurenadministratie. Het register geeft inzicht in de verwerkingen waarvoor een verwerkingsverantwoordelijke of verwerker verantwoordelijk is en biedt de mogelijkheid om de naleving van de AVG aan te tonen. Naast de verplichting structurele verwerkingen in het register te plaatsen is dit een andere reden waarom het voor mkb-kantoren verstandig is een register van verwerkingsactiviteiten bij te houden.

Gegevens die moeten worden vastgelegd in het register zijn onder meer:

- de naam en contactgegevens van de verwerkingsverantwoordelijke/verwerker
- de verwerkingsdoeleinden,
- een beschrijving van de categorieën van betrokkenen, persoonsgegevens en ontvangers aan wie persoonsgegevens worden verstrekt,
- de bewaartermijn en de technische en organisatorische beveiligingsmaatregelen.

2.5 Het melden van een datalek

De AVG stelt strengere eisen aan de registratie van datalekken die zich in de organisatie hebben voorgedaan. Alle datalekken moeten worden gedocumenteerd, zodat de AP kan controleren of de organisatie aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht in de Wbp, die alleen betrekking heeft op de gemelde datalekken. Om invulling te kunnen geven aan de meldplicht van een datalek moeten verwerkingsverantwoordelijke en verwerker een aantal stappen zetten. Deze worden in het stappenplan hieronder toegelicht.

Stappenplan meldingsprocedure datalek

Stap 1: Is de AVG en daarmee de meldplicht datalekken van toepassing?

De organisatie moet vaststellen of de AVG van toepassing is en of er sprake is van verwerking van persoonsgegevens. De AVG is van toepassing als sprake is van geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen. De AVG is niet van toepassing op de verwerking van persoonsgegevens door een natuurlijk persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit.

Stap 2: Is sprake van een datalek of beveiligingsincident?

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan, waarbij persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet kan worden uitgesloten. Registratie van inbreuken op de privacy is verplicht.

Stap 3: Melden datalek bij de AP?

De organisatie die persoonsgegevens verwerkt, moet (systematische) inbreuken op de privacy signaleren. Dit betekent dus dat de organisatie moet beschikken over een vorm van detectie en monitoring om inbreuken tijdig te kunnen signaleren. Als een inbreuk heeft plaatsgevonden en er sprake is van (een aanzienlijke kans op) nadelige gevolgen voor betrokkene is een melding aan de AP noodzakelijk.

De verwerkingsverantwoordelijke meldt een datalek binnen 72 uur nadat hij hiervan kennis heeft genomen aan de AP, zonder onredelijke vertraging. Indien de melding niet binnen 72 uur plaatsvindt, moet ook de reden voor de vertraging worden opgeven. Voor mkb-kantoren is een melding doorgaans alleen noodzakelijk als er persoonsgegevens van gevoelige aard zijn gelekt. Een melding is niet nodig als het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Op de website van de AP is een meldingsformulier beschikbaar. Via dit webformulier kan een melding worden aangevuld of ingetrokken. De melding moet informatie bevatten over de aard en omvang van de inbreuk, de mogelijke gevolgen en de maatregelen die zijn genomen.

Als de verwerker een inbreuk constateert dan stelt hij de verwerkingsverantwoordelijke zo snel mogelijk op de hoogte.

De verwerkingsverantwoordelijke is verplicht alle inbreuken op persoonsgegevens te documenteren, met inbegrip van de feiten omtrent de inbreuk, de gevolgen daarvan en de genomen maatregelen. Dus ook de inbreuken die niet zijn gemeld.

Stap 4: Informeren betrokkene(n) over het datalek?

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk risicovol is voor de rechten en vrijheden van natuurlijke personen, dan brengt de verwerkingsverantwoordelijke de betrokkene direct op de hoogte van de inbreuk. Dit voorkomt ernstige schade bij betrokkenen als gevolg van het verlies, onrechtmatig gebruik of misbruik van hun persoonsgegevens.

Wanneer de verwerker constateert dat een door hem aan de verwerkingsverantwoordelijke gemeld datalek niet wordt gemeld bij de AP of aan betrokkenen, terwijl daar volgens hem wel aanleiding toe is, dan is het verstandig dat hij de verwerkingsverantwoordelijke hierover informeert en dit eventueel ook documenteert.

