Informatiebeveiliging & privacybescherming (Deel I)

Een aanpak waarmee de MKB-accountant
kan voldoen aan de verscherpte eisen
van informatiebeveiliging en privacybescherming

(december 2017)

DEEL I

Informatiebeveiliging & privacybescherming

Een aanpak waarmee de MKB-accountant kan voldoen aan de verscherpte eisen van informatiebeveiliging en privacybescherming

December 2017

INHOUDSOPGAVE

SAMENVATTING & LEESWIJZER

Ook de MKB-accountant wordt geconfronteerd met het toenemende risico van cybercrime en de mogelijke gevolgen daarvan voor zijn bedrijfsvoering en reputatie als professioneel dienstverlener. De vraag is niet of hij wordt gehackt, maar wanneer en of zijn organisatie dan in staat is schade te voorkomen of te beperken. MKB-accountants maken gebruik van gegevens van hun klanten en verwerken persoonsgegevens [**4.2**]. Bedrijfs- en persoonsgegevens kunnen economisch gezien een grote waarde vertegenwoordigen. Het verlies of bekend worden van deze gegevens kan grote bedrijfsschade opleveren voor klanten[1] [2], maar ook voor de MKB-accountant zelf als professioneel dienstverlener[3]. Dit betekent dat de bescherming van zijn bedrijfs- en klantgegevens een essentiële voorwaarde is voor de 'Licence to Operate'.

Een goede informatiebeveiliging is ook nodig om te kunnen voldoen aan de eisen van de Algemene verordening gegevensbescherming (AVG), die op 24 mei 2016 in werking is getreden, en op 25 mei 2018 van toepassing wordt. De periode van 2 jaar tussen de inwerkingtreding van de AVG en het moment dat deze daadwerkelijk van toepassing wordt, stelt organisaties in de gelegenheid om zich voor te bereiden op de AVG. Tijdens deze twee jaar geldt in Nederland nog steeds de Wet bescherming persoonsgegevens (Wbp) uit 2001 en de Meldplicht datalekken, die 1 januari 2016 van kracht is geworden. Na 25 mei 2018 zal de toezichthouder overgaan tot handhaving en kunnen betrokkenen, die menen schade te hebben geleden, zich op de wet (AVG) beroepen. De Autoriteit Persoonsgegevens (AP) heeft bij monde van zijn voorzitter in het Financieele Dagblad van 11 juni 2017 aangegeven dat bedrijven rekening moeten houden met strikt toezicht[4]. In specifieke gevallen kan een geschil aan de rechter worden voorgelegd, die een bindende uitspraak kan doen.

Om de MKB-accountant in staat te stellen tijdig de benodigde maatregelen te treffen, publiceert NEMACC dit rapport, bestaande uit een **DEEL I** en **DEEL II**. Zie de **LEESWIJZER** voor informatie over de inhoud en het gebruik.

WAAROM IS DE AVG BELANGRIJK VOOR DE MKB-ACCOUNTANT?

De AVG scherpt de al bestaande eisen van de Wbp aan, breidt deze uit en brengt deze op Europees niveau. De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacy-rechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De AVG geeft de toezichthouder, de AP, de bevoegdheid hoge boetes op te leggen[5]. Het (niet) melden van een datalek kan ook grote gevolgen hebben voor de reputatie of de waarde van een onderneming[6].

De AGV stelt in [**art. 24, AVG**] stringente eisen aan de technische en organisatorische maatregelen [**4.4**]; deze dienen zodanig passend en effectief te zijn, dat zij waarborgen dat de verantwoordelijke organisatie kan aantonen dat de verwerking van persoonsgegevens in overeenstemming met de verordening (*doorlopend*) wordt uitgevoerd en dat de persoonsgegevens ook nodig zijn voor het doel van de verwerking. Dit betekent dat de AVG een 'open' norm stelt die de organisatie zelf op niveau moet invullen.

[1] https://fd.nl/economie-politiek/1218943/datalekken-doen-aandelenkoers-kelderen

[2] https://www.accountant.nl/nieuws/2017/9/deloitte-cybercrime-kost-economie-miljarden/

[3] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

[4] https://fd.nl/economie-politiek/1204827/miljoenenboete-facebook-is-kinderspel-bij-wat-komen-gaat

[5] De AP kan organisaties na het van toepassing worden van de AVG sancties opleggen van maximaal 20 miljoen euro of 4% van de wereldwijde omzet, afhankelijk van welk bedrag het hoogste is.

[6] De waarde van de internetactiviteiten die Yahoo verkocht aan de telecomreus Verizon leverde 350 miljoen dollar (332 miljoen euro) minder op door enkele grote computerinbraken bij het technologiebedrijf Yahoo, Telegraaf/DFT: 21 februari 2017.

In [**art. 28, AVG**] is bepaald dat een verwerking alleen mag worden uitbesteed aan een (sub)verwerker die afdoende garanties biedt dat passende technische en organisatorische maatregelen zijn getroffen, zodat de verwerking voldoet aan de eisen van de AVG en de rechten van betrokkene zijn gewaarborgd en dit ook kan worden aangetoond. Dit heeft het gevolg dat (potentiële) opdrachtgevers (klanten) alleen zaken mogen doen met MKB-accountants die zo'n garantie kunnen afgeven en dat de MKB-accountant verwerkingen alleen mag uitbesteden aan partijen die ook een dergelijke garantie kunnen afgeven. Dit is in de praktijk ook een zeer essentiële regel omdat in [**art. 82, AVG**] is bepaald dat "*Wanneer meerdere verwerkingsverantwoordelijken of verwerkers bij dezelfde verwerking betrokken zijn, en verantwoordelijk zijn voor schade die door verwerking is veroorzaakt, wordt elke verwerkingsverantwoordelijke of verwerker voor de gehele schade aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk wordt vergoed*".

Verder wordt in [**art. 28, AVG**] voorgeschreven dat de onderlinge relaties worden geregeld in een verwerkersovereenkomst [**4.6, 4.7** en **II: H-4**] waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, het niveau van beveiliging en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Hiermee worden de verantwoordelijkheden expliciet gemaakt.

Verwerkers hebben de plicht het nakomen van de in de overeenkomst vastgelegde verplichtingen aan te tonen. Dit kan door een onderzoek door de verwerkingsverantwoordelijke of een onafhankelijke auditor, die in opdracht van de verwerker / verwerkingsverantwoordelijke een onderzoek uitvoert.

In de nieuwe wet ligt de nadruk - meer dan nu - op de verantwoordelijkheid van organisaties om aan te kunnen aantonen dat zij zich aan de wet houden. Het kunnen aantonen van compliance met wet- en regelgeving is van groot belang in het geval dat een verwerkingsverantwoordelijke of (sub)verwerker door een betrokkene aansprakelijk wordt gesteld voor een inbreuk op zijn rechten, of door de toezichthouder een boete opgelegd krijgt. De verwerkingsverantwoordelijke of de (sub)verwerker kunnen van aansprakelijkheid worden vrijgesteld of zich tegen de boete verweren, als zij kunnen aantonen dat zij zich aan de wet hebben gehouden en dus niet verantwoordelijk zijn voor de geleden schade van betrokkene. In dit kader is het belangrijk dat organisaties beschikken over een Functionaris voor gegevensbescherming (FG) [**4.11**] en een register van verwerkingsactiviteiten [**4.8**], ook als dit door de AVG niet verplicht wordt gesteld.

Een belangrijk punt voor accountants bij het invullen en naleven van de privacywetgeving is de werkelijke inhoud van de rol van de accountant als dienstverlener. De daadwerkelijke rol is bepalend of de accountant in het kader van de AVG optreedt als verwerkingsverantwoordelijke [**4.6**] dan wel als verwerker [**4.7**]. Dit onderscheid is van belang omdat de verwerkingsverantwoordelijke meer en directe verplichtingen heeft met betrekking tot de betrokkene(n) van wie hij persoonsgegevens verwerkt. De verwerker heeft beperktere verplichtingen jegens betrokkenen en heeft in principe alleen te maken met de verwerkingsverantwoordelijke als opdrachtgever voor de uitgevoerde verwerkingen. De verplichting tot het treffen van passende technische en organisatorische maatregelen om de persoonsgegevens toereikend te beschermen en de effectieve werking daarvan aan te kunnen tonen, geldt echter voor zowel de verwerkingsverantwoordelijke als de verwerker.

WAT BETEKENT DIT VOOR DE ACCOUNTANT?

De AVG houdt geen rekening met de omvang van organisaties. Bepalend is of een organisatie persoonsgegevens verwerkt. De wijze waarop een kantoor invulling geeft aan de wettelijke verplichtingen, kan wel per kantoor verschillen.

De aanduiding MKB-accountant kent verschillende verschijningsvormen: een zelfstandige zonder personeel (Zzp'er), een eenmanspraktijk (één AA of RA met een aantal medewerkers), of een meermanspraktijk (meerdere AA's e/o RA's met medewerkers). Een Zzp'er heeft geen medewerkers waarmee moet worden overlegd, afspraken gemaakt en waarvan gedrag gemonitord. Een Zzp'er en waarschijnlijk ook een eenmanspraktijk zul-

len vaak gebruik maken van de diensten van derde partijen bij de invulling / ondersteuning van hun dienstverlening (denk hierbij aan serviceproviders voor de invulling van IT-ondersteuning). Grotere kantoren geven waarschijnlijk 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 gebruik maken van de diensten van (gespecialiseerde) derde partijen kan de belasting voor een kantoor verlichten, wat wel betekent dat afspraken moeten worden vastgelegd in overeenkomsten en de naleving gemonitord en vastgesteld.

In organisaties met medewerkers zullen aanpassingen in de informatiebeveiliging en het doorvoeren van maatregelen in het kader van de AVG om een meer project georiënteerde aanpak vragen. Maar het is uiteindelijk aan de verantwoordelijke(n) voor de organisatie welk keuzes worden gemaakt.

WAT MOET DE ACCOUNTANT MINIMAAL REGELEN

Om aan de eisen van de AVG te voldoen moet de MKB-accountant minimaal de volgende zaken geregeld hebben (zie voor een nadere invulling de hoofdstukken 6 en 7):

- Inzicht in zijn processen en bedrijfs- en persoonsgegevens die hij gebruikt / verwerkt / bewaart voor zijn dienstverlening n voor zijn eigen bedrijfsvoering. Dit ten behoeve van:
    - Het vaststellen of de AVG op zijn organisatie van toepassing is, en zo ja:
        - Het vaststellen van de rechtmatigheid van de verwerking (rechtmatige grondslag);
        - Na te gaan of zijn organisatie een FG moet aanstellen of deze functie nodig heeft;
        - Te bepalen of hij als dienstverlener verwerkingsverantwoordelijke e/o verwerker is.
- Een toereikende beveiliging (passende technische en organisatorische maatregelen), alsmede het kunnen aantonen van de effectieve werking daarvan.
- Schriftelijke afspraken met klanten en (sub)verwerkers over de beveiliging en verwerking van persoonsgegevens en het kunnen aantonen van het nakomen van deze afspraken.
- 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 / betrokkene(n).
- Procedures om als verwerker invulling te kunnen geven aan de meldingsplicht van een datalek aan de verwerkingsverantwoordelijke in de keten van verwerking.
- Procedures om als verwerkingsverantwoordelijke / verwerker een Privacy Impact Assessment / PIA uit te kunnen voeren bij nieuwe verwerkingen, bijvoorbeeld bij het gebruik van data-analyse.
- Bij het inrichten van processen en de beveiliging rekening houden met de verplichte uitgangspunten: Privacy by Design en by Default.
- Het als verwerkingsverantwoordelijke / verwerker inrichten en bijhouden van een register van verwerkingsactiviteiten (verplicht voor organisatie met meer dan 250 medewerkers).

Optioneel, niet verplicht door de AVG maar advies van de onderzoekers

- Het op vrijwillige basis inrichten en bijhouden van een register van verwerkingsactiviteiten.
- Het opstellen van een gedragscode waarin is vastgelegd hoe om te gaan met gegevens binnen de eigen organisatie en in relatie met de klanten.

DE ROL VAN DE BEROEPS- EN BRANCHEORGANISATIES

Het aantal MKB-accountants is relatief groot. De te treffen maatregelen vragen om maatwerk, maar kennen ook meer generieke (branche-brede) uitwerkingsmogelijkheden. De beroeps- en brancheorganisaties kunnen daarom een belangrijke rol vervullen door het ondersteunen van hun leden bij het voldoen aan de nieuwe wetgeving. Gelet op de verwachte complexiteit, impact en de nog korte resterende tijd zullen leden, branche breed, behoefte hebben aan specifieke expertise, alsmede voorbeelden en voorstellen op het terrein van:

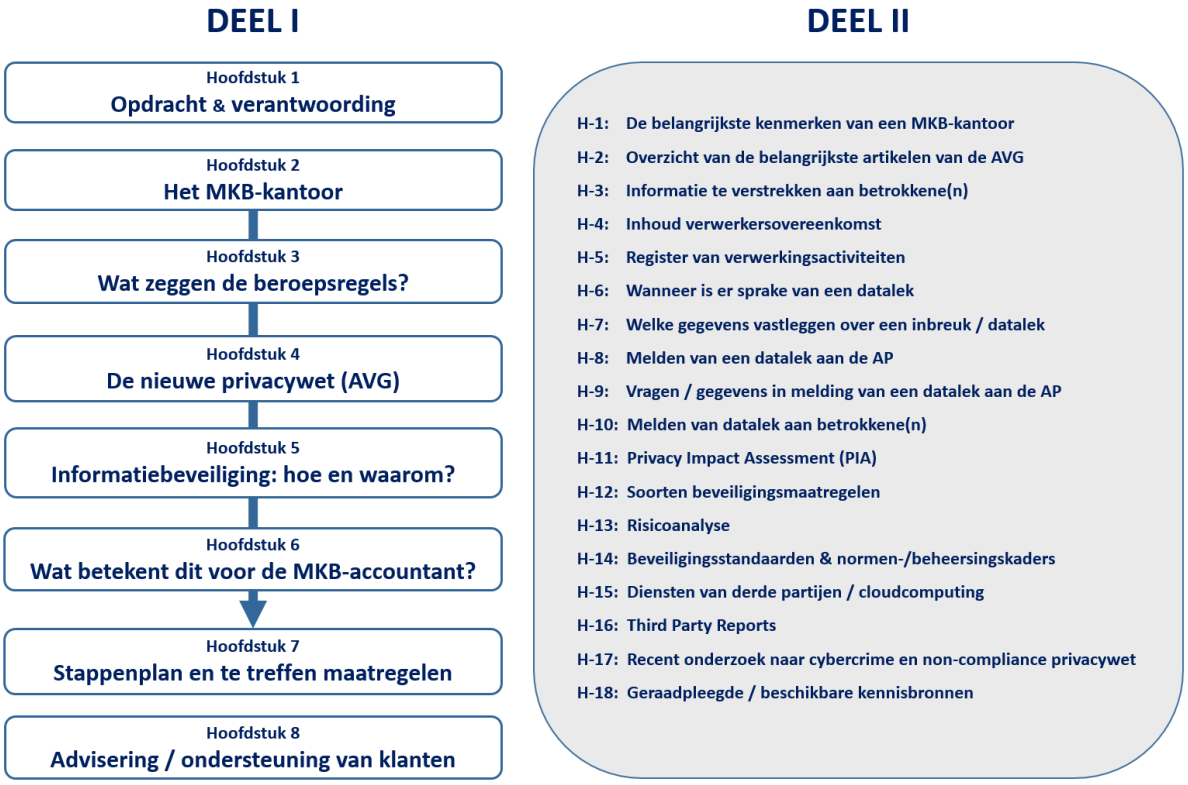
- Op de AVG aangepaste modellen voor Algemene voorwaarden en modelovereenkomsten.
- Een Gedragscode in combinatie met een vorm van privacy-certificering, waarvoor de AVG de mogelijkheid biedt [**art. 40** t/m **43, AVG**]. Een gedragscode kan de basis vormen voor een accountancysector breed beveiligings- en privacy-beleid en helpt accountantskantoren bij het realiseren van een toereikende informatiebeveiliging en privacybescherming, alsmede het kunnen aantonen daarvan. Een voorbeeld daarvan is inmiddels in de markt beschikbaar[7].
- Een model met daarin de beschrijving van standaard verwerkingen die een directe relatie hebben met de dienstverlening van accountants. Deze beschrijvingen kunnen als basis dienen voor de Algemene voorwaarden en modelovereenkomsten.
- Een onderzoek of het voor de groep van MKB-accountants relevant is om aan te sluiten bij een initiatief, waarbij een onafhankelijke derde partij als Trusted Third Party (TTP) de aangesloten partners faciliteert met een standaard beveiligings- en privacy-beleid waaraan alle aangesloten partner zich confirmeren, in combinatie met standaard overeenkomsten[8].
- Een onderzoek of het voor de groep van MKB-accountants relevant is een FG in de vorm van een Service te organiseren. Via een dergelijke service worden zij in staat gesteld over een dergelijke functie / expertise te beschikken, zonder zelf als organisatie een FG aan te moeten stellen. Op dit moment wordt een FG as a Service al door derde partijen in die vorm aangeboden.
- Bij te dragen aan verduidelijking op punten waarop dit rapport geen antwoord geeft, zoals de vaktechnische vragen die in het onderzoek aan de orde kwamen. Bijvoorbeeld:
  - Wat te doen als bij samenstel- of controlewerkzaamheden blijkt dat de organisatie van de klant op belangrijke punten zijn informatiebeveiliging niet op orde heeft en/of niet compliant is met de privacywet, of dat sprake is geweest van een groot datalek dat niet is gemeld bij de AP, met mogelijk ernstige gevolgen voor betrokkenen(n). Zie in dit kader de vragen die zijn gesteld over rol van de accountant bij het datalek bij Equifax[9].
  - Hoe om te gaan met bijzondere persoonsgegevens (waaronder medische gegevens) in het kader van de controle van zorguitgaven. Aan het gebruik daarvan zijn door de wet strikte eisen gesteld. Door de strikte eisen kan de accountant beperkt worden in zijn mogelijkheden zorguitgaven te controleren. In dat kader heeft de minister van Volksgezondheid, Welzijn en Sport[10] aangegeven, dat in ambtelijk overleg is vastgesteld dat het wenselijk is waar dat mogelijk is de onzekerheid over wettelijke voorschriften met betrekking tot de bescherming van persoonsgegevens bij financiële controles in de zorg op te heffen en waar dat noodzakelijk is die bescherming nader in voor-

[7] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med_20120518-besluit-gedragscode-persoonsgegevens-slimme-meter.pdf
[8] https://www.myobi.eu/
[9] https://www.accountant.nl/nieuws/2017/10/vragen-over-rol-accountant-bij-beveiliging-equifax/
[10] Brief van 28 juni 2016 (Kenmerk: 907104-146379 MC)

schriften vorm te geven. Het NBA heeft dit punt ingebracht in de consultatieronde van de Uitvoeringswet AVG. De onderzoekers gaan er vanuit dat dit punt wordt meegenomen in de uiteindelijke wetgeving.

LEESWIJZER

Om de MKB-accountant te ondersteunen bij het voldoen aan de eisen van informatiebeveiliging en privacybescherming bevat dit rapport (**DEEL I** en **DEEL II**) de volgende informatie. Het is aan de gebruiker van dit rapport die onderdelen te selecteren die voor hem/haar van belang zijn.



Afbeelding 1

Het MKB-kantoor [**hoofdstuk 2**]: In dit hoofdstuk is een beknopte beschrijving opgenomen van de werkzaamheden (dienstenpakket) en de organisatie van een MKB-kantoor. Deze beschrijving vormt de basis voor een analyse van de bedrijfsvoering wat betreft complexiteit en beheerbaarheid, als input voor een risicoanalyse en de op basis daarvan te treffen maatregelen en procedures. De gebruiker van dit rapport kan deze beschrijving gebruiken om inzicht te krijgen in de mogelijke risico's die zijn organisatie mogelijk loopt.

Wat zeggen de beroepsregels? [**Hoofdstuk 3**]: In dit hoofdstuk zijn de voor de MKB-accountant relevante bepalingen met betrekking tot informatiebeveiliging en vertrouwelijkheid opgenomen.