2.6 Data Protection Impact Assessment (DPIA)

Organisaties moeten verplicht een DPIA uitvoeren als een beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. Dat zou bijvoorbeeld het geval kunnen zijn bij een bijzondere verwerking of een verwerking waarbij nieuwe technologieën worden gebruikt. Een DPIA wordt toegepast om inzicht te krijgen in de risico's met betrekking tot de bescherming van persoonsgegevens. Deze bepaling geldt ook voor accountantskantoren en zou van toepassing kunnen zijn wanneer die vormen van data-analyse inzetten in de controle of voor klanten bij het analyseren of optimaliseren van hun processen of analyseren van data. In de praktijk worden dergelijke bewerkingen vaak door specialisten uitgevoerd. Meestal in hun eigen omgeving, die ook buiten de EU kan liggen. In dat geval moet het kantoor zorgdragen dat sprake is van passende beveiliging en dat de privacy-rechten van betrokkene worden gewaarborgd.

Organisaties hoeven niet voor elke gegevensverwerking een DPIA uit te voeren. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dat is in ieder geval zo als een organisatie:

- systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
- op grote schaal bijzondere persoonsgegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met camera-toezicht).

2.7 Functionaris voor gegevensbescherming (FG)

Niet alle organisaties zijn verplicht een FG aan te stellen. Een FG is verplicht voor overheidsorganisaties en wanneer een organisatie als kernactiviteit en op grote schaal bijzondere persoonsgegevens verwerkt of stelselmatige observaties van betrokkenen uitvoert. Met het zelf aanstellen of door met anderen gebruik te maken van een FG (FG as a service) kan een mkb-kantoor aantonen dat het beschikt over de nodige expertise op het terrein van de privacywet en -bescherming. Ook al is een FG (of een privacy officer) niet verplicht, dan kan het soms toch zinvol zijn er een te hebben. Bijvoorbeeld wanneer een betrokkene een klacht neerlegt bij de AP en de organisatie moet aantonen dat ze beschikt over de benodigde deskundigheid en voldoet aan de eisen van de AVG. Een FG of privacy officer kan de organisatie bovendien adviseren hoe om te gaan met verwerkingen, een DPIA of een inbreuk of datalek.

2.8 Verplichtingen: Verwerkingsverantwoordelijke of verwerker

Onderstaand overzicht bevat de taken en verplichtingen van verwerkingsverantwoordelijken (Vv) en verwerkers (v), voortvloeiend uit de AVG.

Taken en verplichtingen van verwerkingsverantwoordelijken en verwerkers	Vv	V
Bepaalt het doel en de middelen voor de verwerking van persoonsgegevens.	X	
Verwerkt persoonsgegevens in opdracht/ten behoeve van verwerkingsverantwoordelijke.		X
Zorgt voor passende technische en organisatorische maatregelen opdat de verwerking aan de eisen van de wet voldoet en moet dit kunnen aantonen.	X	X
Voert in voorkomende gevallen een DPIA uit.	X	X
Verwerkt gegevens van betrokkene op basis van een rechtmatige grondslag.	X	X
Vult de rechten van betrokkene(n) in.	X	
Is verantwoordelijk/aansprakelijk voor de gegevensverwerking die door of namens hem wordt uitgevoerd.	X	X
Maakt uitsluitend gebruik van de diensten van (sub)verwerkers, die afdoende garanties kunnen geven met betrekking tot een passende beveiliging.	X	X
Voert in opdracht van een verwerkingsverantwoordelijke alleen verwerkingen uit die zijn gebaseerd op een overeenkomst.		X
Houdt een register van verwerkingsactiviteiten bij. Voor nadere toelichting, zie [2.4].	X	X
Beschikt in voorkomende gevallen over een FG. Voor nadere toelichting, zie [2.7].	X	X
Meldt een datalek bij de AP.	X	
Meldt een datalek bij de verwerkingsverantwoordelijke.		X
Informeert in voorkomende gevallen de betrokkene(n) over een datalek.	X	
Houdt een register van inbreuken/datalekken bij.	X	X
Moet alle schade vergoeden die een betrokkene kan lijden ten gevolge van een verwerking die inbreuk heeft gemaakt op zijn rechten.	X	X

3 | Gevolgen voor de mkb-accountant?

3.1 Invulling IT en beveiliging op kantoorniveau

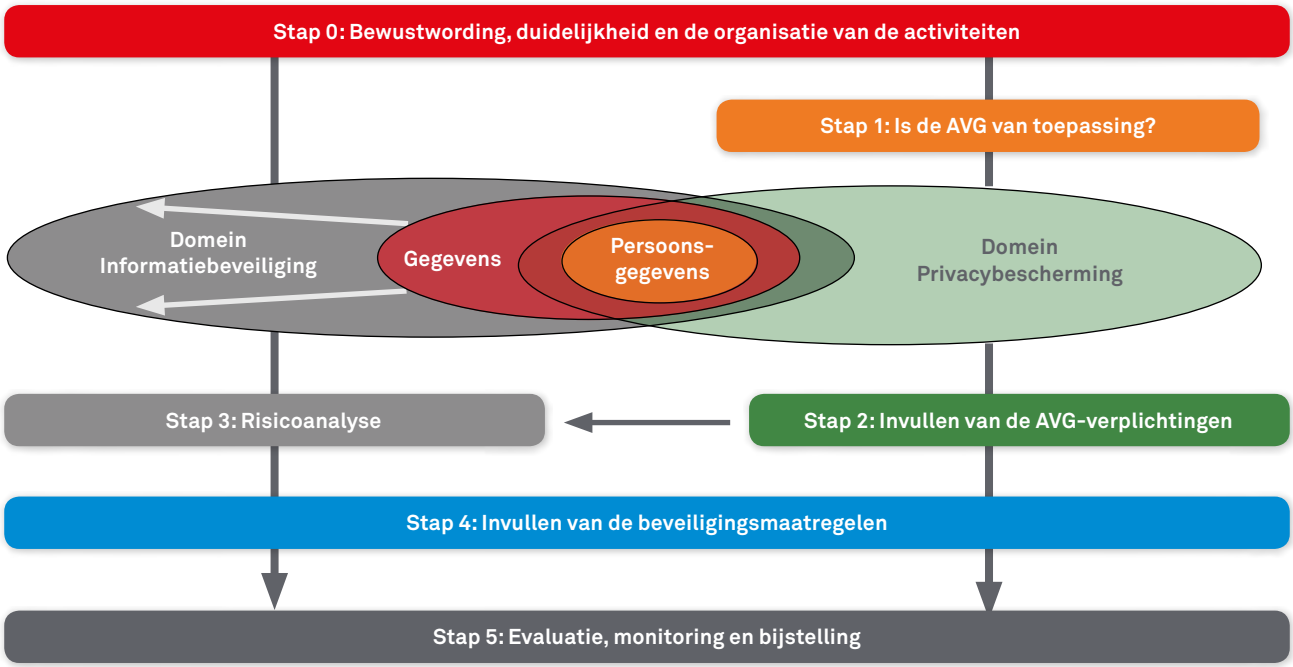
De omvang van uw organisatie is niet van belang voor de toepasselijkheid van de AVG. Bepalend is of een organisatie persoonsgegevens verwerkt. De wijze waarop een kantoor invulling geeft aan deze wettelijke verplichtingen, kan wel per kantoor verschillen. Dit is mede afhankelijk hoe een kantoor is georganiseerd.

Een mkb-accountant kan een zelfstandige zonder personeel (zzp'er), een eenmanspraktijk (accountant plus een aantal medewerkers) of een meermanspraktijk (meerdere accountants plus medewerkers) zijn. Een zzp'er heeft geen medewerkers waarmee moet worden overlegd, afspraken gemaakt of gedrag gemonitord. Een zzp'er en ook een eenmanspraktijk zullen vaak gebruikmaken van de diensten van derde partijen bij de invulling of ondersteuning van hun dienstverlening (serviceproviders voor de invulling van IT-ondersteuning). Grotere kantoren geven vaak zelf meer invulling aan hun processen en de toepassing van IT. In algemene zin kan worden gesteld, dat hoe meer een kantoor zelf invulling geeft aan IT en beveiliging, hoe meer wordt gevraagd van de organisatie zelf.

Het gebruikmaken van diensten van (gespecialiseerde) derde partijen kan de belasting voor het kantoor verlichten. Dit betekent dan wel dat afspraken moeten worden vastgelegd in overeenkomsten en de naleving moet worden gemonitord. In organisaties met medewerkers zullen aanpassingen in de informatiebeveiliging en het doorvoeren van maatregelen in het kader van de AVG om een meer projectmatige aanpak vragen. Het is uiteindelijk aan de verantwoordelijke(n) binnen de organisatie, welke keuzes worden gemaakt.