De nieuwe privacywet (AVG) [**Hoofdstuk 4**]: In dit hoofdstuk zijn de voor de MKB-accountant belangrijkste bepalingen van de nieuwe privacywet opgenomen.

Informatiebeveiliging: hoe en waarom? [**hoofdstuk 5**]: In dit hoofdstuk is een overzicht opgenomen van de actuele bedreigingen op het terrein van cybercrime en oorzaken van datalekken. In dit hoofdstuk wordt ook ingegaan op de inhoud van beveiligingsbeleid, de mogelijk te treffen maatregelen en procedures en een uit te voeren risicoanalyse. Voorts wordt inzicht gegeven in beschikbare beheersingskaders en guidance van de AP.

Wat betekent dit voor de MKB-accountant? [**hoofdstuk 6**]: In dit hoofdstuk wordt aangegeven welke zaken de MKB-accountant minimaal moet regelen om aan de verplichtingen van de nieuwe privacywet te kunnen voldoen en zijn informatiebeveiliging op niveau te brengen. Hierbij wordt ook ingegaan op de rol van de accountant in het kader van de AVG (verwerkingsverantwoordelijk en/of verwerker) en de daaruit voortvloeiende verplichtingen.

In dit hoofdstuk wordt ook een aantal uitgangspunten geformuleerd die de MKB-accountant kan hanteren bij het vormgeven van zijn beveiligingsbeleid. Deze uitgangspunten zijn door de onderzoekers gehanteerd bij de invulling van het **Stappenplan**, dat is opgenomen in **hoofdstuk 7**. Dit Stappenplan gaat uit van de 'Baseline' benadering en dekt de belangrijkste risico's af. Op basis van een eigen risicoanalyse kan de MKB-accountant vervolgens zelf nagaan welke aanvullende maatregelen nog nodig zijn om de informatiebeveiliging en interne beheersing op het voor zijn organisatie vereiste niveau te brengen.

Stappenplan en te treffen maatregelen [**hoofdstuk 7**]: In dit hoofdstuk wordt een concreet plan van aanpak gepresenteerd, met verwijzingen naar de relevante hoofdstukken en hulpmiddelen in de vorm van achtergrond- en detailinformatie, beslissingstabellen, beveiligingsstandaarden en normen-/beheersingskaders, alsmede een overzicht van de belangrijkste bepalingen van de AVG. Ook is een overzicht opgenomen van geraadpleegde bronnen / beschikbare kennisbronnen. Deze hulpmiddelen zijn opgenomen in **DEEL II: Achtergrondinformatie / hulpmiddelen**.

Advisering / ondersteuning van klanten [**hoofdstuk 8**]: In dit hoofdstuk wordt ingegaan op de ondersteuning die de MKB-accountant zijn klant kan bieden bij het op niveau brengen van zijn informatiebeveiliging en het kunnen voldoen aan wet- en regelgeving op het terrein van privacybescherming.

LEGENDA

In dit rapport worden de volgende verwijzingen gebruikt:

[**--.--**]	:	Verwijzing naar artikelen van de AVG of naar hoofdstukken en paragrafen in **DEEL I**.
[**II: H - ..**]	:	De in **DEEL II** opgenomen hulpmiddelen.
[..... - ..]	:	De geraadpleegde / beschikbare kennisbronnen, opgenomen in [**II: H-18**].

1. OPDRACHT & VERANTWOORDING

NEMACC, het samenwerkingsverband van de NBA en de Erasmus Universiteit Rotterdam (EUR), gericht op toepassingsgericht onderzoek ten behoeve van het midden- en kleinbedrijf (hierna: MKB), heeft opdracht gegeven onderzoek te verrichten naar de mogelijkheden voor de MKB-accountant om rekening te houden met de hedendaagse bedreigingen en (nieuwe) verplichtingen op het terrein van informatiebeveiliging en privacybescherming, inclusief de meldplicht datalekken.

DE ONDERZOEKSVRAGEN

Het onderzoek richtte zich op de volgende deelvragen:

A. Welke risico's loopt de MKB-accountant op het gebied van datalekken?

B. Welke aanpak kan de MKB-accountant ondersteunen in een effectieve databescherming binnen zijn bedrijfsprocessen en welke maatregelen moet de MKB-accountant treffen om te kunnen voldoen aan de (vernieuwde) privacywetgeving die 25 mei 2018 van toepassing wordt?

C. Welke toegevoegde waarde kan de MKB-accountant zijn klanten bieden die persoonsgegevens verzamelen, verwerken, bewaren en distribueren?

HET ANTWOORD OP DE ONDERZOEKSVRAGEN

Onderzoeksvraag **A**: Het antwoord op deze onderzoeksvraag wordt gegeven in de hoofdstukken **2** en **5**.

Onderzoeksvraag **B**: Het antwoord op deze onderzoeksvraag wordt gegeven in hoofdstukken **6** en **7**.

Onderzoeksvraag **C**: Het antwoord op deze onderzoeksvraag wordt beantwoord in hoofdstuk **8**.

In hoofdstuk **3** is een overzicht opgenomen van de belangrijkste bepalingen in de beroepsregels gericht op informatiebeveiliging en privacybescherming. In hoofdstuk **4** is een overzicht opgenomen van de voor de MKB-accountant belangrijkste bepalingen van de AVG.

In **DEEL II** is naast een overzicht van de bepalingen van de AVG, achtergrond- en detailinformatie opgenomen, alsmede hulpmiddelen in vorm van beslissingstabellen, beveiligingsstandaarden en normen-/beheersingskaders. Ook is een overzicht opgenomen van geraadpleegde bronnen / beschikbare kennisbronnen [**II: H-18**].

DE GEHANTEERDE UITGANGSPUNTEN / AANPAK

Bij het opstellen van dit rapport zijn de onderzoekers uitgegaan van de bedrijfsvoering van een MKB-accountant en zijn belang om als professioneel dienstverlener te voldoen aan de verwachtingen van zijn klant en de eisen die wet- en regelgeving (beroepsregels en wettelijke eisen) aan hem en zijn organisatie stellen. Uitgangspunt hierbij is het waarborgen van de betrouwbaarheid, bestaande uit integriteit, beschikbaarheid en vertrouwelijkheid, alsmede compliance. Compliance met regelgeving wordt gezien als een minimale vereiste (vorm van hygiëne maatregelen). De definitie van de genoemde kwaliteitscriteria is ontleend aan de publicatie van het CPB (nu AP) waarin zij invulling geeft aan wat naar de mening van de toezichthouder een passend niveau van beveiliging is [**CBP-2**].

Om een referentiekader te hebben, is in dit rapport een beknopte beschrijving opgenomen van de werkzaamheden (dienstenpakket) en organisatie, inclusief het daarbij behorende IT-landschap, van een MKB-kantoor. Voorts is uitgegaan van de privacywetgeving (AVG) die op 25 mei 2018 van toepassing wordt.

Vervolgens zijn in een literatuurstudie de vernieuwde privacywetgeving, recent onderzoek op het terrein van informatiebeveiliging (cybercrime) en privacybescherming, alsmede mogelijk bruikbare beveiligingsstandaarden, normen- en beheersingskaders in kaart gebracht. Deze literatuurstudie vormde vervolgens de basis voor het voorstel voor het Stappenplan en door het MKB-kantoor te nemen acties en te treffen maatregelen.

HET ONDERZOEK

Het onderzoek is uitgevoerd door:

- J. Pasmooij RE RA RO, werkzaam bij de Erasmus School of Accounting & Assurance van de Erasmus Universiteit Rotterdam en Pasmooij Consulting & Education BV;
- Drs. R Snoeker RA, werkzaam bij de Erasmus School of Accounting & Assurance van de Erasmus Universiteit Rotterdam en ICU2 Advice & Support BV.

Voorts dank aan de accountantskantoren, die bereid waren hun inzichten met de onderzoekers te delen en het conceptrapport van commentaar te voorzien.

- BDO;
- DRV Accountants & Adviseurs[11];
- Joanknecht[12];
- Kappenberg Accountancy & Advies[13];
- Lansigt Accountants en Belastingadviseurs[14].

Dit geldt ook voor Verdonck, Klooster & Associates en Duthler Associates, met wie de mogelijke gevolgen voor de bedrijfsvoering en IT voor accountants, alsmede de juridische aspecten van de wet zijn besproken. Daarnaast heeft telefonisch contact plaatsgevonden met Arnout van Kempen[15], die bij een aantal MKB-kantoren onder meer de rol van Compliance Officer vervult.

[11] 12 vestigingen, ca. 550 medewerkers
[12] 1 vestiging, ca. 125 medewerkers
[13] 2 vestigingen, 6 medewerkers
[14] 3 vestigingen, ca. 130 medewerkers
[15] Van Kempen Compliance & Legal Support

2. HET MKB-KANTOOR

In dit hoofdstuk is een beknopte beschrijving opgenomen van de werkzaamheden en de daarbij mogelijk te gebruiken gegevens, alsmede de organisatie en IT-landschap van een MKB-kantoor. Een beknopte beschrijving van de werkzaamheden geeft inzicht in de gegevens die door de accountant (moeten of kunnen) worden gebruikt[16]. Voor bepaalde soorten gegevens geldt dat het gebruik alleen is toegestaan als aan strikte wettelijke eisen is voldaan.

Een MKB-accountant beschikt door de aard van zijn werkzaamheden over gegevens van klanten (op papier of in elektronische vorm). De zorgvuldigheid van het beroep brengt met zich mee dat het uiterst ongewenst is dat gegevens van klanten of van zijn eigen organisatie via zijn systemen openbaar worden of ongeautoriseerd geraadpleegd, gemuteerd of gedistribueerd. Een analyse van de organisatie en het (mogelijke) IT-landschap van een MKB-kantoor geeft inzicht de problematiek waarmee de accountant in de praktijk te maken heeft en welke (potentiële) bedreigingen het gebruik van IT met zich mee brengt.

DE WERKZAAMHEDEN VAN EEN MKB-ACCOUNTANT

De werkzaamheden (dienstenpakket) van een MKB-accountant kunnen o.m. bestaan uit de volgende activiteiten (niet limitatief):

- Het controleren van jaarrekeningen;
- Overige assurance-werkzaamheden;
- Het samenstellen van jaarrekeningen;
- Administratieve dienstverlening, waaronder het bijhouden van bedrijfs- en personeelsadministratie, alsmede salarisverwerking;
- Fiscale en juridische dienstverlening;
- Advies over / ondersteuning bij o.a. pensioen, overnames, fusies, bedrijfsopvolging, waardebepaling, financiering, estate planning, subsidies;
- Werkzaamheden op het terrein van IT-auditing;
- Het aanbieden van online dienstverlening.

Bovenstaande werkzaamheden worden in opdracht van klanten uitgevoerd. Daarnaast is het mogelijk dat het kantoor op eigen initiatief activiteiten ontplooid, bijvoorbeeld het verstrekken van informatie, nieuwsbrief, etc. in het kader van marketing en relatiemanagement.

Op de uitvoering van deze werkzaamheden zijn verschillende standaarden van toepassingen en soms gelden verschillende uitvoeringsregels, zoals controleprotocollen en/of subsidievoorwaarden.

WELKE DATA GEBRUIKT / VERWERKT EEN MKB-ACCOUNTANT

Bij de uitvoering van bovenstaande werkzaamheden krijgt de accountant te maken met een veelheid aan bedrijfs- en persoonlijke gegevens.

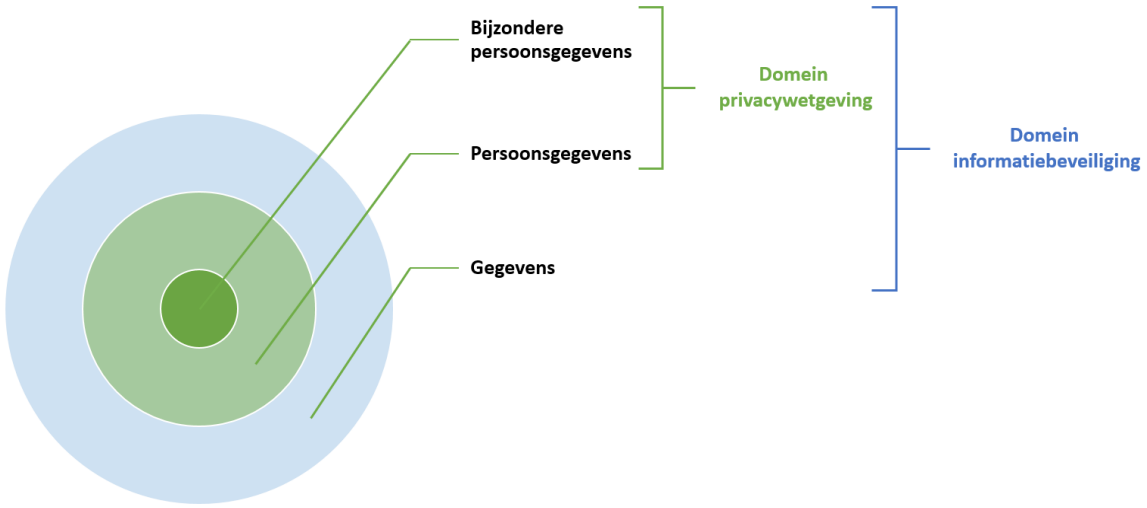
Voorbeelden van gegevens die bij de uitvoering van werkzaamheden kunnen worden gebruikt / bewaard (niet limitatief) zijn:

- Grootboektransacties;
- Inkoopcontracten / -prijzen / -facturen & Verkoopcontracten / -prijzen / facturen;

[16] Niet alleen kennis nemen, maar ook verwerken, misschien zelfs (laten) bewerken, (tijdelijk) opslaan en/of bewaren.

- Debiteuren- / crediteurengegevens - betalingen / banktransacties;
- Orders - kortingen / provisies;
- Begrotingen / budgetten;
- Claims / rechtszaken;
- Fiscale gegevens;
- Notulen / verslagen / correspondentie / e-mailverkeer / berichten sociale media;
- Personeels- / salaris- / verzuimgegevens / Loonbeslag;
- Reis- / kosten- / zorgdeclaraties;
- Relatie- / contactgegevens - identificerende gegevens van klanten;
- Research & Development - recepturen / octrooien.

Privacywetgeving richt zich op organisaties die **persoonsgegevens** [**4.2**] verwerken. Onder verwerken wordt verstaan: verzamelen, vastleggen, ordenen, structureren, raadplegen, verstrekken, bewerken, verwerken of vernietigen. Kortom “alle” activiteiten rond gegevens. Bij elke vorm van verwerking kunnen inbreuken op de privacy optreden.



Afbeelding 2: Overzicht van gegevens

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.

Een gegeven is **geen persoonsgegeven** als maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. Dit wordt **anonimiseren** genoemd.

Een deel van de persoonsgegevens wordt gezien als gevoelige gegevens, ook wel **bijzondere persoonsgegevens** genoemd. Gebruik en verwerking mag alleen onder strikte voorwaarden. Voorbeelden zijn gegevens over:

- 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).

Veel van de gegevens kunnen vanuit een bedrijfseconomisch perspectief een grote waarde vertegenwoordigen voor zijn klanten. Het verlies of bekend worden van klantgegevens via zijn organisatie kan grote bedrijfsschade opleveren voor zijn klant, maar ook als professioneel dienstverlener. Het is niet altijd mogelijk om op voorhand aan te geven welke gegevens nu feitelijk door accountants worden gebruikt of welke gegevens door of via andere partijen, waaronder ingehuurde deskundigen of externe dienstverleners, in de systemen van het accountantskantoor zijn opgeslagen en worden bewaard. Onderstaande voorbeelden illustreren het onverwachts bezit / gebruik van (bijzondere) persoonsgegevens, met mogelijk grote gevolgen:

In de interviews met een aantal accountantskantoren kwam naar voren dat accountants soms onverwacht en onbedoeld worden geconfronteerd met gegevens die niet door hun organisatie in het kader van hun werkzaamheden worden gebruikt, maar bijvoorbeeld wel door hun klanten of hun adviseurs.

Zo bleek een klant in het salarissysteem dat door het accountantskantoor wordt gebruikt, maar ook online toegankelijk en beschikbaar is voor klanten, verzuimgegevens van medewerkers bij te houden. Dit bleken bijzondere persoonsgegevens te zijn die niet door de accountant binnen zijn organisatie mogen worden verwerkt, tenzij daarvoor een wettelijke grondslag bestaat.

In een ander geval werd een accountantskantoor betrokken in de mailwisseling tussen zijn klant en juridische adviseurs over persoonlijke zaken in fiscale aangelegenheden en/of juridische geschillen.

Een ander voorbeeld is de controle van zorgkosten waarbij de accountant in vele gevallen genoodzaakt is om medische gegevens te raadplegen om zijn controle te kunnen uitvoeren. Het gebruik van bijzondere persoonsgegevens (zoals medische gegevens) vereist speciale aandacht, omdat deze niet mogen worden verwerkt, tenzij is voldaan aan in de wet specifiek aangegeven voorwaarden. Het raadplegen van dergelijke gegevens door de accountant is echter bij wet niet toegestaan[17]. Dit betekent dat de accountant dergelijke gegevens op basis van de wet niet kan gebruiken en dus ook niet in zijn bezit mag hebben (controledossier).

Een aanbieder van boekhoudsoftware blijkt, in het geval dat de MKB-accountant gebruik maakt van de Cloudversie, in het contract te hebben opgenomen dat de serviceprovider de klantgegevens mag gebruiken. Weliswaar geanonimiseerd, maar de MKB-accountant heeft daarbij geen zicht meer op het gebruik en of de overeengekomen werkelijk voorwaarden worden nagekomen.

Een MKB-kantoor werd er door zijn klant op gewezen dat het salarispakket, dat door het kantoor ook aan zijn klanten in de vorm van een Cloudtoepassing wordt aangeboden en waarin ook reisdeclaraties worden bijgehouden en verwerkt, op de achtergrond communiceert met Google om de gedeclareerde reisafstanden te kunnen controleren. De vraag is welke toepassingen nog meer toegang hebben tot het salarispakket?

Omdat de accountant bij de uitvoering van werkzaamheden gebruik maakt van technologische ondersteuning (IT-systemen maar ook vormen van data-analyse en process mining op klantdata) is het van belang inzicht te hebben in het IT-landschap van een doorsnee accountantskantoor. Dit inzicht helpt om een beeld te krijgen van de mogelijke bedreigingen die de betrouwbaarheid, continuïteit en vertrouwelijkheid van de processen en gegevens kunnen aantasten.

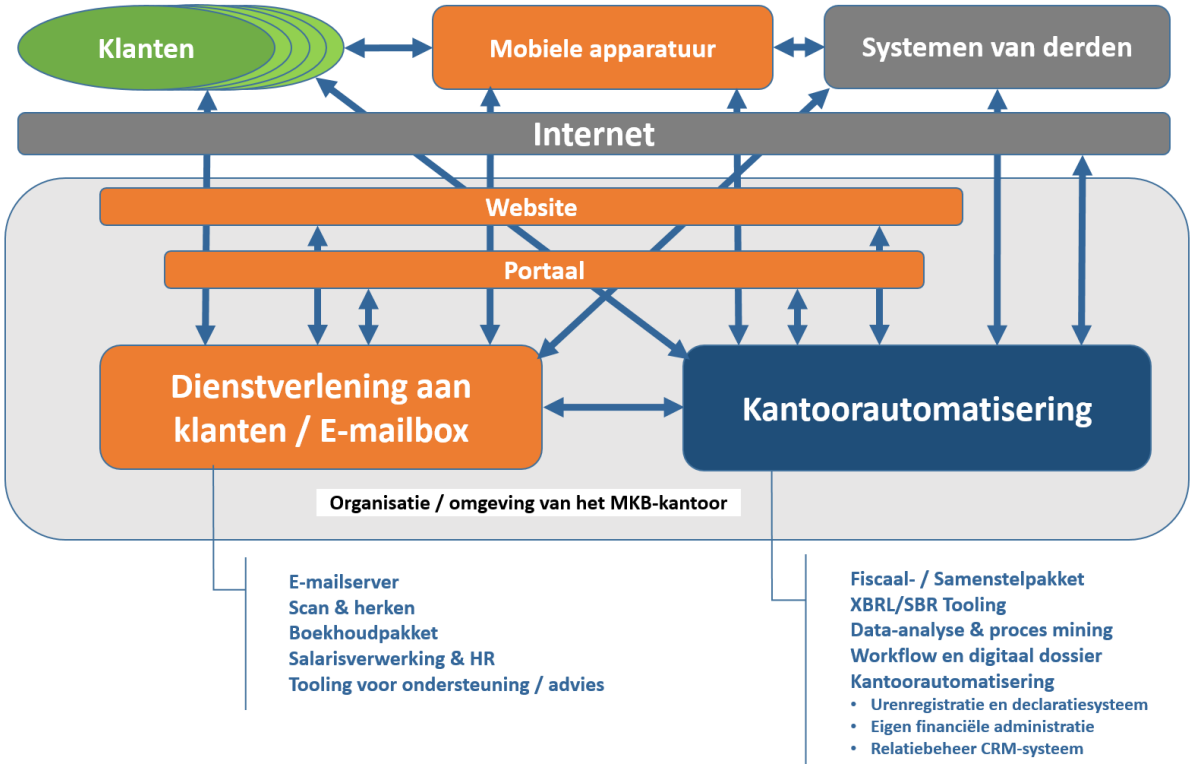
[17] Het gebruik van medische gegevens om controle van zorguitgaven te kunnen uitvoeren is onderwerp van gesprek tussen de NBA en de AP. De minister van VWS heeft in een brief (gedateerd 28 juni 2016) aangegeven dat gebruik in het kader van de controle mogelijk moet zijn, en zo nodig wettelijk moet worden geregeld.

HET IT-LANDSCHAP VAN EEN MKB-KANTOOR

Op basis van de interviews met een aantal MKB-kantoren is een beeld ontstaan van de organisatie en het IT-landschap van een MKB-kantoor. De gebruikte toepassingen zijn in functionele zin omschreven. In deze illustratie zijn ook de onderlinge relaties (communicatie / gegevensuitwisseling) tussen de verschillende toepassingen en partijen weergegeven.

Door het gebruik van kleur is het onderscheid aangegeven tussen:

- toepassingen die door de accountant zelf worden gebruikt en waartoe gebruikers geen toegang hebben (**blauw**);
- gemengde toepassingen waarin ook door derde partijen wordt gewerkt (**oranje**) of informatie geplaatst (zoals een mailbox);
- toepassingen van derden waar de accountant geen zeggenschap over heeft (**grijs**).



Afbeelding 3: IT-landschap MKB-kantoor

In de praktijk kan het voorkomen dat meerdere toepassingen in één computerprogramma beschikbaar zijn. Maar ook dat gebruik wordt gemaakt van de diensten van derde partijen / cloudproviders.

KENMERKEN / RISICOGEBIEDEN VAN HET MKB-KANTOOR

De diversiteit van de dienstverlening, in combinatie met het gebruik van een veelheid van gegevens en een in veel opzichten vaak complex IT-landschap, brengt risico's met zich mee. In [**II: H-1**] is een gedetailleerd overzicht opgenomen van de belangrijkste kenmerken van een MKB-kantoor. Onderstaand zijn de belangrijkste kenmerken van een MKB-kantoor aangegeven. Deze kenmerken maken het MKB-kantoor kwetsbaar voor verlies/misbruik van data en verstoring van de bedrijfsvoering, alsmede non-compliance met de privacywetgeving.

De belangrijkste risico's voor het kantoor zijn:

De integrale aanpak van analyse tot implementatie van de gevolgen van privacywetgeving vraagt om een substantiële inzet van mensen en middelen. Risico: gelet op de omvang van veel MKB-kantoren is vaak niet voldoende diepgaande **kennis van IT en privacy** en voldoende **personele capaciteit beschikbaar**.

Een **uitgebreid dienstenpakket** waarin een **veelheid aan data** wordt gebruikt, waaronder (bijzondere) persoonsgegevens, alsmede een diversiteit aan invulling, vraagt om managementaandacht. Risico: de aanwezige managementaandacht kan niet ten volle aan deze aspecten worden besteed.

Veelvuldige **communicatie met klanten via meerdere kanalen**. Risico: niet alle afspraken met klanten over de wijze waarop data wordt uitgewisseld zijn eenduidig vastgelegd. Risico: klanten houden zich hier niet aan. Risico: worden de kansen op een datalek effectief gemitigeerd?

Veelvuldig **gebruik van de diensten van** - vaak meerdere - **derde partijen**. Risico: onbevoegden verkrijgen toegang tot data.

Voor de communicatie met klanten en derde partijen wordt vaak **gebruik gemaakt van publieke diensten**, zoals het internet, maar ook voor de uitwisseling en soms zelfs opslag van data (WeTransfer, Dropbox, Google Drive of OneDrive). Risico: bij het gebruik van deze diensten heeft de gebruiker onvoldoende waarborgen dat aan de verplichtingen van de AVG wordt voldaan.

Een **complexe IT-infrastructuur** door het gebruik van meerdere applicaties en dienstverleners. Risico: een voldoende beveiligingsniveau kan niet worden gerealiseerd.

Gemengd gebruik van de applicaties: applicaties worden zowel door de klanten als het MKB-kantoor gebruikt. Risico: de accountant heeft geen zicht op welke gegevens door de klant in zijn IT-omgeving worden geplaatst / verwerkt en waarvoor hij qua beveiliging mede verantwoordelijk wordt.

Afwezigheid van de toepassing van een **geïntegreerde vorm van toegangsbeveiliging**, inclusief centraal beheer van autorisaties en bevoegdheden. Risico: ongewenst verkrijgen van toegang omdat een voldoende beveiligingsniveau niet (eenvoudig) is te realiseren of alleen tegen een zwaardere beheerlast.

Gebruikmaken van mobiele apparatuur (laptops, tablets en smartphones, zelfs wearables), die weer eigen specifieke bedreigingen meebrengen. Risico: ongewenst verkrijgen van toegang omdat een voldoende beveiligingsniveau niet (eenvoudig) is te realiseren of alleen tegen een zwaardere beheerlast.

De **e-mailbox en de website** van het kantoor staan **open voor communicatie** met derden. Daarnaast zijn applicaties soms gekoppeld met sociale media. Risico: ongewenst verkrijgen van toegang tot data of systemen.

Onduidelijkheid **op welke plaatsen welke data is opgeslagen.** Risico: de accountant weet niet of hij voldoet aan de bepalingen van de privacywet en of de data goed zijn beveiligd.

In [**6.3**] is aangegeven welke keuzes een MKB-accountant kan maken bij het formuleren van zijn beveiligingsbeleid en het daarop aansluitende **Stappenplan** en te treffen maatregelen in [**7**], waarbij rekening is gehouden met de belangrijkste risico's van een MKB-kantoor, naast de oorzaken van verlies/misbreuk van data en verstoring van de bedrijfsvoering.

3. WAT ZEGGEN DE BEROEPSREGELS?

In dit hoofdstuk wordt ingegaan op de bepalingen in de beroepsregels voor de MKB-accountant, gericht op informatiebeveiliging en privacybescherming.

VERORDENING GEDRAGS- EN BEROEPSREGELS ACCOUNTANTS (VGBA)

De relevante bepalingen zijn:

> De accountant past de bij een professionele dienst relevante wet- en regelgeving toe [**art.13, VGBA**].
>
> De accountant die de beschikking krijgt over gegevens of inlichtingen waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, is verplicht tot geheimhouding van die gegevens of inlichtingen, behoudens voor zover hij: ……..[**art. 16, VGBA**].
>
> De accountant treft redelijkerwijs te nemen maatregelen om ervoor te zorgen dat degene die onder zijn verantwoordelijkheid werkzaamheden uitvoert ten behoeve van een professionele dienst of aan wie hij advies of ondersteuning vraagt, de vertrouwelijkheidsverplichtingen naleeft zoals deze voor accountants gelden [**art. 19, VGBA**].
>
> De accountant identificeert en beoordeelt omstandigheden die een bedreiging kunnen zijn voor het zich houden aan een fundamenteel beginsel en neemt met betrekking tot dergelijke omstandigheden een toereikende maatregel die ertoe leidt dat hij zich houdt aan de fundamentele beginselen [**art. 21, VGBA**].

De bovenstaande regelgeving houdt in dat de accountant op basis van een risicoanalyse de benodigde maatregelen treft om de integriteit, beschikbaarheid en vertrouwelijkheid van de onder zijn verantwoordelijkheid berustende gegevens te waarborgen.

STANDAARD 230: CONTROLEDOCUMENTATIE

Standaard 230 verplicht de accountant controledocumentatie op te stellen met o.m. als doel verantwoording af te kunnen leggen over zijn werkzaamheden. In de standaard is geen opsomming opgenomen van in de controledocumentatie op te nemen gegevens. De vorm en inhoud zijn afhankelijk van verschillende factoren, zoals de aard van de uitgevoerde controlewerkzaamheden, de significantie van de verkregen controle-informatie, of de gehanteerde controlemethodologie en hulpmiddelen. Het kan in de praktijk betekenen dat in zijn controledocumentatie bedrijfsgegevens, persoonsgegevens of zelfs bijzondere persoonsgegevens zijn opgenomen.

NBA-HANDREIKING 1124 EN DE WWFT

De Wet ter voorkoming van witwassen en financiering van terrorisme (WWFT) verplicht accountants tot het uitvoeren van een klantenonderzoek [**art. 3, lid 1, WWFT**]. Het klantenonderzoek houdt o.m. in het identificeren van de (potentiële) klant en het verifiëren van diens identiteit. De wet geeft specifieke aanwijzingen voor de vastlegging van de identiteits- en verificatiegegevens [**art. 33, WWFT**]. Deze vastlegging moet toegankelijk zijn, wat redelijkerwijs veronderstelt dat controle eenvoudig kan plaatsvinden. Vastlegging kan derhalve in het klantdossier of in een centrale administratie of een combinatie daarvan. Van een natuurlijk persoon dient ter identificatie het volgende te worden vastgelegd (geslachtsnaam, voornamen, geboortedatum, adres en woonplaats dan wel plaats van vestiging).

De verificatie van de identiteit van de persoon kan plaatsvinden aan de hand van een document met persoonsidentificerend nummer (paspoort, rijbewijs, identiteitskaart) [**MinFin-1**]. Om de uitgevoerde verificatie (achteraf) aan te kunnen tonen moeten de identificerende gegevens van het gebruikte document worden vastgelegd (aard, nummer, datum, plaats van uitgifte), of kan een afschrift van dit document in de administratie van de accountant worden opgenomen. Omdat de privacywet strikte eisen stelt aan het mogen verzamelen en gebruiken van persoonsgegevens heeft het College bescherming persoonsgegevens (CPB, nu AP) in CPB Richtsnoeren [**CBP-1**] aangegeven wat private partijen in dit kader wel en niet is toegestaan. De AP staat de accountant toe dat deze in het kader van zijn identificatieplicht een afschrift van het daarbij gebruikte identiteitsbewijs in zijn administratie mag opnemen.

4. DE NIEUWE PRIVACYWET (AVG)

In dit hoofdstuk is een overzicht opgenomen van de belangrijkste bepalingen van de AVG, die voor de MKB-accountant van belang zijn. Waar relevant is verwezen naar de van toepassing zijnde artikelen van de AVG, de volledige tekst van deze artikelen is opgenomen in [**II, H-2**]. Voorts is gebruik gemaakt van de guidance die de AP heeft verstrekt in de publicaties over de meldplicht datalekken en de AVG. Omdat op het moment van het schrijven van dit rapport, de AP nog bezig is met het verwerken van de ontvangen reacties op de consultatie[18] gericht op de Uitvoeringswet Algemene verordening gegevensbescherming [**V&J-1**], is het mogelijk dat bij de uiteindelijke invoering de wettelijke bepalingen op punten door de Nederlandse overheid nog worden aangescherpt of nader ingevuld. De ruimte voor de Nederlandse regering om voor der Nederlandse situatie aanpassingen aan te brengen zijn echter uiterst gering, zodat de kern van de wet niet verandert.

4.1 DOEL EN TOEPASSINGSGEBIED VAN DE WET

In de AVG worden regels vastgesteld betreffende de bescherming van natuurlijke personen (**betrokkenen**) in verband met de **verwerking** van **persoonsgegevens** en betreffende het vrije verkeer van persoonsgegevens [**art. 1, AVG**].

WANNEER IS DE AVG VAN TOEPASSING?

De verordening is van toepassing op:

De geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een **bestand** zijn opgenomen of die bestemd zijn om daarin te worden opgenomen [**art. 2, lid 1, AVG**].

> **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de **betrokkene**), zie [**4.2**];
>
> Voor de **betrokken partijen**, zie [**4.3**];
>
> **Verwerking**: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens: zie verder: zie verder, zie [**4.4**];
>
> **Bestand**: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

Op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking binnen of buiten de Unie plaatsvindt [**art. 3, lid 1, AVG**].

Op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met [**art. 3, lid 2, AVG**]:

[18] https://www.internetconsultatie.nl/uitvoeringswetavg

a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of

b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.

Door een verwerkingsverantwoordelijke die niet in de Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het lidstatelijke recht van toepassing is [**art. 3, lid 3, AVG**].

Wanneer de AVG van toepassing is, is ook de meldplicht datalekken van toepassing [**art. 33 en 34, AVG**].

WANNEER IS DE AVG NIET VAN TOEPASSING?

De AVG **is niet van toepassing** op de verwerking van persoonsgegevens [**art. 2, lid 2 AVG**]:

a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;

b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;

c) door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;

d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

4.2 WANNEER IS SPRAKE VAN PERSOONSGEGEVENS?

Een **persoonsgegeven is elk gegeven** over een geïdentificeerde of identificeerbare natuurlijk persoon (de betrokkene). Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct[19] of indirect[20] kan worden geïdentificeerd, met name aan de hand van een identificator, zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door servers ontvangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen.

Een gegeven is **geen persoonsgegeven**, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. Dit wordt **anonimiseren** genoemd.

Het toepassen van cryptografische bewerkingen zoals encryptie of hashing op identificerende gegevens leidt tot **pseudonimisering** (het vervangen van een identificerend gegeven door een ander identificerend gegeven) maar niet tot anonimisering. Een voorbeeld van een dergelijke bewerking is het versleutelen of hashen van klantnummers. Als verantwoordelijke bent u, ook na de encryptie of hashing, nog steeds in staat om de betrok-

[19] Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum.

[20] Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaald persoon.

kene te identificeren. Er is dus nog steeds sprake van persoonsgegevens. Wel is pseudonimiseren een waardevolle beveiligingsmaatregel die bij een datalek de kans op daadwerkelijk misbruik van de gelekte persoonsgegevens aanzienlijk kan verlagen.

Het anonimiseren (verwijderen van de direct identificerende gegevens) biedt op zichzelf niet altijd voldoende garantie dat er geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit een andere bron, kan immers desondanks, soms zonder bijzondere inspanning, identificatie tot stand worden gebracht. Verder moet bij anonimiseren rekening worden gehouden met de stand van de techniek. Wat bij een bepaalde stand van de techniek als anoniem kan worden beschouwd, aangezien het gegeven niet redelijkerwijs tot een persoon te herleiden is, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding.

VOORBEELDEN VAN PERSOONSGEGEVENS

- Naam, zakelijk of huisadres, locatie, geboortedatum, titulatuur, geslacht;
- E-mailadres, telefoonnummers, inhoud van e-mails, surfgedrag;
- werkgever, functie, personeelsnummer, loopbaan, opleidingen, competenties;
- Medische gegevens;
- Antwoorden, klachten, meningen, publicaties;
- Overtredingen, veroordelingen;
- Gebruikersnamen, wachtwoorden, IP-adressen, tracking cookies, RFID-nummer, MAC-adressen.

Een deel van de persoonsgegevens wordt gezien als gevoelige gegevens, deze worden ook wel bijzondere persoonsgegevens genoemd. Aan het gebruik en de verwerking zijn strikte eisen gesteld.

BIJZONDERE PERSOONSGEGEVENS

De wet onderkent ook bijzondere persoonsgegevens [**art. 9, AVG**]. Deze gegevens hebben betrekking op:

- Ras of etnische afkomst;
- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuiging;
- Het lidmaatschap van een vakbond;
- Genetische gegevens[21];
- Biometrische gegevens met het oog op de unieke identificatie van een persoon[22];
- Gegevens over gezondheid[23];
- Gegevens over seksueel gedrag en seksuele gerichtheid.

In de nieuwe wetgeving wordt de verwerking van foto's niet systematisch meer beschouwd als verwerking van bijzondere persoonsgegevens. De context van de verwerking is in deze relevant. Alleen onder bepaalde omstandigheden, bijvoorbeeld wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken, kunnen foto's worden aangemerkt als biometrische gegevens.

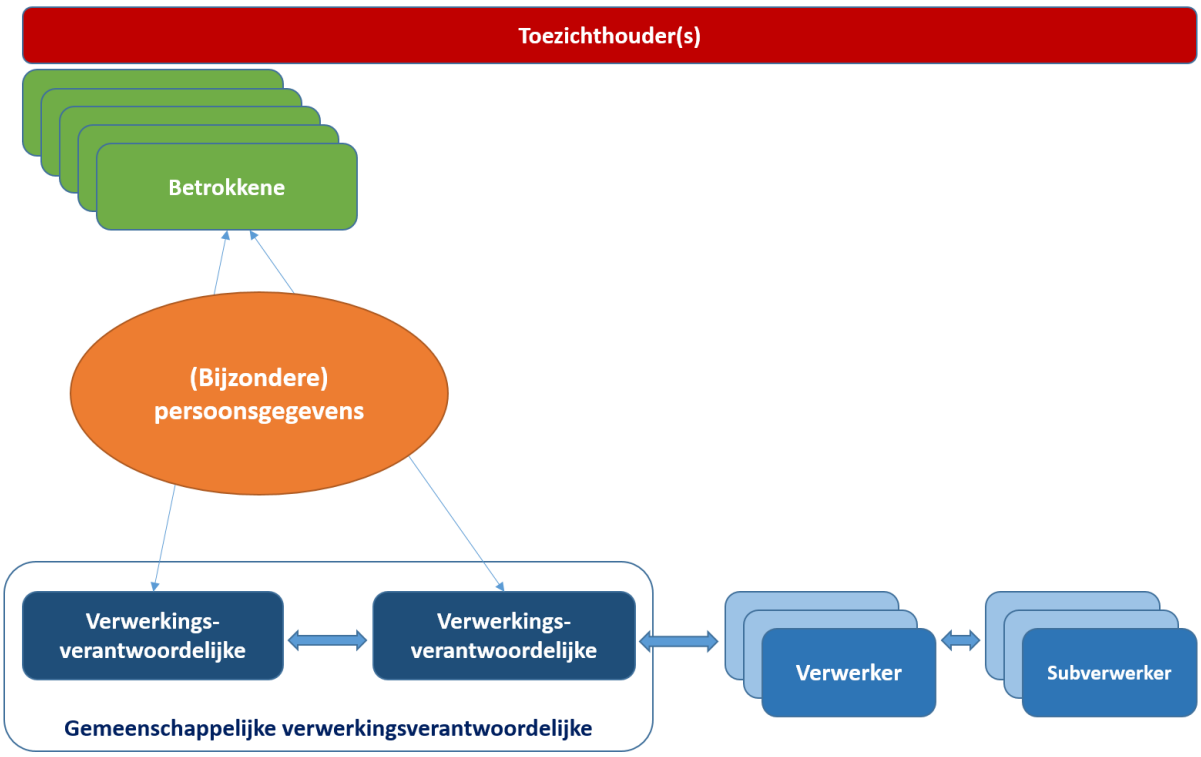
[21] Genetische gegevens zijn gegevens die betrekking hebben op iemands genen. Hieronder wordt onder andere verstaan het DNA van een persoon of materiaal waaruit informatie met betrekking tot het DNA kan worden afgeleid.
[22] Biometrische gegevens zijn exacte meetgegevens over personen, welk gegeven in meerdere of mindere mate de volgende eigenschappen bevat: universeel; uniek; en permanent. Hieronder wordt onder andere verstaan het netvlies, de iris, de vingerafdrukken, de geometrie van de handomtrek, gelaatsherkenning, de stem, het handschrift, de manier om zich voort te bewegen.
[23] Gegevens over de gezondheid zijn gegevens die betrekking hebben op de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

In beginsel is verwerking van bijzondere persoonsgegevens verboden, tenzij sprake is van in de wet benoemde uitzonderingen. De belangrijkste uitzonderingen zijn dat:

- Betrokkene toestemming heeft gegeven;
- Verwerking noodzakelijk is voor de uitvoering van verplichtingen en uitoefening van specifieke rechten op het gebied van het arbeidsrecht en sociale zekerheidsrecht en sociale beschermingsrecht;
- Verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene;
- De gegevens openbaar zijn gemaakt;
- De verwerking noodzakelijk is voor de instelling, uitoefening of verdediging van een rechtsvordering;
- De verwerking noodzakelijk is voor doelen van preventieve of arbeidsgeneeskunde, voor beoordeling van arbeidsgeschiktheid, medische diagnosen, verstrekken van gezondheidszorg of sociale diensten.