3.2 Stappenplan AVG NEMACC

Op basis van de AVG heeft de NBA een stappenplan laten ontwikkelen door NEMACC. Hiermee kunnen mkb-kantoren zich voorbereiden op de AVG. Het stappenplan houdt rekening met het verschil in omvang en organisatie van mkb-kantoren. Ook heeft de NBA op het besloten deel van de website een toolkit geplaatst. Hierin is onder meer een uitleg van het stappenplan van de Autoriteit Persoonsgegevens opgenomen.



Afbeelding 3: Stappenplan AVG

Stap 0: Bewustwording, beleid en organiseren activiteiten

Zorg voor bewustwording

Zorg dat u en uw medewerkers op de hoogte zijn van de implicaties van de privacywet en betrek medewerkers bij uw plannen en activiteiten met betrekking tot informatiebeveiliging en privacybescherming. Dit om verzekerd te zijn van hun actieve betrokkenheid en medewerking.

Beveiligings- en privacy-beleid

Formuleer als leiding van de organisatie een beveiligings- en privacy-beleid waarin is aangegeven aan welke eisen de organisatie moet voldoen en op welke wijze de organisatie daar invulling aan geeft. Geef ook aan wat van de medewerkers wordt verwacht.

Belangrijke uitgangspunten bij het formuleren van een beveiligings- en privacy-beleid zijn:

- *Behoud de regie*; dit betekent dat uw organisatie het initiatief neemt om afspraken te maken met partijen hoe om te gaan met gegevens.
- *Zorg voor beheerste flexibiliteit*; werk met gestandaardiseerde klantoplossingen met behoud van keuzevrijheden binnen aangegeven grenzen.
- *Voorkom complexiteit*; wat in de praktijk betekent dat uw organisatie m.b.t. de informatievoorziening kiest voor de beste oplossing voor het geheel in plaats van de beste deeloplossingen.
- *Hanteer het 'Need to know'-principe*; wees selectief bij het verlenen van bevoegdheden en toegang tot gegevens en processen.
- *Bewaar alleen gegevens die wettelijk nodig zijn*;
- *Focus op gedrag*; stimuleer en beloon actief, bewust, verantwoordelijk en alert gedrag.

Het beveiligings- en privacy-beleid en de keuzes die daarin worden gemaakt, komen onder meer tot uiting in een gedragscode en de te nemen maatregelen.

Organisatie

De activiteiten ten aanzien van de informatiebeveiliging en privacybescherming vragen doorgaans om een projectmatige aanpak, waarbij meerdere partijen betrokken zijn: IT en HR-specialisten, Juridische zaken, compliance officers, derden waarmee u zaken doet en natuurlijk uw klanten. Belangrijke voorwaarde is dat het projectteam over de benodigde middelen (financieel en personeel) beschikt om de noodzakelijke activiteiten uit te kunnen voeren.

Stap 1: Bepaal aan welke eisen u moet voldoen

Breng de verwerkingen van persoonsgegevens in kaart

De eerste en belangrijkste vraag die een accountant in het kader van de AVG moet beantwoorden is welke verwerkingen van persoonsgegevens in zijn kantoor plaatsvinden.

Om deze vraag te kunnen beantwoorden is inzicht nodig in de verwerkingen en de daarbij behorende persoonsgegevens, die onder verantwoordelijkheid van de accountant, al dan niet in opdracht van andere partijen (klanten) plaatsvinden. Ook moet de accountant nagaan of er een rechtmatige grondslag is voor de verwerking.

Ga na of uw organisatie een FG moet aanstellen of deze functie nodig heeft

De organisatie moet volgens de AVG nagaan of zij een FG moet aanstellen. Ook al is dat niet het geval, dan kan een mkb-kantoor toch overwegen een FG te benoemen of op andere wijze in deze functie te voorzien. Zie paragraaf 2.7.

Bepaal of u verwerkingsverantwoordelijke of verwerker bent

Een vraag die de mkb-accountant moet beantwoorden is of hij verwerkingsverantwoordelijke of verwerker is. De rol en context van zijn werkzaamheden bepalen welke maatregelen een accountant moet nemen met betrekking tot bepaalde verwerking(en) van persoonsgegevens.

Als accountant kunt u bij de uitvoering van uw dienstverlening *'verwerker'* of *'verwerkingsverantwoordelijke'* zijn. Als u als accountant het doel en/of de middelen bepaalt, bent u verwerkingsverantwoordelijke. Als uw klant dat doet dan bent u verwerker.