4.3 DE BELANGRIJKSTE PARTIJEN

De belangrijkste partijen die [**art, 4, AVG**] onderkent zijn:



Afbeelding 4: Betrokken partijen en relatie tot elkaar

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Het is mogelijk dat in bepaalde gevallen de wetgever aangeeft wie verwerkingsverantwoordelijke is voor een bepaalde verwerking van persoonsgegevens.

Verwerker: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Als een verwerker de doeleinden en middelen van een verwerking bepaalt, wordt deze organisatie als verwerkingsverantwoordelijke beschouwd, met de daarmee samenhangende verplichtingen.

Subverwerker: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat ten behoeve van de verwerker persoonsgegevens verwerkt.

Toezichthoudende autoriteit: een door een lidstaat ingestelde onafhankelijke overheidsinstantie. Voor Nederland is dat de Autoriteit Persoonsgegevens (AP).

De wet onderkent ook nog een **Ontvanger** en een **Derde**. Dit zijn partijen in de vorm van een natuurlijk persoon of rechtspersoon, een overheidsinstantie, of een dienst of een ander orgaan - niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken - aan wie/waaraan persoonsgegevens worden verstrekt.

De feitelijke activiteiten die deze partijen met de persoonsgegevens ontplooien, maakt of zij in het kader van de verwerking kwalificeren voor de rol van **Verwerkingsverantwoordelijke** of **Verwerker**, met de daarbij behorende verplichtingen. Een voorbeeld is een universiteit die gebruik maakt van de onderzoeksgegevens van een andere universiteit en deze gegevens verder verwerkt / gebruikt.

4.4 DE VERWERKING VAN PERSOONSGEGEVENS

De verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens [**art. 4, AVG**].

EISEN AAN DE VERWERKING

Persoonsgegevens moeten [**art. 5, lid 1, AVG**]:

- worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (**rechtmatigheid, behoorlijkheid en transparantie**);
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt;
- toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (**minimale gegevensverwerking**);
- juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (**juistheid**);
- worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is;
- door het nemen van **passende technische of organisatorische maatregelen** op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (**integriteit en vertrouwelijkheid**).

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze eisen en moet dit kunnen aantonen (**verantwoordingsplicht**) [**art. 5, lid 2, AVG**].

PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

In de AVG is niet in detail uitgewerkt wat onder passende technische en organisatorische maatregelen moet worden verstaan. Wel heeft het CBP (nu AP) eerder in een publicatie met betrekking tot de Wbp aangegeven wat onder een passend niveau van beveiliging moet worden verstaan [**CBP-2**] en [**CBP-4**]. Dit niveau van beveiliging vormt ook de basis voor een eerder in samenwerking met de NBA en NOREA ontwikkeld normenkader,

dat nog steeds als toetsingskader wordt gehanteerd bij het uitvoeren van assurance-opdrachten, waarbij wordt nagegaan of een organisatie voldoet aan de privacywet[24]. Dit normenkader en de inmiddels gepubliceerde aanvulling daarop als gevolg van de AVG [**NOREA-3**], is door de onderzoekers meegenomen bij het formulieren van de maatregelen en procedures die de MKB-accountant moet treffen.

In de AVG zijn wel een aantal bepalingen opgenomen, die direct betrekking hebben op wat naar de mening van de wetgever passende technische of organisatorische maatregelen zijn.

Een belangwekkend artikel betreft art. 24 van de AVG. In lid 1. wordt bepaald dat: "*Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.*"

Passend gegevensbeschermingsbeleid: In [**art. 24, AVG**] wordt aangegeven dat de organisatie beschikt over een "*passend gegevensbeschermingsbeleid*".

Privacy by design en **Privacy by default**: De wetgever heeft in de AVG Privacy by design en Privacy by default als verplichte uitgangspunten genomen en verwacht dat met deze uitgangspunten bij de inrichting van processen en beveiliging rekening wordt gehouden [**art. 25, lid 1, AVG**].

- **Privacy by design** houdt in dat er al bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens goed worden beschermd.
- **Privacy by default** houdt in dat technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat, als standaard, alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel dat moet worden bereikt. Bijvoorbeeld door:
    - een app die wordt aangeboden niet de locatie van gebruikers registreert als dat niet nodig is;
    - op een website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf wordt aangevinkt;
    - als iemand zich op een nieuwsbrief wil abonneren niet meer gegevens worden gevraagd dan nodig is.

De wetgever verwacht dat de verwerkingsverantwoordelijke (maar ook de verwerker) van het begin af aan overwegingen met betrekking tot de privacy betrekt bij het opstellen van nieuw beleid of het ontwerp van nieuwe systemen met betrekking tot de verwerking van persoonsgegevens.

In dit kader passen het toepassen van pseudonimiseren en anonimiseren. Zie voor een nadere toelichting [**4.2**]

Stand van de techniek, uitvoeringskosten en risico's: De wetgever verwacht dat bij het inrichten van de beveiliging rekening wordt gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen [**art. 32, lid 1, AVG**]. Een op het risico afgestemd beveiligingsniveau omvat onder meer:

- pseudonimiseren en versleuteling (encryptie) van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

[24] https://www.privacy-audit-proof.nl/

- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Risicoanalyse is vereist: Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig, hetgeen met name tot lichamelijke, materiële of immateriële schade kan leiden, zoals discriminatie, identiteitsdiefstal of -fraude, financiële verliezen of reputatieschade. Teneinde de veiligheid te waarborgen en te voorkomen dat de verwerking inbreuk maakt op de verordening, dient de verwerkingsverantwoordelijke of de verwerker de aan de verwerking inherente risico's te beoordelen en maatregelen, zoals versleuteling, te treffen om die risico's te beperken.

Alleen toegang in opdracht: De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt. Dit geldt ook voor medewerkers of derde partijen die in opdracht van de verwerkingsverantwoordelijke en/of de verwerker diensten leveren in het kader van de informatiebeveiliging. Denk hierbij aan computercrisisteams (computer emergency response teams), computercalamiteitenteams (computer security incident response teams), aanbieders van elektronische communicatienetwerken en -diensten en aanbieders van beveiligingstechnologie en -diensten.

Naleving moet kunnen worden aangetoond: Om de naleving van deze verordening aan te kunnen tonen, moet de verwerkingsverantwoordelijke interne beleidsmaatregelen nemen en maatregelen toepassen die voldoen aan met name de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen. Het aansluiten bij een goedgekeurde **gedragscode** of **goedgekeurd certificeringsmechanisme** wordt door de AVG aangegeven als een mogelijkheid om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen [**art. 24, lid, AVG**].

Deze bepaling is voor MKB-accountants zéér essentieel, omdat de klanten zich genoodzaakt zullen voelen (wettelijk verplicht) om schriftelijke garanties van de MKB-accountant te vragen. Volgens art. 28, lid 1 moet de MKB-accountant (als verwerker) garanties afgeven waarin wordt verklaard dat passende technische en organisatorische maatregelen worden toegepast die waarborgen dat de verwerking aan de vereisten van deze verordening voldoet en dat de bescherming van de rechten van de betrokkene is gewaarborgd.

Producten ook verantwoordelijk: Bij de ontwikkeling, de uitwerking, de keuze en het gebruik van toepassingen, diensten en producten die zijn gebaseerd op de verwerking van persoonsgegevens, of die persoonsgegevens verwerken bij de uitvoering van hun opdracht, dienen de producenten van de producten, diensten en toepassingen te worden gestimuleerd om bij de ontwikkeling en de uitwerking van dergelijke producten, diensten en toepassingen rekening te houden met het recht op bescherming van persoonsgegevens en, met inachtneming van de stand van de techniek, erop toe te zien dat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming. De beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen moeten ook bij openbare aanbestedingen in aanmerking worden genomen.

Privacy Impact Assessment: Bij nieuwe verwerkingen moet een ‘gegevensbeschermingseffectbeoordeling’, ook wel Privacy Impact Assessment (PIA) genoemd, worden uitgevoerd. Zie verder [**4.10**].

RECHTMATIGHEID VAN DE VERWERKING

De verwerking is alleen rechtmatig indien en voor zover ten minste aan één van de onderstaande voorwaarden is voldaan [**art. 6, lid 1, AVG**]:

Toestemming van de betrokkene: Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge

verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt. Hiertoe zou kunnen behoren het klikken op een vakje bij een bezoek aan een internetwebsite, het selecteren van technische instellingen voor diensten van de informatiemaatschappij of een andere verklaring of een andere handeling waaruit in dit verband duidelijk blijkt dat de betrokkene instemt met de voorgestelde verwerking van zijn persoonsgegevens.

Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit, mag derhalve niet als toestemming gelden. Dus actieve **Opt-in**, geen systeem van **Opt-out**.

De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend. Indien de betrokkene zijn toestemming moet geven na een verzoek via elektronische middelen, dient dat verzoek duidelijk en beknopt te zijn en niet onnodig storend voor het gebruik van de dienst in kwestie. Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven ervan [**art. 7, AVG**]. Wanneer sprake is van een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, is de verwerking van persoonsgegevens van een kind rechtmatig wanneer het kind ten minste 16 jaar is. Wanneer het kind jonger is dan 16 jaar is zulke verwerking slechts rechtmatig indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt [**art. 8, AVG**].

Verwerking in het kader van een overeenkomst: De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.

Verwerking in het kader van een wettelijke verplichting: de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust. Voorbeeld is de bepaling in de WWFT met betrekking tot het uitvoeren van een klantenonderzoek;

Verwerking in het kader van vitale belangen: de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen. Een voorbeeld is wanneer de verwerking noodzakelijk is voor humanitaire doeleinden, onder meer voor het monitoren van een epidemie en de verspreiding daarvan [**overweging 46, AVG**];

Verwerking in het kader van een algemeen belang: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

Verwerking in het kader van gerechtvaardigde belangen: de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

4.5 RECHTEN VAN DE BETROKKENE

De betrokkene heeft de volgende rechten:

Recht op transparante informatie en duidelijke communicatie [**art. 12, AVG**]: De verwerkingsverantwoordelijke:

- neemt passende maatregelen opdat de betrokkene de gevraagde informatie[25] in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is. De informatie wordt schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen, verstrekt. Indien de betrokkene daarom verzoekt, kan de informatie mondeling worden meegedeeld, op voorwaarde dat de identiteit van de betrokkene is vastgesteld;
- faciliteert de uitoefening van de rechten van de betrokkene;
- verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van zijn verzoek informatie over het gevolg dat aan zijn verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.

Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

Wanneer de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, deelt hij deze laatste onverwijld en uiterlijk binnen één maand na ontvangst van het verzoek mee waarom het verzoek zonder gevolg is gebleven, en informeert hij hem over de mogelijkheid om klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen.

Het verstrekken van informatie aan de betrokkenen geschiedt kosteloos. Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de verwerkingsverantwoordelijke ofwel:

- een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan; ofwel
- weigeren gevolg te geven aan het verzoek.

Het is aan de verwerkingsverantwoordelijke om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

De verwerkingsverantwoordelijke mag wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon (betrokkenen) die het verzoek indient, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

De aan betrokkenen verstrekte informatie mag worden verstrekt met gebruikmaking van gestandaardiseerde iconen, om de betrokkene een nuttig overzicht, in een goed zichtbare, begrijpelijke en duidelijk leesbare vorm, van de voorgenomen verwerking te bieden. Wanneer de iconen elektronisch worden weergegeven, zijn ze machine leesbaar.

De verwerkingsverantwoordelijke verstrekt de informatie:

- binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
- indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
- indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

[25] Betreft de communicatie met betrekking tot de rechten van betrokkenen, zoals aangegeven in de artikelen 13 t/m 22 en artikel 34 AVG

Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als eerder genoemde.

Het verstrekken van de eerder genoemde informatie is niet noodzakelijk wanneer en voor zover:

- de betrokkene reeds over de informatie beschikt;
- het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen;
- het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven aan een door wetgever aangewezen partij, of;
- de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lidstatelijke recht, waaronder een statutaire geheimhoudingsplicht.

Te verstrekken informatie:

- wanneer persoonsgegevens bij de betrokkene worden verzameld [**art. 13, AVG**]: Zie in dit verband de opsomming opgenomen in [**II: H-3];**
- wanneer de persoonsgegevens **niet** van de betrokkene zijn verkregen [**art. 14, AVG**]. Zie in dit verband de opsomming opgenomen in [**II: H-3]**.

Recht van inzage [**art. 15, AVG**]: De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen in die persoonsgegevens, aan wie verstrekt of door wie verwerkt en onder welke voorwaarden.

Recht op rectificatie [**art. 16, AVG**]: De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. De verwerkingsverantwoordelijke stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie of het verwijderen van zijn persoonsgegevens of beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

Recht op beperking van de verwerking [**art. 18, AVG**]: De betrokkene heeft het recht de verwerking door een verwerkingsverantwoordelijke te beperken indien sprake is van een van de volgende situaties:

- de juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren;
- de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
- de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

Recht op vergetelheid [**art. 17, AVG**]: De betrokkene heeft het recht dat de verwerkingsverantwoordelijke zonder onredelijke vertraging op zijn verzoek zijn persoonsgegevens verwijdert en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te verwijderen wanneer sprake is van een van de volgende situaties:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;

- de betrokkene zijn toestemming waarop de verwerking berust heeft ingetrokken en er geen andere rechtsgrond voor de verwerking is;
- de betrokkene maakt bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking;
- de persoonsgegevens zijn onrechtmatig verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan een in de wet opgenomen wettelijke verplichting die op de verwerkingsverantwoordelijke rust.

Recht op overdraagbaarheid van gegevens [**art. 20, AVG**]: De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt.

Recht op bezwaar: De betrokkene heeft het recht bewaar te maken wanneer zijn persoonsgegevens:

- worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft [**art. 22, AVG**];
- ten behoeve van direct marketing worden verwerkt, met inbegrip van profilering die betrekking heeft op direct marketing [**art. 21, AVG**].

Recht op kennisgeving aan een ontvanger [**art. 19, AVG**]: De verwerkingsverantwoordelijke stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie of verwijdering van persoonsgegevens of beperking van de verwerking overeenkomstig artikel 16, artikel 17, lid 1, en artikel 18, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

4.6 VERPLICHTINGEN VAN DE VERWERKINGSVERANTWOORDELIJKE

In de AVG beperkt de wetgever zich bij de formulering van de eisen die aan de verwerkingsverantwoordelijke worden gesteld tot de hoofdlijnen [**art. 24, AVG**]. Een nadere uitwerking vindt feitelijk plaats in de artikelen die betrekking op de verwerker [**art. 28, AVG**] en de beveiliging van de verwerking [**art. 32, AVG**].

Hierdoor komt de verantwoordelijkheid voor het treffen van ‘passende maatregelen’ ten volle bij zowel de verwerkingsverantwoordelijke, als bij (sub)verwerker(s) te liggen. De verwerkingsverantwoordelijke is (eind)verantwoordelijk voor de verwerking, ook als (delen van) de verwerking zijn uitbesteed aan een (sub)verwerker. Het is aan de verwerkingsverantwoordelijke om zorg te dragen dat bij uitbesteding de verwerker (en eventueel subverwerkers) aan hun verplichtingen voldoen. In deze uitwerking moeten de eisen aan de verwerkingsverantwoordelijke in samenhang worden bezien met de eisen aan de verwerker [**4.7**]. Dit vereist contractuele vastleggingen met betrekking tot de gegevens, de verwerkingen en de beveiliging, alsmede het kunnen aantonen daarvan.

Behalve het in opzet en bestaan regelen van die ‘passende maatregelen’ wordt ook gevraagd om aan te tonen dat deze doorlopend effectief zijn geweest. Hiermee verdwijnen bekende en vertrouwde accountantsbegrippen als ‘materialiteit, ‘x % betrouwbaarheid’, ‘steekproef’, ‘redelijke mate van zekerheid’ of ‘negative assurance’ op de achtergrond. Immers indien een inbreuk heeft plaatsgevonden die tot een schadeclaim van de betrokkene leidt of kan leiden, bestaat er geen zekerheid dat die ook is gedetecteerd bij toepassing van de genoemde begrippen. De risk based benadering van de accountant wordt in de wet vervangen door accountability, wat impliceert dat je moet kunnen verantwoorden over alle uitgevoerde verwerkingen. Zie voor een nadere toelichting Register van verwerkingsactiviteiten [**4.8**].

BEVEILIGING VAN DE VERWERKING

De verwerkingsverantwoordelijke is verplicht passende en effectieve technische en organisatorische maatregelen te treffen, om [**art. 24, lid 1 en overweging 074, AVG**]:

- te waarborgen en te kunnen aantonen dat elke verwerking in overeenstemming met de verordening wordt uitgevoerd;
- ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan.

De maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd.

De verantwoordelijkheid en aansprakelijkheid van de verwerkingsverantwoordelijke moeten worden vastgesteld voor elke verwerking van persoonsgegevens die door of namens hem wordt uitgevoerd.

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene.

Zie verder ook de toelichting op wat passende beveiliging is [**4.4**].

GEBRUIK VAN EEN (SUB)VERWERKER

Wanneer een verwerkingsverantwoordelijke voor de verwerking van persoonsgegeven gebruik maakt van de diensten van een verwerker, doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden, opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd en dit ook kan worden aangetoond. Van verwerking door een verwerker is bijvoorbeeld sprake bij het verwerken van persoonsgegevens in de Cloud of bij externe hosting van een website waar persoonsgegevens worden verwerkt [**art. 28, lid 1, AVG**].

De verwerking door een verwerker moet worden geregeld in een overeenkomst die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Voor de inhoud van een verwerkersovereenkomst [**II: H-4**].

Na de voltooiing van de verwerking ten behoeve van de verwerkingsverantwoordelijke, dient de verwerker, naargelang de wens van de verwerkingsverantwoordelijke, de persoonsgegevens terug te geven of te wissen, tenzij een wettelijke bepaling die op verwerker van toepassing is de verplichting oplegt de persoonsgegevens op te slaan.

MELDEN VAN EEN DATALEK

De verwerkingsverantwoordelijke is verplicht een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, te melden aan de bevoegde toezichthoudende autoriteit (en de betrokkene), tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Nadere informatie over hoe te handelen bij het optreden van een datalek is aangegeven in [**4.9**].

REGISTER VAN VERWERKINGSACTIVITEITEN

De verwerkingsverantwoordelijke houdt een register bij van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden [**art. 30, lid 1, AVG**].

Deze verplichting geldt niet voor of organisaties die minder dan 250 personen in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of het de verwerking van bijzondere persoonsgegevens betreft. Een voorbeeld kan zijn grootschalige verwerking van persoonsgegevens, zoals salarissen of medische gegevens in een situatie waarin het MKB-kantoor deze verwerkingen voor zijn werknemers uitvoert.