In het overleg met de AP is naar voren gekomen, dat de rol van de accountant als verwerkingsverantwoordelijke moet worden gezien in de context van zijn werkzaamheden. Dit betekent dat zijn verantwoordelijkheid bij de uitvoering van bepaalde werkzaamheden beperkt is tot de zogenaamde contextuele verantwoordelijkheid.

Naar de mening van de AP moet de accountant, in het geval hij zelfstandig werkzaamheden uitvoert waarbij diens onafhankelijkheid essentieel is, worden gezien als verwerkingsverantwoordelijke voor wat betreft:

- de verwerkingen die hij in het kader van zijn opdracht uitvoert met
  - de persoonsgegevens (A) die hij van zijn klant heeft ontvangen, of
  - zelfstandig (aanvullend) (B) heeft verzameld,
- de informatie die uit deze verwerking(en) voortvloeit in de vorm van opdrachtdocumentatie/controle-informatie.

In het geval dat zich bij de accountant een datalek voordoet met betrekking tot de persoonsgegevens die de accountant van de klant heeft ontvangen (A), meldt de accountant dit datalek bij de AP en informeert hij de klant. Accountant en klant stemmen af wie een eventuele melding doet aan betrokkene(n). Als het datalek gegevens van bijvoorbeeld de werknemer(s) van de klant betreft, ligt het in de rede dat de klant aan de betreffende werknemers meldt dat een datalek heeft plaatsgevonden bij de accountant. Het zou voor betrokkenen in deze context niet logisch zijn als de accountant hen hierover zou informeren in plaats van de klant.

Voor zover het de persoonsgegevens betreft die de accountant zelf heeft verzameld (B), meldt hij dit datalek als verwerkingsverantwoordelijke bij de AP en informeert indien noodzakelijk de betrokkenen. Wanneer dit voor betrokkenen niet logisch zou zijn kan ook hier de melding aan betrokkenen door de klant worden verricht.

Voert de accountant in opdracht van de klant louter uitvoerende werkzaamheden uit, zoals het verwerken van salarissen, het bijhouden van administraties, het opstellen van een fiscale aangifte of het invullen van formulieren, dan is hij verwerker. Het 'doel' en de 'middelen' worden in deze situatie door de klant/opdrachtgever bepaald.

In alle gevallen van het verwerken van persoonsgegevens moet sprake zijn van een rechtmatige grondslag en passende beveiliging. Is de klant verwerkingsverantwoordelijke dan mag de accountant de klant vragen de rechtmatige grondslag aan te tonen. De accountant legt in dat geval de verantwoordelijkheid voor de rechtmatige grondslag vast in afspraken met de klant. Is van een rechtmatige grondslag geen sprake dan kan dat betekenen dat de accountant de gevraagde dienst niet kan leveren.

Wanneer verwerkingsverantwoordelijke én wanneer verwerker?

De feitelijke situatie is bepalend of de accountant wordt aangemerkt als verwerkingsverantwoordelijke dan wel als verwerker.

1. De accountant is *verwerkingsverantwoordelijke* voor de verwerkingen waarvoor hij doel en/of middelen bepaalt. Voorbeelden zijn:
   - het als werkgever verzamelen van de wettelijk vereiste gegevens van zijn werknemers. Grondslag is het moeten voldoen aan een wettelijke verplichting;
   - het als dienstverlener verzamelen van de identificerende gegevens van klanten/opdrachtgevers. Grondslag is het moeten voldoen aan een wettelijke verplichting;
   - het als ondernemer of dienstverlener verzamelen van contactgegevens van potentiële klanten en relaties. Dit betreft bijvoorbeeld de gegevens van personen die inschrijven op een nieuwsbrief of graag informatie willen ontvangen. Bij het verkrijgen van deze gegevens zal de accountant de expliciete toestemming vragen van de betrokkene om deze gegevens te mogen gebruiken en bewaren ('Opt-in').
2. De accountant is verwerker voor de verwerkingen van persoonsgegevens die hij in opdracht van de klant (verwerkingsverantwoordelijke) uitvoert. Voorbeelden zijn:
   - Het verwerken van salarissen;
   - Het bijhouden van een administratie;
   - Overeengekomen specifieke werkzaamheden;
   - Het opstellen van een fiscale aangifte;[3]
   - Het invullen van aanvragen, formulieren, etc.
3. De accountant wordt aangemerkt als verwerkingsverantwoordelijke (contextuele verantwoordelijkheid) voor de verwerkingen van persoonsgegevens die in opdracht van de klant (verwerkingsverantwoordelijke) worden uitgevoerd, maar waarbij de onafhankelijke uitoefening van het accountantsberoep een voorwaarde is. Voorbeelden zijn:
   - Het samenstellen van een jaarrekening;
   - Het beoordelen of controleren van een jaarrekening;
   - Het uitvoeren van een assurance-opdracht;
   - Advisering of consultancy;
   - Het uitvoeren van een bijzondere opdracht.