In het kader van het kunnen aantonen van de naleving van de verordening AVG is het ook voor kleine organisaties van belang om een register van verwerkingsactiviteiten bij te houden [**overweging 082, AVG**]. Zie verder [**4.8**] en [**II: H-5**].

4.7 VERPLICHTINGEN VAN DE (SUB)VERWERKER

BEVEILIGING VAN DE VERWERKING

Op grond van de verplichting aan de verwerkingsverantwoordelijk moet de verwerker, die in opdracht van een verwerkingsverantwoordelijke een verwerking uitvoert, in staat zijn om afdoende garanties te bieden met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd en dit kan worden aangetoond. [**art. 28, AVG**]. Zie verder ook de toelichting op wat passende beveiliging is [**4.4**].

VERWERKERSOVEREENKOMST

De verwerking door een (sub)verwerker moet worden geregeld in een overeenkomst [**art. 28, lid 3, AVG**] die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Voor de inhoud van een verwerkersovereenkomst [**II: H-4**].

SUBVERWERKING

De verwerker maakt geen gebruik van de diensten een subverwerker zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke [**art. 28, lid 2, AVG**].

In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

Wanneer een verwerker gebruik maakt van de diensten van een subverwerker om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in de overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in deze verordening voldoet [**art. 28, lid 4, AVG**].

Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker. Voor de inhoud van een verwerkersovereenkomst [**II: H-4**].

MELDEN VAN EEN DATALEK

De (sub)verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens. Nadere informatie over hoe te handelen bij het optreden van een datalek is aangegeven in [**4.9**].

REGISTER VAN VERWERKINGSACTIVITEITEN

De verwerker houdt een register bij van alle categorieën van verwerkingsactiviteiten die hij in opdracht van een verwerkingsverantwoordelijke heeft verricht [**art. 30, lid 2, AVG**].

Deze verplichting geldt niet voor of organisaties die minder dan 250 personen in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking van bijzondere persoonsgegevens betreft. Een voorbeeld kan zijn grootschalige verwerking van persoonsgegevens, zoals salarissen of medische gegevens in een situatie waarin het MKB-kantoor deze verwerkingen voor zijn klanten uitvoert of zijn klanten als service-provider de mogelijkheid biedt deze verwerkingen zelf uit te voeren met behulp van 'zijn' software.

In het kader van het kunnen aantonen van de naleving van de verordening AVG is het ook voor kleine organisaties van belang om een register van verwerkingen bij te houden [**overweging 082, AVG**]. Zie verder [**4.8**] en [**II: H-5**].

4.8 REGISTER VAN VERWERKINGSACTIVITEITEN

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 [**art. 30, AVG**].

Een register van verwerkingsactiviteiten heeft tot doel inzicht te geven in de verwerkingen waarvoor een verwerkingsverantwoordelijke / verwerker verantwoordelijk is, en biedt de mogelijkheid om de naleving van de AVG aan te tonen. Vooral om deze reden adviseren de onderzoeker MKB-kantoren om een register van verwerkingsactiviteiten bij te houden.

Het register bestaat uit een schriftelijke registratie, elektronisch is ook toegestaan [**art. 30, lid 3, AVG**]. Voor de gegevens die moeten worden vastgelegd, zie [**II: H-5**].

De verwerkingsverantwoordelijke / (sub)verwerker kunnen het register, in voorkomend geval, in het kader van het aantonen van compliance met de AVG, ter beschikking stellen van de toezichthoudende autoriteit [**art. 30, lid 4, AVG**].

In het geval van de verwerkingsverantwoordelijke spreekt de AVG over een register waarin de verwerkingsactiviteiten worden bijgehouden die onder zijn verantwoordelijkheid plaatsvinden [**art. 30, lid 1, AVG**]. Het register kan in dat geval gezien worden als een vastlegging / beschrijving van de administratieve organisatie van een bedrijf. Voor de gegevens die moeten worden vastgelegd, zie [**II: H-5**].

Van de verwerker wordt verwacht dat deze een register bijhoudt van alle categorieën van verwerkingsactiviteiten die hij in opdracht van een verwerkingsverantwoordelijke heeft verricht [**art. 30, lid 2, AVG**]. Deze eis wordt niet aan de verwerkingsverantwoordelijke gesteld, maar een vorm van registratie van uitgevoerde verwerkingen is wel nodig om naleving achteraf te kunnen aantonen.

De vraag dringt zich dan op, op welke wijze deze bewijslast kan worden ingevuld. De registratie van verwerkingsactiviteiten leidt in combinatie met de ketenverantwoordelijkheden tot een uitbreiding van die vastleggingen, met dynamisch onderhoud, tot alle partijen die bepaalde verwerkingen verrichten. Dit heeft een grote impact op de uitwisseling van gegevens en vraagt op zich weer om een contractuele basis.

De verplichtingen van de verwerkingsverantwoordelijke / verwerker zijn dus verstrekkend en daarmee worden alle subverwerkers ook direct medeverantwoordelijk in de keten.

Om in de breedte aan deze eisen te kunnen voldoen, staat het MKB-kantoor voor de vraag of dit zelfstandig kan worden georganiseerd of dat voor deze gegevensuitwisseling en registratie van verwerkingsactiviteiten gebruik gemaakt moet worden van externe partijen, die deze netwerken en gerelateerde verwerkersovereenkomsten dynamisch onderhouden.

In de AVG wordt de mogelijkheid van een gedragscode aangegeven als een mogelijkheid de aantoonbaarheid te organiseren. Een opgestelde en door de AP goedgekeurde gedragscode wordt dan algemeen verbindend voor de actoren binnen de keten voor die verwerking. Partijen die zich aansluiten bij de gedragscode geven daarmee aan in opzet en bestaan de benodigde maatregelen te hebben getroffen [**overweging 98, AVG**]. Naleving van de gedragscode kan plaatvinden door een vorm van certificering waarbij de werking van de in de gedragscode aangegeven maatregelen en procedures wordt beoordeeld. Voorbeelden daarvan onder de huidige wet (Wbp) zijn beschikbaar op [**NOREA-1**].

Het gebruik van een gedragscode door een sector / branche kan ondersteund worden door het gebruik van een Trusted Third Party (TTP als betrouwbare derde partij) om deze gedragscode geautomatiseerd te controleren[26]. Dergelijke partijen kunnen een certificaat afgeven waaruit blijkt dat alle relevante informatie is vastgelegd in een bedrijfsdossier. Hiermee wordt expliciet gemaakt dat het MKB-kantoor ‘accountable’ is voor contractspartijen waar diensten aan worden geleverd en worden afgenomen.

4.9 HET MELDEN VAN EEN DATALEK

In de AVG is de verplichting om een inbreuk in verband met persoonsgegevens te melden aan de toezichthouder en in sommige gevallen ook aan de betrokkenen opgenomen in de artikelen 33 en 34, AVG.

Zodra de Uitvoeringswet AVG in werking treedt, vervalt de huidige meldplicht datalekken die in de Wbp is opgenomen.

Vooruitlopend op het inwerkingtreden van de Uitvoeringswet gaan wij in dit rapport wel uit van de bepalingen in de AVG. De AVG stelt wel strengere eisen aan de registratie van de datalekken die zich in de organisatie hebben voorgedaan. **Alle datalekken** moeten worden gedocumenteerd. Met deze documentatie moet de AP kunnen controleren of de organisatie aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht, die alleen betrekking heeft op de gemelde datalekken.

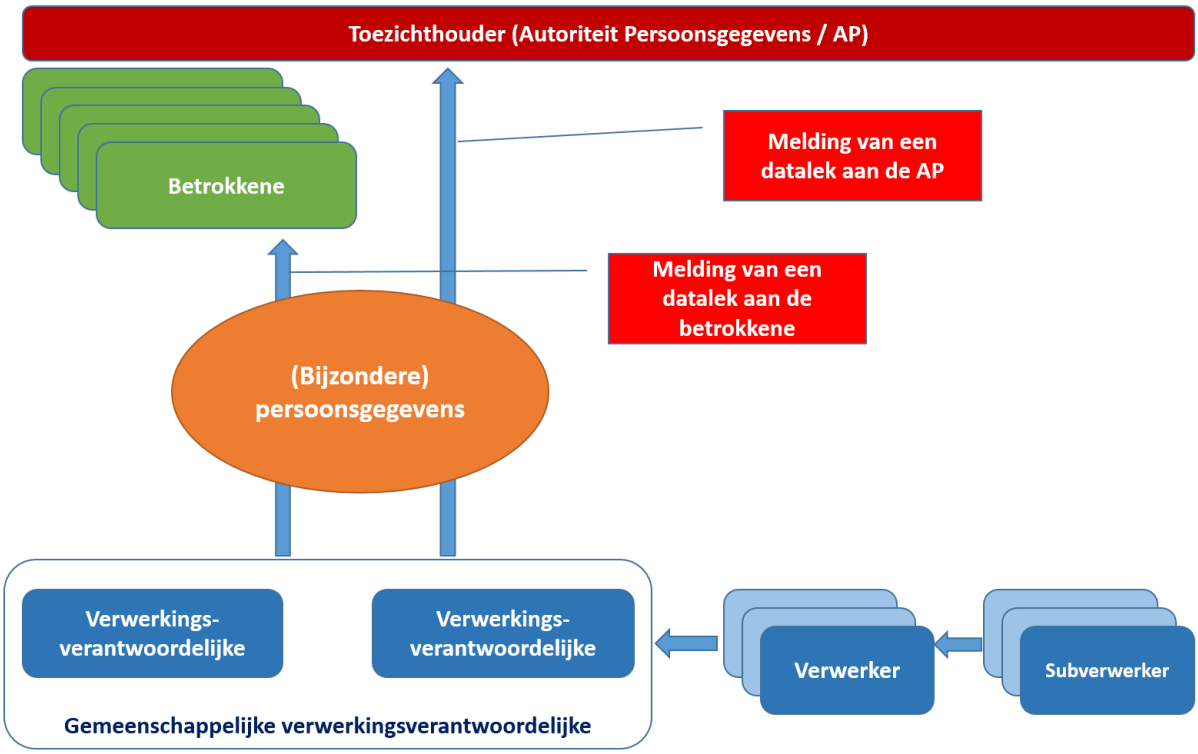
Omdat de meldplicht in de AVG vergelijkbaar is met de huidige meldplicht, is in de onderstaande beschrijving van de belangrijkste bepalingen gebruik gemaakt van de guidance die de AP in het kader van de meldplicht datalekken heeft gepubliceerd [**AP-1**]. Uitgangspunt is hierbij de bepalingen van de AVG, die vervolgens op basis van de guidance van AP nader worden toegelicht en voorzien van praktische handvaten om invulling te kunnen geven aan de wettelijke verplichting(en).

Het proces van wel of niet melden bestaat uit een aantal stappen waarin een aantal beslissingen moeten worden genomen. Alvorens in te gaan op de verschillende stappen, kort welke partijen bij het melden zijn betrokken en wie doet wat.

[26] Technieken die hierbij van belang kan zijn: zoals “Smart contracts” of van “Sticky notes”

WIE MOET WAT MELDEN EN AAN WIE?

In onderstaande afbeelding zijn de betrokken partijen bij een melding visueel weergegeven.



Afbeelding 5: Betrokken partijen bij een melding van een inbreuk / datalek

De AVG stelt de volgende eisen aan de **verwerkingsverantwoordelijke** en aan de **verwerker** [**art. 33** en **34, AVG**]:

Als een **inbreuk** in verband met persoonsgegevens heeft plaatsgevonden, meldt de **verwerkingsverantwoordelijke** deze zonder onredelijke vertraging en, indien mogelijk, **uiterlijk 72 uur** nadat hij er kennis van heeft genomen, aan de **toezichthouder** (AP), tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

De **verwerker** informeert de **verwerkingsverantwoordelijke** zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

De **verwerkingsverantwoordelijke** documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthouder in staat de naleving van dit artikel te controleren.

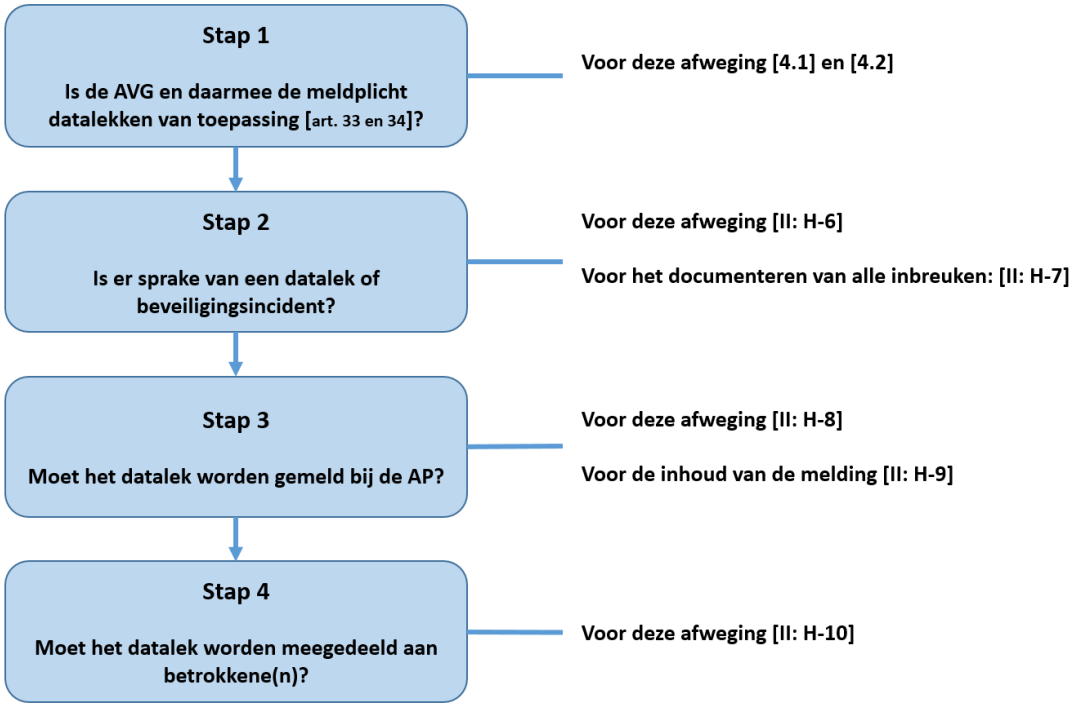
Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de **verwerkingsverantwoordelijke** de **betrokkene** de inbreuk in verband met persoonsgegevens onverwijld mee.

Wanneer een **verwerker** vaststelt dat de door hem aan de **verwerkingsverantwoordelijke** gemeld datalek niet leidt tot een melding bij de AP/ mededeling aan betrokkenen, zal hij in gesprek moeten gaan met verwerkingsverantwoordelijke. Wanneer de verwerker van mening is dat aanzienlijke schade kan worden voorkomen door een melding aan de AP en een mededeling aan betrokkene, kan hij besluiten om zelfstandig actie te ondernemen. Dit om zijn mogelijke aansprakelijkheid te beperken.

HET PROCES VAN MELDEN

Om invulling te kunnen geven aan de meldplicht van een datalek moeten verwerkingsverantwoordelijke en verwerker een aantal beslissingen nemen. In de volgende paragrafen is aangeven welke afwegingen moeten worden gemaakt en op welke wijze de beslissingen kunnen worden genomen. In **DEEL II** zijn een aantal beslissingstabellen opgenomen, alsmede voorbeelden van beveiligingsincidenten, die wel of niet aanleiding zijn voor een melding aan de AP en betrokkene(n).

Om te komen tot en melding aan de AP en mogelijk de betrokkenen moeten de volgende stappen worden gezet:



Afbeelding 6

STAP 1: IS DE AVG EN DAARMEE DE MELDPLICHT DATALEKKEN VAN TOEPASSING?

Vastgesteld moet worden of de AVG van toepassing en of er sprake is van verwerking van persoonsgegevens. In dit kader wordt verwezen naar [**4.1** en **4.2**].

STAP 2: IS SPRAKE VAN EEN DATALEK OF BEVELIGINGSINCIDENT?

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een **beveiligingsincident** moet bijvoorbeeld gedacht worden aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.

Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als een onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kan worden uitgesloten. Bij de afweging of sprake is van een datalek kan gebruik worden gemaakt van een beslissingstabel en nadere toelichting die is opgenomen in [**II: H-6**].

Als alleen sprake is van een zwakke plek in de beveiliging, wordt dat een beveiligingslek genoemd en niet een datalek. Bij een beveiligingslek behoeft geen melding te worden gedaan aan de AP. Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk.

Persoonsgegevens van gevoelige aard zijn bijvoorbeeld:

- Bijzondere persoonsgegeven;
- Gegevens over de financiële of economische situatie van de betrokkene, zoals gegevens over (problematische) schulden, salaris- en betalingsgegevens;
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, zoals gegevens over gokverslaving, prestaties op school of werk of relatieproblemen;
- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen;
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft, is het mogelijk dat een datalek moet worden gemeld waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

Registratie van inbreuken is verplicht: De verwerkingsverantwoordelijke en de verwerker **zijn verplicht** alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen te documenteren. Dus ook de inbreuken die niet zijn gemeld. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

In [**II: H-7**] is een overzicht opgenomen welke gegevens in het kader van een beveiligingsincident of datalek moeten worden gedocumenteerd.

De verwerkingsverantwoordelijke of de verwerker moeten alle schade vergoeden die iemand kan lijden ten gevolge van een verwerking die inbreuk maakt op zijn rechten. De verwerkingsverantwoordelijke of de verwerker moet van zijn aansprakelijkheid worden vrijgesteld indien deze kan aantonen dat hij niet verantwoordelijk is voor de schade. Het begrip ‘schade’ moet ruim worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen van de AVG. De betrokkenen dienen volledige en daadwerkelijke vergoeding van door hen geleden schade te ontvangen. Wanneer verwerkingsverantwoordelijken of verwerkers betrokken zijn bij dezelfde verwerking, dienen zij elk voor de volledige schade aansprakelijk te worden gehouden.

STAP 3: MOET HET DATALEK WORDEN GEMELD BIJ DE AP?

Bij de afweging of het datalek moet worden gemeld bij de AP kan gebruik worden gemaakt van een beslissingstabel en nadere toelichting die is opgenomen in [**II: H-8**].

Op de website van de AP is een webformulier beschikbaar, dat kan worden gebruikt voor een melding. Via dit webformulier kan de melding zo nodig worden aangevuld of ingetrokken.

In de **melding aan de AP** wordt ten minste het volgende omschreven of meegedeeld:

- de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;

- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

Een overzicht van de vragen die moeten worden beantwoord en de gegeven die moeten worden verstrekt, is opgenomen in [**II: H-9**].

STAP 4: MOET HET DATALEK WORDEN MEEGEDEELD AAN BETROKKENE(N)?

Als u tot de conclusie komt dat u als verwerkingsverantwoordelijke een datalek moet melden aan de AP, betekent dit niet automatisch dat u dit datalek ook moet melden aan de betrokkene. U moet hiervoor een aparte afweging maken. De wet geeft aan dat u een melding moet doen aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij moet u bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kunt u er in principe van uit gaan dat u het datalek niet alleen moet melden aan de AP.

Uw melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door, bijvoorbeeld, een gelekt wachtwoord te vervangen.

De wet schrijft voor dat u de melding onverwijld moet doen. U moet daarbij rekening houden met het feit dat de betrokkene naar aanleiding van uw melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder u de betrokkene daarover informeert, hoe eerder deze in actie kan komen.

De **melding aan de betrokkene** bevat een omschrijving, in duidelijke en eenvoudige taal, van:

- de aard van de inbreuk in verband met persoonsgegevens en;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Een melding aan betrokkene **is niet vereist** wanneer een van de volgende voorwaarden is vervuld:

- de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling (cryptografische bewerkingen zoals encryptie en hashing). U moet wel per geval bepalen of de maatregelen die u heeft genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten;
- de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
- de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de AP, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de eerder aangegeven voorwaarden, waarom niet behoeft te worden gemeld, is voldaan.

Bij de afweging of een datalek wel of niet aan een betrokkene moet worden gemeld, kan gebruik worden gemaakt van een beslissingstabel en nadere toelichting die is opgenomen in [**II: H-10**]. Hier is ook aangegeven op welke wijze en wanneer een datalek aan betrokkene kan worden gemeld.

4.10 PRIVACY IMPACT ASSESSMENT / PIA

WANNEER EEN PIA?

In [**art. 35, AVG**] is aangegeven dat wanneer een verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uitvoert van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. De AVG hanteert hiervoor het begrip 'gegevensbeschermingseffectbeoordeling', ook wel bekend onder de Engelse term Privacy Impact Assessment, afgekort PIA.

Een PIA is met name vereist in de volgende gevallen:

- een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering;
- bij grootschalige verwerking van bijzondere categorieën van persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafrechtelijke feiten);
- stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

De AP kan via openbaarmaking aangeven voor welke soort verwerkingen wel of geen PIA verplicht is.

De AVG geeft aan dat wanneer er een FG is aangewezen, de verwerkingsverantwoordelijke zijn advies inwint [**art. 35, lid 2, AVG**].

De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.

Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de PIA wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

Wanneer uit een PIA blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de AP [**art. 36, AVG**]. In dit artikel is ook aangegeven welke informatie de verwerkingsverantwoordelijke in dat geval moet aanleveren bij de AP.

Het blijft evenwel een abstracte normstelling, die in belangrijke mate door de verwerkingsverantwoordelijke zelf geïnterpreteerd zal moeten worden. Sinds 1 september 2013 is het uitvoeren van een PIA bij ontwikkeling van nieuwe wetgeving en systemen die zien op de verwerking van persoonsgegevens verplicht voor de rijksoverheid. Deze verplichting wordt bij het van kracht worden van de AVG uitgebreid naar het bedrijfsleven.

DE INHOUD VAN EEN PIA

Een PIA bevat ten minste:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

GEBRUIK VAN NIEUWE TECHNOLOGIEËN

In de AVG wordt expliciet aandacht besteed aan het gebruik van nieuwe technologieën bij het verwerken van persoonsgegevens. Van belang in een tijd waarin o.a. accountantskantoren, maar ook andere organisaties vormen van data-analytics (waaronder proces mining) inzetten in de controle of om klanten te ondersteunen bij het analyseren of optimaliseren van hun processen of het analyseren van data. In de praktijk worden dergelijke bewerkingen vaak door specialisten uitgevoerd, vaak ook in hun eigen (externe) omgeving, die ook buiten de EU kan liggen. Bij het inschakelen van derde partijen is in feite sprake van het gebruik van een subverwerker, waarbij de bepalingen gelden die de AVG aan het uitbesteden van de verwerking van persoonsgegevens stelt. Hoe gevoelig dit kan liggen is pijnlijk duidelijk geworden bij de Belastingdienst, waar de vraag werd gesteld of er data van belastingplichteigen buiten de omgeving van de Belastingdienst door derde partijen werd verwerkt.

In [**II: H-11**] is nadere informatie over een PIA opgenomen.

4.11 FUNCTIONARIS VOOR GEGEVENSBESCHERMING / FG

Organisaties zijn niet verplicht om een FG aan te stellen tenzij sprake is van een overheidsorganisatie of de verwerking van bijzondere persoonsgegevens. De aard van de verwerkingen, bijvoorbeeld van bijzondere persoonsgegevens, kan voor een MKB-kantoor reden zijn om een FG aan te stellen. Een andere belangrijke reden kan zijn dat door de aanstelling van een FG het MKB-kantoor aantoont dat het beschikt over de nodige expertise op het terrein van de privacywet en -bescherming. Dit betekent dan wel dat de FG-functie op adequate wijze moet zijn ingevuld.

Er zullen zich in de praktijk allerlei situaties voordoen, waarbij de expertise van een FG gewenst is. Bijvoorbeeld bij de invulling van de wettelijke bepalingen van de AVG, een nieuwe verwerking of de besluitvorming rond een beveiligingsincident / datalek. De wetgeving stelt kleinere organisaties in staat over een dergelijke functie/ expertise te beschikken in de vorm van een service, die op dit moment al door derde partijen in die vorm wordt aangeboden. Het niet hebben van een dergelijke functionaris / functie kan in het nadeel van de betrokken organisatie (verwerkingsverantwoordelijke / verwerker) werken in het geval dat een gedupeerde betrokkene een klacht neerlegt bij de AP en de desbetreffende organisatie moet aantonen dat zij niet beschikt over de benodigde deskundigheid, maar wel aan alle eisen van de AVG heeft voldaan.

Een FG kan een organisatie ook adviseren hoe om te gaan met verwerkingen, een PIA of een inbreuk / datalek. Om die reden adviseren de onderzoekers MKB-kantoren een dergelijke functie / voorziening te overwegen.

In de AVG zijn bepalingen opgenomen over de FG in [**art. 37, 38** en **39, AVG**].

WANNEER EEN FG?

De AVG verplicht organisaties in bepaalde gevallen een FG aan te stellen [**art. 37, AVG**].

POSITIE VAN DE FG

De AVG verwacht dat een FG [**art. 38, AVG**]:

- Tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens:
- De verwerkingsverantwoordelijke / verwerker ondersteunen door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid;
- Geen instructies ontvangt met betrekking tot de uitvoering van zijn taken;
- Niet ontslagen of gestraft wordt voor de uitvoering van zijn taken;
- Rechtstreeks verslag uitbrengt aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.

Betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening.

De FG is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.

De FG kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

TAKEN VAN DE FG

De FG vervult ten minste de volgende taken [**art. 39, AVG**]:

a. de verwerkingsverantwoordelijke / verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen;
b. toezien op naleving van de AVG en het beleid van de verwerkingsverantwoordelijke / verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
c. desgevraagd advies verstrekken met betrekking tot PIA's en toezien op de uitvoering;
d. samenwerken met en optreden als aanspreekpunt voor de AP.

De FG houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

5. INFORMATIEBEVEILIGING: HOE EN WAAROM?

In dit hoofdstuk wordt ingegaan op de aanpak van informatiebeveiliging[27], mede in het kader van de privacybescherming. Onderwerpen die aan de orde komen zijn:

- Het doel en het belang van informatiebeveiliging;
- Welke mogelijke beveiligingsmaatregelen kunnen worden getroffen;
- Risicoanalyse als basis voor het treffen van maatregelen;
- Hoe om te gaan met diensten van derden, zoals clouddiensten;
- Welke beveiligingsstandaarden en normenkaders zijn beschikbaar als basis voor te treffen beveiligingsmaatregelen.

Het hoofdstuk wordt afgesloten met actueel onderzoek naar (de impact van) cybercrime en de stand van zaken met betrekking tot privacybescherming en datalekken. Dit onderzoek geeft inzicht in mogelijke risico's en gebieden die (extra) aandacht behoeven.

5.1 DE AANPAK VAN INFORMATIEBEVEILIGING

Informatiebeveiliging omvat het geheel aan maatregelen waarmee organisaties hun informatie beveiligen. Het gaat daarbij om alle informatie die de organisatie verwerkt, zowel digitaal als niet digitaal. Organisaties hebben niet alleen informatie nodig om hun bedrijfsprocessen uit te voeren, maar ook om hun interne bedrijfsvoering bij te sturen en strategische beslissingen te nemen. De term 'informatiebeveiliging' wordt ook gebruikt voor het vakgebied dat zich bezighoudt met het beveiligen van informatie.

Informatiebeveiliging richt zich op het waarborgen van de betrouwbaarheid, bestaande uit **integriteit**, **beschikbaarheid** en **vertrouwelijkheid** van processen en data.

Naast de drie bovengenoemde aspecten, die betrekking hebben op de informatie en de verwerking ervan, wordt nog een vierde en een vijfde aspect onderkend, weten:

- **Beheersbaarheid**: Beheersbaarheid is de mate waarin het object (organisatie, systeem of proces) kan worden aangestuurd en/of bijgestuurd, zodat het object bij voortduring aan de daaraan gestelde eisen voldoet of kan voldoen. Beheersbaarheid is de verantwoordelijkheid van het management;
- **Controleerbaarheid**: Controleerbaarheid betreft de mogelijkheid om met voldoende zekerheid (achteraf) vast te kunnen stellen of wordt/is voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Informatiebeveiliging richt zich op de organisatie, de systemen en de processen met als doel deze, alsmede de verwerkte en opgeslagen data te beschermen tegen dreigingen die de integriteit, beschikbaarheid en vertrouwelijkheid kunnen aantasten, alsmede compliance.

Informatiebeveiliging is een managementverantwoordelijkheid waarin afwegingen worden gemaakt tussen de te bereiken doelen en risk appetite versus de te nemen maatregelen. Dit betreft een risk based benadering. De dwingende bepalingen in de AVG maken echter dat de ondernemer (MKB-accountant) beperkt worden in zijn keuzemogelijkheden, omdat hij passende maatregelen moeten treffen om de rechten van betrokkenen te kunnen waarborgen.

[27] De inhoud van dit hoofdstuk is mede gebaseerd op de beschrijving van informatiebeveiliging in de publicatie [**CBP-2**]

SOORTEN BEVEILIGINGSMAATREGELEN

In de praktijk zijn verschillende vormen van beveiligingsmaatregelen te onderscheiden. Onderstaand is een beknopt overzicht opgenomen. In [**II: H-12**] is een uitgebreid overzicht met toelichting opgenomen.

Maatregelen kunnen worden onderscheiden naar:

- hun soort (verschijningsvorm): organisatorische, fysieke (technische) en logische (softwarematige) maatregelen;
- hun doel en zijn gericht op een bepaald moment van de incidentencyclus: preventieve, detectieve, repressieve en correctieve maatregelen;
- hun plaats in de organisatie, systemen en processen: User, Application en General IT Controls.

HET NIVEAU VAN INFORMATIEBEVEILIGING

Het realiseren van een toereikende informatiebeveiliging is een complex vraagstuk omdat o.m.:

- Het een samenspel is van gebruikers, toepassingen (applicaties) en een technische infrastructuur[28];
- De mens de onzekere factor is en niet altijd conform procedures werkt;
- Onderling verschillende applicaties met elkaar moeten samenwerken;
- De uitvoering vaak bij verschillende partijen in verschillende ketens is belegd (van applicatieontwikkeling tot het gebruik van clouddiensten);
- Gegevens op verschillende locaties worden opgeslagen en verwerkt;
- De verschillende technische componenten (bijvoorbeeld servers, laptops of smartphones) een onderling verschillende bescherming van gegevens en applicaties bieden.

Daarom vraagt informatiebeveiliging om een gestructureerde aanpak die, vanwege de cybercrime-ontwikkelingen, periodiek moet worden uitgevoerd. De inrichting van informatiebeveiliging is gebaseerd op de Plan-Do-Check-Act-cyclus. Vervolgens geeft een risicoanalyse aan welke risico's moeten worden afgedekt om aan de betrouwbaarheidseisen te voldoen. Bij de keuze van maatregelen kan gebruik worden gemaakt van beveiligingsstandaarden.

Het treffen van maatregelen op basis van een risicoanalyse stelt de verantwoordelijke in staat om beargumenteerd passende maatregelen te treffen die een passend beveiligingsniveau garanderen. Een uitgebreide toelichting op het uitvoeren van een risicoanalyse is opgenomen in [**II: H-13**].

BEVEILIGINGSSTANDAARDEN & NORMEN-/BEHEERSINGSKADERS

Een risicoanalyse geeft aan welke risico's worden onderkend en maken besluiten over te treffen maatregelen om deze te kunnen beheersen mogelijk. Beveiligingsstandaarden en normenkaders geven houvast bij het daadwerkelijk treffen van passende maatregelen om de risico's af te dekken. Veel beveiligingsstandaarden bevatten ook een 'Basisset' of 'Baseline' aan maatregelen die in de meeste situaties noodzakelijk zijn om tot adequate beveiliging te komen. Beveiligingsstandaarden vormen een weerslag van de 'Lessons learned' die bij de beveiliging in een specifieke branche of in een specifieke technologische omgeving zijn opgedaan. Ze geven weer welke maatregelen door beveiligingsdeskundigen binnen de betreffende context in het algemeen als 'passend' worden beschouwd en, in het geval van de meer technisch gerichte standaarden, welke technologische middelen bij de beveiliging worden toegepast. Er worden ook regelmatig nieuwe beveiligingsstandaarden en nieuwe versies van bestaande beveiligingsstandaarden gepubliceerd, waarmee wordt aangesloten op de nieuwste ont-

[28] Apparatuur, besturingssystemen, database managementsystemen, netwerken

wikkelingen binnen het vakgebied. Correct gebruik van actuele beveiligingsstandaarden stelt de verantwoordelijke in staat om passende maatregelen te treffen en om tot een evenwichtig en effectief samenstel van organisatorische, fysieke en logische maatregelen te komen.

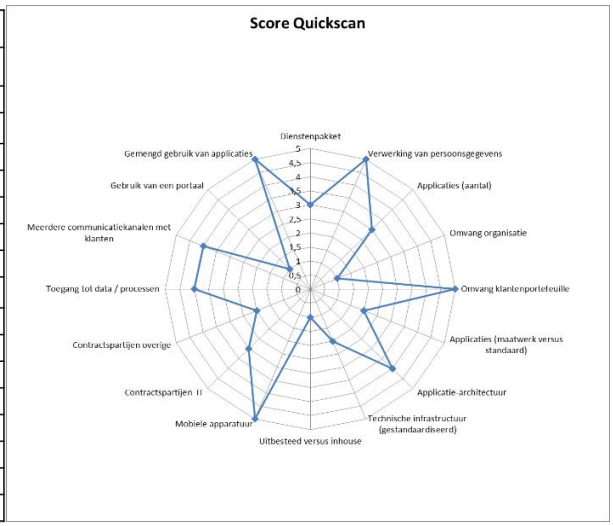
In [**II: H-14**] is een overzicht opgenomen van standaarden en normen-/beheersingskaders gericht op informatiebeveiliging en privacybescherming. Deze zijn bruikbaar in het kader van dit rapport en doelgroep (MKB) en bieden praktische handvaten bij de invulling van informatiebeveiliging en privacybescherming.

5.2 RISICOANALYSE VERSUS BASELINE BENADERING

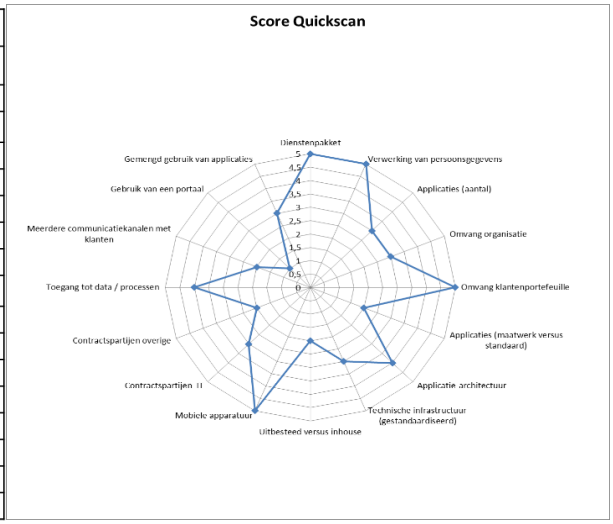
RISICOANALYSE EN QUICKSCAN

Om passende beveiligingsmaatregelen te kunnen nemen is het van belang inzicht te hebben op welke gebieden uw kantoor de grootste risico's loopt. Dit inzicht kan worden verkregen door het uitvoeren van een risicoanalyse. Omdat het uitvoeren van een risicoanalyse veel tijd in beslag kan nemen, kan als eerste stap gebruik worden gemaakt van een QuickScan. Dit met als doel een eerste indruk te krijgen welke gebieden als eerste aandacht nodig hebben en waar maatregelen direct effectief kunnen zijn. In onderstaande voorbeelden is per aandachtsgebied via een score van 1 (laag) t/m 5 (hoog) het risico (kans x verwachte schade) ingeschat dat ingeschat dat de organisatie loopt op verlies van data of verstoring van de bedrijfsvoering.

Aandachtgebieden	Scores (range) van mate van risico					Score
	Laag				Hoog	
	1	2	3	4	5	
Dienstenpakket	Beperkt				Uitgebreid	3
Verwerking van persoonsgegevens	Weinig tot geen				Veel	5
Applicaties (aantal)	Klein				Groot	3
Omvang organisatie	Klein				Groot	1
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	2
Uitbesteed versus inhouse	Uitbesteed				Inhouse	1
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	4
Gebruik van een portaal	Ja				Nee	1
Gemengd gebruik van applicaties	Nee				Ja	5



Aandachtgebieden	Scores (range) van mate van risico					Score
	Laag				Hoog	
	1	2	3	4	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 7: QuickScan

BASELINE BENADERING

Omdat het uitvoeren van een risicoanalyse in de praktijk, afhankelijk van de omvang en complexiteit van de organisatie en de processen en het IT-landschap, een aanzienlijke inspanning kan vragen van de organisatie en medewerkers, kan de organisatie ook kiezen voor de baseline benadering. Als start wordt een basisbeveiligingsniveau ingevoerd, 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.

Bij het opstellen van het Stappenplan [**7**] zijn de onderzoekers uitgegaan de baseline benadering en het beveiligingsbeleid, zoals onderstaand geformuleerd. Voorts is rekening gehouden met de oorzaken voor verlies/misbruik van data en verstoring van de bedrijfsvoering [**2.4** en **5.3**], in combinatie met de risico's van een MKB-kantoor en de dreigingen van cybercrime. Daarbij is gekozen voor de managementaanpak **Plan** >>>> **Do** >>>> **Check** >>>> **Act**.

Plan: Als basis voor de set van beveiligingsmaatregelen is uitgegaan van de Code voor Informatiebeveiliging ISO 27002 [**NEN-2**] en de Tactische Baseline Informatiebeveiliging van de gemeenten [**VNG-1**]. Voorts is een aantal activiteiten benoemd die de randvoorwaarden moeten scheppen voor de invoering van informatiebeveiliging en compliance met de privacywetgeving.

Do: De maatregelen zijn als acties geformuleerd, de technische invulling is afhankelijk van de organisatie en IT-omgeving van het MKB-kantoor. Het kan goed zijn dat specifieke IT-kennis noodzakelijk is voor het kunnen uitvoeren van de aangegeven acties en de te treffen maatregelen.

Check: Na invoering van deze set van maatregelen moet het kantoor op basis van opgedane ervaringen, evaluatie en een vorm van risicoanalyse nagaan of aanpassing of uitbreiding van maatregelen noodzakelijk is.

Act: Voorts wordt verwacht dat het functioneren wordt gemonitord en dat periodiek wordt nagegaan of aanpassing noodzakelijk is.

De maatregelen die op basis van (nieuwe) privacywetgeving noodzakelijk zijn, zijn direct ontleend aan deze wet. Hierbij is o.m. gebruik gemaakt van de guidance die door de AP in het kader van de invoering van de meldplicht datalekken per 1 januari 2016 [**AP-1**] en de geplande invoering van de AVG zijn ontwikkeld [**AP-2**].

5.3 DIENSTEN VAN DERDE PARTIJEN

Op dit moment zijn veel vormen van uitbesteding van IT-diensten of het gebruik de diensten van derde partijen, onder te brengen in het model van cloudcomputing waarin de verschillende dienstconcepten en toepassingsmodellen visueel zijn aangegeven.

De 'klassieke' uitbesteding van de verwerking en opslag van gegevens kwalificeert in dit model als een IaaS (Infrastructure as a Service) in de vorm van een Private Cloud. De uitbestedende partij blijft zelf verantwoordelijk voor het beheer en het onderhoud van de systemen, en dus ook de beveiliging daarvan, de clouddienstverlener levert alleen verwerkings- en opslagcapaciteit.

Zoals uit de analyse van het applicatie- en IT-landschap (Hoofdstuk 2) naar voren kwam, maken veel kantoren gebruik van Software as a Servic (SaaS) toepassingen, in de vorm van een Public Cloud. In dat geval is de cloudaanbieder verantwoordelijk voor de functionaliteit en het onderhoud en het beheer daarvan, maar ook voor de verwerking en opslag van de gegevens. De gebruiker (het MKB-kantoor) blijft wel verantwoordelijk voor wie toegang heeft tot de processen en de data. Bekend voorbeelden van een SaaS-toepassing zijn de boekhoudpakketten, zoals Exact Online, Reeleezee en AFAS.