In deze laatste situatie heeft de accountant als verwerkingsverantwoordelijke een beperkte rol voor wat betreft de persoonsgegevens die hij van de klant/opdrachtgever heeft ontvangen. De klant/opdrachtgever blijft als verwerkingsverantwoordelijke verantwoordelijk voor de relatie met betrokkene en het invulling geven aan zijn of haar rechten.
De website van de NBA bevat een actueel overzicht waarin u terug kunt vinden of de account bij een bepaald type opdracht een verwerkingsverantwoordelijke of een verwerker is.[4]

3 LET OP: Bij aangiften IB is de accountant wel (functioneel) verwerkingsverantwoordelijke.
4 https://www.nba.nl/tools-en-voorbeelden/model-bewerkersovereenkomst/

Stap 2: Invulling geven aan de AVG-bepalingen

De mkb-accountant die persoonsgegevens verwerkt moet een aantal zaken geregeld hebben voor 25 mei 2018. In onderstaand overzicht is alles op een rij gezet.

Zaken die de mkb-accountant minimaal moet regelen voor 25 mei 2018

1. Een toereikende beveiliging (passende technische en organisatorische maatregelen) en de effectieve werking daarvan kunnen aantonen. Zie verder Stappen 3 en 4.
2. Schriftelijke afspraken met klanten en (sub)verwerkers over de beveiliging en verwerking van persoonsgegevens en kunnen aantonen dat deze worden nagekomen
3. Procedures om als verwerkingsverantwoordelijke invulling te kunnen geven aan de rechten van betrokkene(n) en om in voorkomende gevallen een datalek te kunnen melden aan de toezichthouder of betrokkene(n).
4. Procedures om als verwerker invulling te kunnen geven aan de meldingsplicht van een datalek aan de verwerkingsverantwoordelijke.
5. Processen en beveiliging waarbij rekening is gehouden met de principes van: Privacy by Design en by Default.
6. Procedures om als verwerkingsverantwoordelijke of verwerker in voorkomende gevallen een Data Protection Impact Assessment (DPIA) uit te kunnen voeren.
7. Het inrichten en bijhouden van een register van verwerkingsactiviteiten, zie 2.4.

Optioneel, niet verplicht door de AVG maar ter overweging aan de organisatie.

8. Een gedragscode waarin is vastgelegd hoe om te gaan met gegevens binnen de eigen organisatie en in relatie met de klanten.