Omdat de verschillende dienstenconcepten en toepassingsmodellen verschillende risico's en taak-/verantwoordelijkheidsverdeling tussen aanbieder en gebruiker met zich meebrengen, is het van belang dat het MKB-kantoor op de hoogte is van deze risico's en de onderlinge taak-/verantwoordelijkheidsverdeling. Dit om vast te kunnen stellen welke beveiligingsmaatregelen zijn organisatie zelf moet treffen, en welke maatregelen hij mag verwachten bij de derde partij. Meer informatie over cloudcomputing is opgenomen in de NBA-publicatie: De mkb-accountant en Cloud Computing [**NBA-12**].

In [**II: H-15**] is een uitgebreid overzicht opgenomen van de verschillende dienstconcepten en toepassingsmodellen, alsmede de daarbij behorende risico's.

Een manier om als gebruiker vooraf zicht te krijgen op de kwaliteit van een dienstverlener en zijn dienstverlening, is na te gaan of de derde partij beschikt over een vorm van certificering (ISO of Keurmerk Zeker-Online) van dienstverlening of dat periodiek een assurance-rapport kan worden overlegd. Voorbeelden van assurancerapporten en vormen van certificering zijn opgenomen in [**II: H-16**].

De AVG stelt echter hogere eisen aan de inzet van derde partijen. De derde partijen die betrokken zijn op de verwerking van persoonsgegevens zullen moeten voldoen aan alle eisen zoals die door de AVG aan verwerkers worden gesteld. Bij het gebruik maken van derde partijen moet rekening worden gehouden met het feit dat persoonsgegevens niet zonder waarborgen buiten de EU mogen worden verwerkt / opgeslagen. Voor verwerking / opslag in de US zijn afspraken gemaakt in het kader van het Privacy Shield.

5.4 OORZAKEN VERLIES/MISBRUIK DATA EN VERSTORING

Recent onderzoek naar cybercrime en privacy (non-compliance met regelgeving en datalekken) geeft inzicht in beveiligingsrisico's en mogelijke oorzaken. Voorts wordt duidelijk op welke punten organisaties nog te kort schieten en actie geboden is. Onderstaand is een samenvatting opgenomen die is gebaseerd op recent onderzoek; een overzicht van dit onderzoek en de belangrijkste uitkomsten is opgenomen in [**II: H-17**].

DE FACTOR MENS

De menselijke component van informatiebeveiliging kent een eigen dynamiek:

- **Gebrek aan kennis en capaciteit**: MKB-bedrijven hebben over het algemeen beperkte middelen en vaak een beperkt inzicht in de risico's die ze lopen, waardoor het in de praktijk moeilijk blijkt om tot een goed beveiligingsniveau te komen;
- **Te ruime of niet actuele autorisaties** waardoor meer medewerkers/derden dan strikt noodzakelijk (nog steeds) toegang hebben tot gegevens en processen/toepassingen;
- **Menselijk gedrag**:
    - De technologie alleen is vaak niet de oorzaak of de oplossing. De werknemer achter de laptop, pc of tablet is vaak de zwakste schakel (menselijk falen waardoor procedures niet worden nageleefd, wachtwoorden gedeeld, en de IT-infrastructuur niet goed wordt beheerd of beveiligd, of te weinig alert op mogelijk potentieel bedreigende situaties / voorvallen;
    - E-mail wordt nog steeds gezien als het meest gebruikte medium om ransomware te verspreiden, naast phishing-emails, waarmee gebruikers naar een valse (bank)website worden gelokt, om ze daar - nietsvermoedend - te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer of te verleiden tot het aanklikken van geïnfecteerde weblinks;
    - Het versturen van persoonsgegevens naar of afgegeven aan de verkeerde ontvanger of het per ongeluk publiceren van persoonsgegevens of aan verkeerde klant tonen op portaal;
    - Het kwijtraken van apparatuur, gegevensdragers (bijvoorbeeld USB-sticks) e/o papier door verlies, diefstal of verkeerd verzenden met de post;

- **Combinatie van zakelijk en privé**: Een probleem dat op IT-gebied werk en privé door elkaar lopen. Malware op de privé-computer of tablet kan ook de werkomgeving besmetten.

TECHNISCHE INFRASTRUCTUUR / APPLICATIELANDSCHAP

- **Basis beveiliging niet op orde**: Binnen het MKB is het risico aanwezig dat de basisbeveiliging niet op orde is (technisch falen waardoor kwaadwillende gebruik kunnen maken van de zwakte in de bescherming). Er worden geen sterke wachtwoorden gebruikt, beveiligingssoftware wordt onregelmatig geüpdatet, en er worden onvoldoende back-up's van belangrijke bestanden gemaakt, waardoor organisaties kwetsbaar zijn voor externe dreigingen, waaronder het gebruik van ransomeware (gijzelsoftware) die organisaties kunnen chanteren door data te versleutelen en deze pas na betaling vrij te geven.
- **Onvoldoende beveiligde IoT-apparatuur**: Door toepassing van apparaten (Internet of Things / IoT) die via internet kunnen worden bestuurd, kunnen criminelen toegang krijgen tot bedrijfsdata / persoonsgegevens en processen. Dit kan o.m. leiden tot verlies van data, verstoring van processen, het verspreiden van kwaadaardige software of identiteitsfraude.
- **Complexe configuraties** van hardwarecomponenten, software-oplossingen, en een diversiteit aan koppelingen. Software-oplossingen bestaan uit verschillende generaties, zijn deels zelf ontwikkeld, deels semi-standaard, deels componenten uit andere bronnen. Door dit geheel neemt de beheersbaarheid af en nemen de kansen op 'gaten' in de beveiliging toe.

OORZAKEN VAN DATALEKKEN (BRON: AP)

In 2016 heeft de AP 5.849 meldingen ontvangen. Dit jaar staat de teller al op 7.364.

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.

6. WAT BETEKENT DIT VOOR DE MKB-ACCOUNTANT?

In dit hoofdstuk wordt aangegeven welke zaken de MKB-accountant minimaal moet regelen om aan de verplichtingen van de nieuwe privacywet (AVG) te kunnen voldoen. Hierbij wordt ook ingegaan op de rol van de accountant in het kader van de AVG (verwerkingsverantwoordelijk en/of verwerker) en de daaruit voortvloeiende verplichtingen.

In dit hoofdstuk wordt ook een aantal uitgangspunten geformuleerd die de MKB-accountant kan hanteren bij het vormgeven van zijn beveiligingsbeleid. Bij het formuleren van deze uitgangspunten is rekening gehouden met de verplichtingen van de AVG, de belangrijkste kenmerken van een MKB-kantoor en de belangrijkste oorzaken voor verlies / misbruik van data en de verstoring van de bedrijfsvoering. Deze aspecten zijn gehanteerd bij de invulling van het Stappenplan, dat is opgenomen in [**7**]. Dit Stappenplan gaat uit van de 'Baseline' benadering en dekt de belangrijkste risico's af. Op basis van een eigen risicoanalyse kan de MKB-accountant vervolgens zelf nagaan welke aanvullende maatregelen nog nodig zijn om de informatiebeveiliging en interne beheersing op het voor zijn organisatie vereiste niveau te brengen.

6.1 WAT ZIJN DE GEVOLGEN VAN DE AVG

De AVG scherpt de al bestaande eisen van de Wbp aan, breidt deze uit en brengt deze op Europees niveau. De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacy-rechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De AVG geeft de toezichthouder, de AP, de bevoegdheid hoge boetes op te leggen[29]. Het (niet) melden van een datalek kan ook grote gevolgen hebben voor de reputatie of de waarde van een onderneming[30].

De AGV stelt in art. 24 stringente eisen aan de technische en organisatorische maatregelen [**4.4**]; deze dienen zodanig passend en effectief te zijn dat zij waarborgen dat de verantwoordelijke organisatie kan aantonen dat de verwerking van persoonsgegevens in overeenstemming met de verordening (*doorlopend*) wordt uitgevoerd en dat de persoonsgegevens ook nodig zijn voor het doel van de verwerking. Dit betekent dat de AVG een 'open' norm stelt die de organisatie zelf op niveau moet invullen.

In art. 28 van de AVG is bepaald dat een verwerking alleen mag worden uitbesteed aan een (sub)verwerker die afdoende garanties biedt dat passende technische en organisatorische maatregelen heeft getroffen, zodat de verwerking voldoet aan de eisen van de AVG en de rechten van betrokkene zijn gewaarborgd en dit ook kan worden aangetoond. Dit heeft het gevolg dat (potentiële) opdrachtgevers (klanten) alleen zaken mogen doen met MKB-accountants die zo'n garantie kunnen afgeven en dat de MKB-accountant verwerkingen alleen mag uitbesteden aan partijen die ook een dergelijke garantie kunnen afgeven. Dit is in de praktijk ook een zeer essentiële regel omdat in art. 82 AVG is bepaald dat "*Wanneer meerdere verwerkingsverantwoordelijken of verwerkers bij dezelfde verwerking betrokken zijn, en verantwoordelijk zijn voor schade die door verwerking is veroorzaakt, wordt elke verwerkingsverantwoordelijke of verwerker voor de gehele schade aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk wordt vergoed*".

Verder wordt in [**art. 28, AVG**] voorgeschreven dat de onderlinge relaties worden geregeld in een verwerkersovereenkomst [**4.6, 4.7** en **II: H-4**] waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, het niveau van beveiliging

[29] De AP kan organisaties na het van toepassing worden van de AVG sancties opleggen van maximaal 20 miljoen euro of 4% van de wereldwijde omzet, afhankelijk van welk bedrag het hoogste is.

[30] De waarde van de internetactiviteiten die Yahoo verkocht aan de telecomreus Verizon leverde 350 miljoen dollar (332 miljoen euro) minder op door enkele grote computerinbraken bij het technologiebedrijf Yahoo, Telegraaf/DFT: 21 februari 2017.

en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Hiermee worden de verantwoordelijkheden expliciet gemaakt.

Verwerkers hebben de plicht het nakomen van de in de overeenkomst vastgelegde verplichtingen aan te tonen. Dit kan door een onderzoek door de verwerkingsverantwoordelijke of een onafhankelijke auditor, die in opdracht van de verwerker / verwerkingsverantwoordelijke een onderzoek uitvoert.

In de nieuwe wet ligt de nadruk - meer dan nu - op de verantwoordelijkheid van organisaties om aan te kunnen aantonen dat zij zich aan de wet houden. Het kunnen aantonen van compliance met wet- en regelgeving is van groot belang in het geval dat een verwerkingsverantwoordelijke of (sub)verwerker door een betrokkene aansprakelijk wordt gesteld voor een inbreuk op zijn rechten, of door de toezichthouder een boete opgelegd krijgt. De verwerkingsverantwoordelijke of de (sub)verwerker kunnen van aansprakelijkheid worden vrijgesteld of zich tegen de boete verweren, als zij kunnen aantonen dat zij zich aan de wet hebben gehouden en dus niet verantwoordelijk zijn voor de geleden schade van betrokkene. Het beschikken over een FG [**4.11**] en een register van verwerkingsactiviteiten [**4.8**] zijn twee in het oog springende voorwaarden.

Een belangrijk punt voor accountants bij het invullen en naleven van de privacywetgeving is de werkelijke inhoud van de rol van de accountant als dienstverlener. De daadwerkelijke rol is bepalend of de accountant in het kader van de AVG optreedt als verwerkingsverantwoordelijke [**4.6**] dan wel als verwerker [**4.7**]. Dit onderscheid is van belang omdat de verwerkingsverantwoordelijke meer en directe verplichtingen heeft met betrekking tot de betrokkene(n) van wie hij persoonsgegevens verwerkt. De verwerker heeft beperktere verplichtingen jegens betrokkenen en heeft in principe alleen te maken met de verwerkingsverantwoordelijke als opdrachtgever voor de uitgevoerde verwerkingen. De verplichting tot het treffen van passende technische en organisatorische maatregelen om de persoonsgegevens toereikend te beschermen en de effectieve werking daarvan aan te kunnen tonen, geldt echter voor zowel de verwerkingsverantwoordelijke als de verwerker.

WAT BETEKENT DIT VOOR DE ACCOUNTANT

Om aan de eisen van de AVG te voldoen moet de MKB-accountant minimaal de volgende zaken geregeld hebben:

- Inzicht in zijn processen en bedrijfs- en persoonsgegevens die hij gebruikt / verwerkt / bewaart voor zijn dienstverlening en voor zijn eigen bedrijfsvoering. Dit ten behoeve van:
    - Het vaststellen of de AVG op zijn organisatie van toepassing is, en zo ja:
        - Het vaststellen van de rechtmatigheid van de verwerking (rechtmatige grondslag);
        - Na te gaan of zijn organisatie een FG moet aanstellen of deze functie nodig heeft;
        - Te bepalen of hij als dienstverlener verwerkingsverantwoordelijke e/o verwerker is.
- Een toereikende beveiliging (passende technische en organisatorische maatregelen), alsmede het kunnen aantonen van de effectieve werking daarvan.
- Schriftelijke afspraken met klanten en (sub)verwerkers over de beveiliging en verwerking van persoonsgegevens en het kunnen aantonen van het nakomen van deze afspraken; benoem expliciet de verantwoordelijkheden als verwerkingsverantwoordelijke of als (sub)verwerker.
- 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 / betrokkene(n).
- Procedures om als verwerker invulling te kunnen geven aan de meldingsplicht van een datalek aan de verwerkingsverantwoordelijke in de keten van verwerking.

- Procedures om als verwerkingsverantwoordelijke / verwerker een Privacy Impact Assessment / PIA uit te kunnen voeren bij nieuwe verwerkingen, bijvoorbeeld bij het gebruik van data-analyse.
- Bij het inrichten van processen en de beveiliging rekening houden met de verplichte uitgangspunten: Privacy by Design en by Default.
- Het als verwerkingsverantwoordelijke / verwerker inrichten en bijhouden van een register van verwerkingsactiviteiten (verplicht voor organisatie met meer dan 250 medewerkers).

Optioneel, niet verplicht door de AVG maar advies van de onderzoekers

- Het op vrijwillige basis inrichten bijhouden van een register van verwerkingsactiviteiten.
- Het opstellen van een gedragscode waarin is vastgelegd hoe om te gaan met gegevens binnen de eigen organisatie en in relatie met de klanten.

Nadere uitwerking in het stappenplan in hoofdstuk 7

In hoofdstuk 7 is uitwerkt welke stappen en activiteiten de MKB-accountant kan uitvoeren om te kunnen voldoen aan de eisen van informatiebeveiliging en privacybescherming. De voorgestelde aanpak is gebaseerd op de baseline aanpak. Waar van belang zijn verwijzingen opgenomen naar de regelgeving [**3** en **4**] en naar **DEEL II** waarin achtergrond- en detailinformatie, beslissingstabellen, beveiligingsstandaarden en normen-/beheersingskaders en nadere informatie over verplichtingen in het kader van de AVG zijn opgenomen.

ACCOUNTANT VERWERKINGSVERANTWOORDELIJKE OF VERWERKER

In deze paragraaf worden de rollen van de accountant (als ondernemer en als dienstverlener) getypeerd aan de hand van de karakteristieken van de verwerkingsverantwoordelijke en de verwerker. Hierbij is van belang dat het onderstaande betrekking heeft op de verwerking van persoonsgegevens, en dus niet op de verwerking / het gebruik van gegevens in algemene zin.

Verplichtingen van verwerkingsverantwoordelijke en verwerker

Dit onderscheid is van belang omdat de verwerkingsverantwoordelijk en verwerker op punten andere verplichtingen hebben, zoals in onderstaand overzicht is weergegeven.

Vv = Verwerkingsverantwoordelijke, **V** = Verwerker.

	Vv	V
Bepaalt het doel en de middelen voor de verwerking van persoonsgegevens.	**X**	
Verwerkt persoonsgegevens in opdracht / ten behoeve van een 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 Privacy Impact Assessment (PIA) 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**

	Vv	V
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 een nadere toelichting, zie [**4.8**].	X	X
Beschikt over een functionaris voor gegevensbescherming (FG). Voor een nadere toelichting, zie [**4.11**].	X	X
Meldt een datalek bij de Autoriteit Persoonsgegevens (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

Verwerkingsverantwoordelijke versus verwerker

Onderstaande toelichting (op hoofdlijnen) is gebaseerd op overleg tussen de NBA en AP dat, mede op verzoek van de onderzoekers, op 15 november 2017 heeft plaatsgevonden. In dat overleg is afgesproken dat de NBA nadere guidance omtrent dit onderwerp zal afstemmen met de AP en op de NBA-website plaatsen. De verwachting is dat dit eind 2017, begin 2018 zal plaatsvinden. Tevens zal de NBA nadere informatie verstrekken over met klanten te maken afspraken en te gebruiken modelovereenkomsten.

Vooruitlopend hierop onderstaand overzicht, waarbij is uitgegaan van de meest voorkomende diensten / werkzaamheden van een MKB-kantoor.

Wat zegt de AVG over verwerkingsverantwoordelijke / verwerker?

De bepalingen in de AVG die van belang zijn in het kader van de rol van verwerkingsverantwoordelijke of verwerker zijn:

- **Definities** [**art. 4, AVG**]:
    - **Verwerkingsverantwoordelijke**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, **het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt**.
    - **Verwerker**: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
    - **Subverwerker**: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat ten behoeve van de verwerker persoonsgegevens verwerkt.
- **Doel en middelen** [**art. 28, lid 10, AVG**]: in dit artikel is bepaald dat als een verwerker de doeleinden en/of middelen van een verwerking bepaalt, deze organisatie als verwerkingsverantwoordelijke wordt beschouwd, met de daarmee samenhangende verplichtingen.

- **Uitbesteding van werkzaamheden** [**art. 28, lid 3, AVG**]: in dit artikel is met betrekking tot het uitbesteden van een verwerking aan een derde (verwerker) aangegeven dat de verwerking door een verwerker wordt geregeld in een **overeenkomst** die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin **het onderwerp** en **de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens** en **de categorieën van betrokkenen,** en **de rechten en verplichtingen van de verwerkingsverantwoordelijke** worden omschreven. Die overeenkomst bepaalt met name dat de verwerker de persoonsgegevens **uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke**.

Interpretatie van het standpunt van de AP

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 in de praktijk dat zijn verantwoordelijkheid bij de uitvoering van bepaalde werkzaamheden (verwerkingen) minder ver strekt dan die van zijn klant als het gaat om rechten van betrokkenen.

Naar de mening van de AP moet de accountant, in het geval hij in zelfstandigheid en onafhankelijkheid werkzaamheden uitvoert, 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,**
- **en de informatie die uit deze verwerking(en) voortvloeit in de vorm van opdrachtdocumentatie / controle-informatie**.

In het geval dat zich een datalek voordoet met betrekking tot de persoonsgegevens die de accountant van de klant heeft ontvangen (**A**), meldt de accountant dit datalek bij de klant. Het is aan de klant om als verwerkingsverantwoordelijke dit datalek te melden bij de AP en indien noodzakelijk de betrokkene te informeren.
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 betrokkene.

Als de accountant in opdracht van de klant louter uitvoerende werkzaamheden uitvoert, zoals het verwerken van salarissen, het bijhouden van administraties, het opstellen van een fiscale aangifte of het invullen van formulieren, is hij in het kader van de AVG **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. In het geval dat de klant als verwerkingsverantwoordelijke persoonsgegevens verstrekt, mag de accountant van de klant desgevraagd verlangen dat deze kan aantonen dat sprake is van een rechtmatige grondslag. De accountant legt de verantwoordelijkheid voor de rechtmatige grondslag voor de verwerking van persoonsgegevens vast in afspraken met de klant (verwerkingsverantwoordelijke). Als er geen sprake is van een rechtmatige grondslag kan dat betekenen dat de accountant de gevraagde dienst niet kan leveren.

Het voorgaande resulteert in het volgende overzicht.