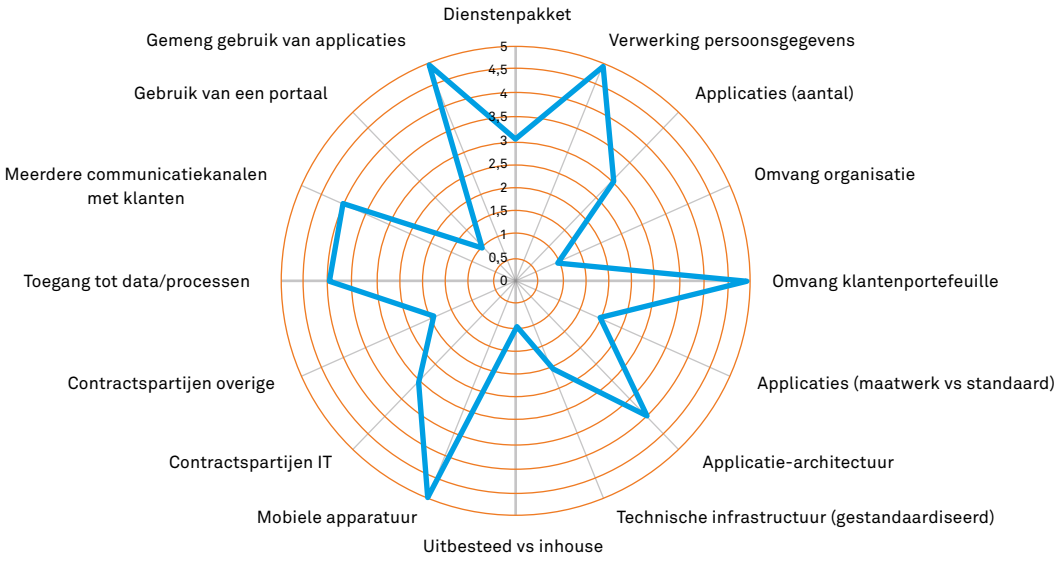
Stap 3: Verkrijg inzicht in de risico's

Risicoanalyse en Quick Scan

Om passende beveiligingsmaatregelen te kunnen nemen is het van belang inzicht te hebben in de grootste risico's die het kantoor loopt. Dit kan door het uitvoeren van risicoanalyse. Omdat een risicoanalyse veel tijd in beslag kan nemen, kan het kantoor beter beginnen met het uitvoeren van Quick Scan. Dit om een eerste indruk te krijgen welke gebieden als eerste aandacht vergen en waar maatregelen direct effectief kunnen zijn.

Ter illustratie is op de volgende pagina een afbeelding van een Quick Scan opgenomen. Via een score van 1 (laag) t/m 5 (hoog) wordt per aandachtgebied het risico ingeschat op kwetsbaarheid voor inbreuken. De scan geeft een overzicht van de verschillende aandachtsgebieden.

Aandachtsgebieden	Scores (range) van mate van risico					Score
	Laag 1	**2**	**3**	**4**	**Hoog 5**	
Dienstenpakket	Beperkt				Uitgebreid	5
Verwerking van persoonsgegevens	Weinig tot geen				Veel	5
Applicaties (aantal)	Klein				Groot	3
Omvang organisatie	Klein				Groot	3
Omvang klantenportefeuille	Klein				Groot	5
Applicaties (maatwerk versus standaard)	Standaard				Maatwerk	2
Applicatie-architectuur (o.a. aantal)	Eenvoudig				Complex	4
Technische infrastructuur (gestandaardiseerd)	Wel				Niet	3
Uitbesteed versus inhouse	Uitbesteed				Inhouse	2
Mobiele apparatuur	Nee				Ja	5
Contractspartijen IT	Weinig				Veel	3
Contractspartijen overige	Weinig				Veel	2
Toegang tot data / processen	Beperkt				Ruim	4
Meerdere communicatiekanalen met klanten	Nee				Ja	2
Gebruik van een portaal	Ja				Nee	1
Gemengd gebruik van applicaties	Nee				Ja	3



Afbeelding 4: Quick Scan

Baseline benadering

Naast een quick scan kan de organisatie ook kiezen voor de baseline benadering, als basis. Het basisbeveiligingsniveau is vaak gebaseerd op de maatregelen, zoals aangegeven in de Code voor Informatiebeveiliging, of een subset daarvan. Op een later moment wordt via het proces van risicoanalyse nagegaan of het basisbeveiligingsniveau toereikend is of dat voor bepaalde processen/systemen aanvullende maatregelen noodzakelijk zijn. In het NEMACC-rapport hebben de onderzoekers gekozen voor deze aanpak. In het daarin aangegeven Stappenplan is een set van maatregelen aangegeven die een mkb-kantoor op korte termijn kan invoeren (indien nog nodig). Zie verder Stap 4.

Stap 4: Het invullen van de beveiligingsmaatregelen

In deze stap voert de organisatie de maatregelen in die tot doel hebben de gegevens en processen te beschermen tegen inbreuken, verlies, etc. De maatregelen hebben betrekking op de volgende gebieden:

- de organisatie;
- de gegevens;
- het dienstenpakket/klantenportefeuille;
- de applicaties/applicatie-architectuur;
- de technische infrastructuur;
- derde partijen (sub)verwerkers;
- de toegang en de uitwisseling van data;
- het gebruik van mobiele apparatuur.

Het gebruikmaken van derde partijen

Bij het inrichten van informatiebeveiliging heeft de organisatie, naast het zelf treffen van de nodige maatregelen, ook nog een andere optie. Veel, vooral de wat kleinere mkb-kantoren, zullen door hun beperkte omvang (schaal) en gebrek aan deskundigheid niet of moeilijk in staat zijn om de gewenste beveiligingsmaatregelen zelf te realiseren. Het gebruikmaken van de diensten van derde partijen kan in dat geval een oplossing bieden. Voorbeelden zijn: het gebruik van toepassingen in de Cloud waardoor data op een veilige plaats wordt bewaard en het gebruik van beveiligde communicatie en mobiele apparaten. Voorwaarde is wel dat zaken worden gedaan met betrouwbare partijen (zoals ook de privacywetgeving vereist). Ook moet het kantoor in staat zijn om de inhoud en de kwaliteit van de geleverde diensten en naleving van de afspraken vast te kunnen stellen.

Een andere optie is dat bepaalde vormen van dienstverlening die een te groot beveiligingsrisico vormen en dus schadelijk kunnen zijn voor het kantoor of de reputatie worden beëindigd.

Stap 5: Evaluatie, monitoring en bijstelling

In deze afsluitende stap worden procedures ingevoerd om het functioneren van de ingevoerde maatregelen te kunnen evalueren, te monitoren, en desgewenst bij te kunnen stellen. Ook worden procedures opgezet om het gedrag te monitoren, om het niet-naleven van afspraken tijdig te kunnen signaleren (detectie) en om een juiste afhandeling van incidenten en verstoringen te garanderen.

4 | Advisering/ondersteuning van klanten

Vanzelfsprekend kunnen mkb-accountants een rol spelen bij het adviseren of ondersteunen van hun klanten bij het inrichten en op niveau brengen van hun informatiebeveiliging en het tijdig compliant zijn met de (vernieuwde) privacy-wetgeving.

Voorwaarde hiervoor is wel dat de mkb-accountant beschikt over de benodigde technische en juridische kennis. Indien hij daarover niet zelf beschikt, kan hij IT-specialisten inhuren of samenwerken met andere partijen (IT-juristen).

Bij de advisering of ondersteuning van klanten is het van belang dat de mkb-accountant de bedrijfsvoering van de desbetreffende organisatie en de daarbij behorende (bedrijfs)risico's als uitgangspunt neemt. De aard en omvang van de verwerkingen en de daarbij gebruikte (bijzondere) persoonsgegevens in combinatie met de aard en omvang de organisatie, dienstverlening, processen, etc. is bepalend voor de maatregelen die een organisatie moet treffen.

Dit vereist een inventarisatie van de verwerkingen en de daarbij te gebruiken persoonsgegevens en een vorm van risicoanalyse om duidelijk te krijgen welke maatregelen nodig zijn, naast de maatregelen en procedures die de AVG verplicht stelt. Denk aan passende beveiliging, aan de rechtmatige grondslag, relatie met betrokkene en een protocol voor het melden. De AVG-problematiek bij een organisatie in de zorg, bijvoorbeeld een huisartsenpraktijk, is volstrekt anders dan bij een handels- of transportonderneming, of een organisatie die internationaal en mogelijk zelfs buiten de EU opereert. De invulling van informatiebeveiliging en privacybescherming zal daar op moeten aansluiten.

Het bij klanten vragen om aandacht voor de problematiek van informatiebeveiliging en privacybescherming is natuurlijk altijd een eerst goede stap als start voor advisering. Vragen die daarbij kunnen worden gesteld zijn:

- Zijn uw medewerkers op de hoogte van de nieuwe privacyregels?
- Verwerkt uw organisatie persoonsgegevens, en zo ja, welke gegevens, in welke verwerkingen, waar opgeslagen en voor wie toegankelijk?
- Beschikt uw organisatie over een FG (indien verplicht)?
- Beschikt uw organisatie over passende beveiliging om de privacy-rechten van de betrokkene(n) van wie u persoonsgegevens verwerkt te kunnen beschermen?
- Beschikt uw organisatie over maatregelen procedures om invulling te kunnen geven aan de rechten van betrokkene(n)?
- Beschikt uw organisatie m.b.t. de verwerking van persoonsgegevens als verwerkingsverantwoordelijke/(sub)verwerker over de vereiste overeenkomsten?
- Beschikt uw organisatie over een protocol/procedures om een datalek te kunnen melden en (indien nodig) betrokkene(n) te informeren?
- Beschikt uw organisatie over maatregelen en procedures om inbreuken/datalekken m.b.t. persoonsgegevens te kunnen documenteren?
- Zijn uw medewerkers zich bewust van de huidige dreigingen op het terrein van informatiebeveiliging (cybercrime) en de belangrijkste oorzaken van datalekken?
- Weten uw medewerkers wat u in het kader van informatiebeveiliging en privacybescherming van hen verwacht, qua houding en gedrag?

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
E nba@nba.nl
I www.nba.nl