1. De accountant is **verwerkingsverantwoordelijke** voor de verwerkingen waarvoor hij doel en 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 [**MINFIN-1**];

- het als **ondernemer / dienstverlener** verzamelen van de 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;
   - Het invullen van aanvragen, formulieren, etc.
3. De accountant is **verwerkingsverantwoordelijke (contextuele verantwoordelijkheid)** voor de verwerkingen van persoonsgegevens die in opdracht van de klant (verwerkingsverantwoordelijke) worden uitgevoerd, maar waarbij de accountant niet het doel maar wel de middelen bepaalt. Voorbeelden zijn:
   - Het samenstellen van een jaarrekening[31];
   - Het beoordelen of controleren van een jaarrekening;
   - Het uitvoeren van een assurance-opdracht;
   - Advisering of consultancy;
   - Het uitvoeren van een bijzondere opdracht.

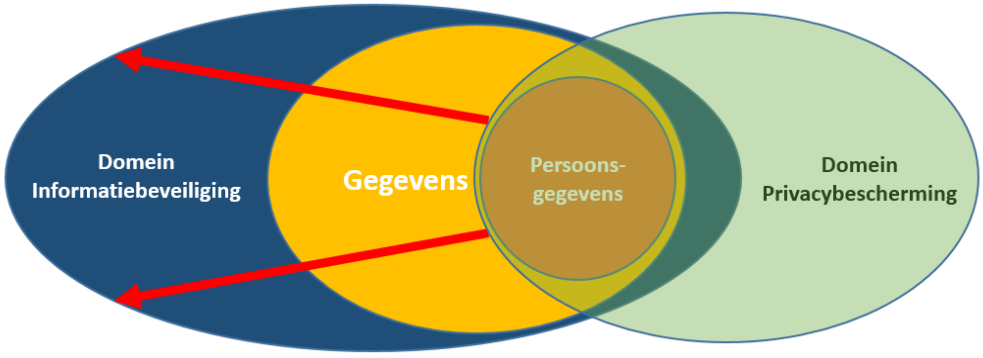
De feitelijke situatie is dus bepalend of de MKB-accountant wordt aangemerkt als **verwerkingsverantwoordelijke** of als **verwerker.** Hierbij geldt voor de MKB-accountant de bijzonderheid dat zijn rol in de situatie ad. 3 als verwerkingsverantwoordelijke bepaald wordt in de context van zijn werkzaamheden. Zijn rol is beperkt 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/haar rechten.

6.2 INFORMATIEBEVEILIGING VERSUS PRIVACYBESCHERMING

Informatiebeveiliging omvat het geheel aan maatregelen waarmee organisaties hun informatie (gegevens), maar ook processen beveiligen. Deze maatregelen zijn gericht op het waarborgen van de betrouwbaarheid, bestaande uit integriteit, continuïteit en vertrouwelijkheid.

De privacywetgeving richt zich specifiek op persoonsgegevens, waarbij de eis tot beveiligen (passende technische en organisatorische maatregelen) overeenkomt met de doelstelling van informatiebeveiliging. Daarnaast stelt de privacywet eisen aan het gebruik (verkrijgen, verwerken, bewaren, etc.) van de persoonsgegevens, alsmede eisen met betrekking tot het eerbiedigen van de rechten van betrokkene (de eigenaar van de persoonsgegevens), alsmede hoe te handelen bij inbreuken en datalekken. Genoemde relatie is onderstaand visueel weergegeven.

[31] Deze werkzaamheden zijn vooralsnog onder de situatie ad. 3 geplaatst, gezien het zelfstandige karakter van de werkzaamheden van de accountant bij het uitvoeren van deze dienst. Om te kunnen bepalen of de accountant bij de uitvoering van deze werkzaamheden mogelijk toch kan worden beschouwd als verwerker, heeft de AP aan de NBA nadere informatie gevraagd over deze vorm van dienstverlening en de daarbij uit te voeren activiteiten (verwerkingen). In de nadere guidance die de NBA over de rol van de accountant nog op de NBA-website zal plaatsen, zal hierover duidelijkheid worden verstrekt.

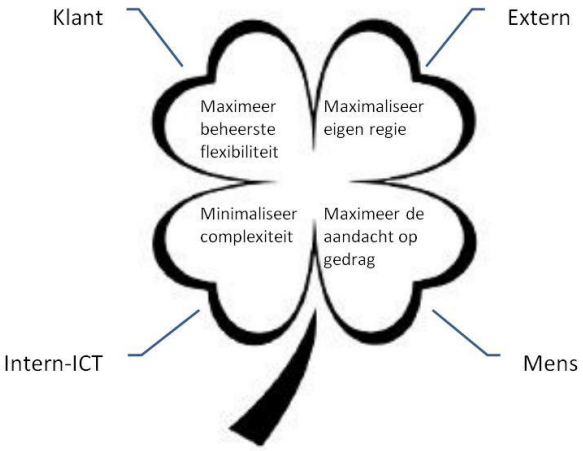


Afbeelding 8: Relatie informatiebeveiliging versus privacybescherming met de uitstralende werking van de AVG op de informatiebeveiliging

In bovenstaande afbeelding is zichtbaar dat een goede informatiebeveiliging een voorwaarde is voor het kunnen realiseren van een goede privacybescherming die voldoet aan de verplichtingen van de AVG. De twee genoemde domeinen - informatiebeveiliging en privacybescherming - komen dan ook tot uiting in het Stappenplan en het overzicht van de te treffen maatregelen.

6.3 UITGANGSPUNTEN BEVEILIGINGSBELEID

Bij de invulling van het Stappenplan en de keuze van de maatregelen hebben wij de volgende 'Leading principles' gehanteerd. Deze principes zullen in elke situatie (omvang van de MKB-organisatie, diversiteit van dienstverlening, etc.) tot een specifieke invulling van het stappenplan (set van maatregelen) leiden.



Afbeelding 9: Beveiligingsklavertje vier

Maximaliseer eigen regie

- Neem initiatief door verantwoordelijkheden binnen de organisatie (bestuur, FG) en met partijen (klanten / opdrachtgevers en verwerkers) expliciet te maken;
- Inventariseer de gevolgen van de AVG voor uw organisatie;
- Leg afspraken over gegevens, verwerkingen en verantwoordelijkheden vast;
- Creëer een eigen IT-accounting dat de basis vormt voor de verantwoording dat alle waarborgen effectief zijn gebleken.

Maximeer beheerste flexibiliteit

- Vertaal de flexibiliteit van dienstverlening naar klanten in beheersbare bedrijfsvoering door maximale automatisering;

- Standaardiseer de klantoplossingen maximaal met behoud van keuzevrijheden (vergelijking: de ruime keuzemogelijkheden van standaard auto's die het idee van maatwerk geven).

Minimaliseer complexiteit

- Pas 'Need to know' toe voor alle partijen (medewerkers, klanten, dienstverleners) in het verlenen van bevoegdheden. Voorkom overtollige of tegenstrijdige bevoegdheden die tot inbreuken kunnen leiden;
- Reduceer complexiteit in de informatievoorziening door de beste oplossing voor het geheel te kiezen en niet alleen de beste deeloplossing. Het geheel van de beste deeloplossingen kan voor een hoge mate van complexiteit en dus voor management (lees: privacy) problemen zorgen;
- Wees selectief in creatieve tijdelijke oplossingen, deze blijken vaak zeer structurele vormen aan te nemen;
- Minimaliseer de opgeslagen persoonsgegevens omdat persoonsgegevens alleen mogen worden verwerkt als er een grondslag voor is, of, in aanvulling, wanneer er toestemming van de betrokkene is. Deze gegevens mogen alleen verwerkt worden met betrekking tot het doel waarvoor ze verkregen zijn, voorkom 'bijvangsten' aan gegevens die onbedoeld/ongewenst tot extra verplichtingen leiden. Dit vraagt om de nodige beheersingsmaatregelen.

Maximeer de aandacht op gedrag

- Stimuleer actief, bewust, verantwoordelijk en alert gedrag, omdat de 'mens' in vele gevallen de zwakste schakel is in het geheel van beheersingsoplossingen;
- Zorg ervoor dat de relevante mensen in de organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels en op de hoogte blijven.

7. STAPPENPLAN EN TE TREFFEN MAATREGELEN

In dit hoofdstuk wordt de MKB-accountant een concrete aanpak aangeboden als eerste stap om te kunnen voldoen aan de eisen van informatiebeveiliging en privacybescherming. De voorgestelde aanpak is gebaseerd op de baseline aanpak. Deze resulteert in een uitgewerkt **Stappenplan** en een **voorstel voor te treffen maatregelen** gericht op informatiebeveiliging en privacybescherming, incl. compliance. Waar van belang zijn verwijzingen opgenomen naar de regelgeving [**3** en **4**] en naar **DEEL II** waarin achtergrond- en detailinformatie, beslissingstabellen, beveiligingsstandaarden en normen-/beheersingskaders en nadere informatie over verplichtingen in het kader van de AVG zijn opgenomen.

Bij de invulling van het **Stappenplan** is uitgegaan van de belangrijkste oorzaken voor verlies/misbruik van data en verstoring van de bedrijfsvoering, zoals aangegeven in [**5.4**] en [**II: H-17**]. Voorts is rekening gehouden met de belangrijkste kenmerken van een MKB-kantoor met betrekking tot cybercrime en non-compliance met regelgeving [**2** en **II: H-1**].

Het stappenplan bestaat uit 6 hoofdstappen, met een aantal substappen. Per stap is een aantal te treffen maatregelen aangegeven.

ZZP'ER VERSUS EENMANS- / MEERMANSPRAKTIJK

De AVG houdt geen rekening met de omvang van organisaties. Bepalend is of een organisatie persoonsgegevens verwerkt. De wijze waarop een kantoor invulling geeft aan de wettelijke verplichtingen, kan wel per kantoor verschillen.

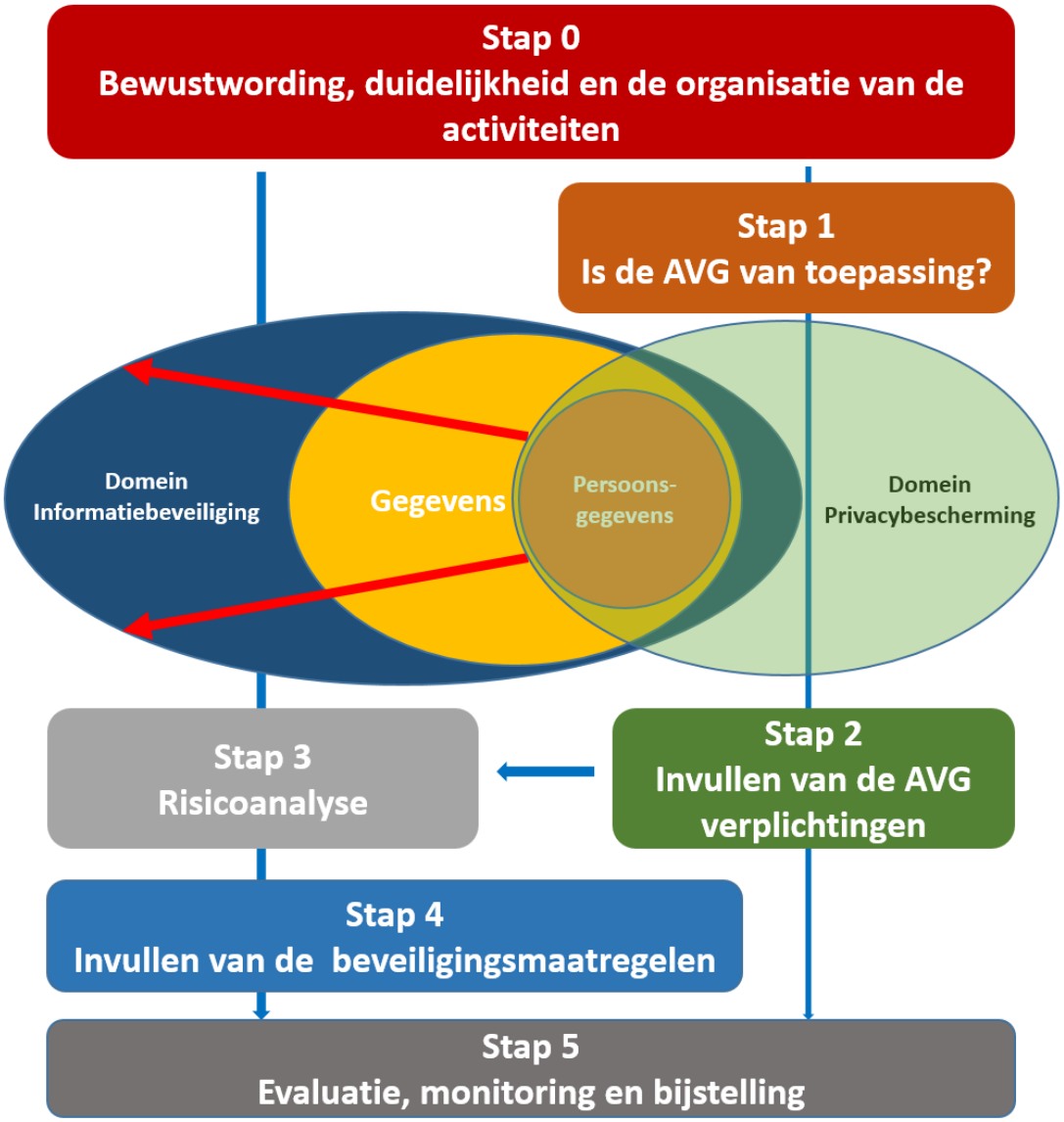
De aanduiding MKB-accountant kent verschillende verschijningsvormen: een zelfstandige zonder personeel (Zzp'er), een eenmanspraktijk (één AA of RA met een aantal medewerkers), of een meermanspraktijk (meerdere AA's e/o RA's met medewerkers). Een Zzp'er heeft geen medewerkers waarmee moet worden overlegd, afspraken gemaakt en waarvan gedrag gemonitord. Een Zzp'er en waarschijnlijk ook een eenmanspraktijk zullen vaak gebruik maken van de diensten van derde partijen bij de invulling / ondersteuning van hun dienstverlening (denk hierbij aan serviceproviders voor de invulling van IT-ondersteuning). Grotere kantoren geven waarschijnlijk 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 gebruik maken van de diensten van (gespecialiseerde) derde partijen kan de belasting voor een kantoor verlichten, wat wel betekent dat afspraken moeten worden vastgelegd in overeenkomsten en de naleving gemonitord en vastgesteld.

In organisaties met medewerkers zullen aanpassingen in de informatiebeveiliging en het doorvoeren van maatregelen in het kader van de AVG om een meer project georiënteerde aanpak vragen. Maar het is uiteindelijk aan de verantwoordelijke(n) voor de organisatie welk keuzes worden gemaakt.

Bij het formuleren van het stappenplan zijn de onderzoekers uitgegaan van een kantoor met medewerkers. Een Zzp'er hoeft geen projectorganisatie op te zetten, naar ook deze zal een projectmatige aanpak moeten hanteren om overzicht te houden en efficiënt te kunnen werken.

Op verzoek van de opdrachtgever (NEMACC) is in stappenplan aangegeven welke activiteiten zeker op zeer korte termijn moeten worden uitgevoerd (indien nodig); deze zijn gekenmerkt met een: 



Afbeelding 10: Stappenplan

Stap 0: Zorg voor bewustwording, duidelijkheid en de organisatie van de activiteiten

Deze stap is vooral van belang voor kantoren met medewerkers. Medewerkers zullen moeten worden geïnformeerd over de implicaties van de privacywet en over uw plannen / activiteiten met betrekking tot informatiebeveiliging en privacybescherming. Dit om het management onder meer te verzekeren van hun actieve betrokkenheid en medewerking.

In deze stap past ook dat de leiding van de organisatie het beveiligings- en privacy-beleid formuleert. Hierin wordt aangegeven aan welke eisen de organisatie moet voldoen en op welke wijze de organisatie daar invulling aan geeft, alsmede wat van de medewerkers wordt verwacht. Zie in dit verband [**6.4**]. Dit beleid en de keuzes die daarin worden gemaakt, komen onder meer tot uiting in een gedragscode en de te nemen maatregelen.

Dergelijke activiteiten worden veelal in een projectvorm uitgevoerd, waarbij meerdere partijen betrokken zijn, zoals IT, HR, Juridische zaken, Compliance, alsmede contractspartijen, en natuurlijk klanten. Hierbij van belang dat de verantwoordelijkheid voor het project duidelijk is en het project over de benodigde middelen (financieel en personeel) kan beschikken om de noodzakelijke activiteiten uit te voeren.

Stap	Maatregel	Verwijzing	
0	**Bewustwording, duidelijkheid en organisatie van de activiteiten**		
0.1	Benoem op bestuurlijk niveau een verantwoordelijke voor de informatiebeveiliging van het kantoor.	[**NEN-2**][32]	
0.2	Benoem op bestuurlijk niveau een verantwoordelijke voor de inrichting en compliance met betrekking tot privacybescherming.		
0.3	Informeer uw medewerkers over uw plannen met betrekking tot informatiebeveiliging en privacybescherming en verzeker u van hun actieve betrokkenheid en medewerking. Houd hen periodiek op de hoogte van de vorderingen. Zorg ook dat zij op de hoogte zijn van de verplichtingen van de (nieuwe) privacywet en voorkomende cybercrime dreigingen en datalekken.	[**AP-2**]	
0.4	Start een project om voor 25 mei 2018 gereed te zijn voor het van kracht worden van de AVG. Dit vereist betrokkenheid van de medewerkers, de ondersteunende diensten, zoals IT, HR, Juridische zaken, Compliance, alsmede de medewerking van contractspartijen, incl. klanten.	[**AP-2**]	
0.5	Zorg dat het project over de benodigde middelen (financieel en personeel) kan beschikken om de noodzakelijke activiteiten uit te voeren		
0.6	Formuleer de uitgangspunten voor het beveiligings- en privacy-beleid waarin de leiding van de organisatie aangeeft aan welke eisen de organisatie moet voldoen en op welke wijze de organisatie daar invulling aan geeft, alsmede wat van de medewerkers wordt verwacht.	[**NEN-2**] [**NEN-2**]	

Stap 1: Is de AVG op uw organisatie van toepassing?

De eerste en belangrijkste vraag die de accountant in het kader van de AVG moet beantwoorden is of er in zijn organisatie sprake is van verwerking van persoonsgegevens. Indien dit het geval is moet de accountant voor deze verwerking(en) rekening houden met de bepalingen van de AVG.

Om deze vraag te kunnen beantwoorden is inzicht nodig in de verwerkingen en de daarbij behorende persoonsgegeven, die onder zijn verantwoordelijkheid, al dan niet opdracht van andere partijen - kan zijn klanten - plaatsvinden. Hierbij moet ook de rechtmatigheid van de verwerking worden vastgesteld (de rechtmatige grondslag).

De accountant moet nagaan of zijn organisatie een FG moet aanstellen. Als dat niet het geval is kan de accountant overwegen om toch een dergelijke functionaris te benoemen of op een andere wijze in deze functie te voorzien. Zie verder [**2.9**].

Een vraag die de accountant moet beantwoorden is of hij/zij als dienstverlener in het kader van de AVG gezien moet worden als verwerkingsverantwoordelijke e/o verwerker. De rol bepaalt welke maatregelen hij/zij in die rol met betrekking tot de desbetreffende verwerking(en) / persoonsgegevens moet nemen. Zie in dit verband [**6.1**].

[32] NEN-2 is de meest actuele ISO standaard (2015) gericht op de inrichting van informatiebeveiliging. Deze standaard is echter niet gratis beschikbaar. Wel gratis beschikbaar is de Tactische-Baseline-Informatiebeveiliging Nederlandse gemeenten (BIG) [VNG-2], waarin de vorige versie van NEN-2 (2005 / 2007) is opgenomen.

Stap	Maatregel	Verwijzing	
1	**Het uitvoeren van een aantal inventarisaties**		
1.1	Breng in kaart: • het huidige dienstenpakket; • de verwerkingen die daarbij worden uitgevoerd; • de daarbij gebruikte / te gebruiken bedrijfs- en persoonsgegevens; • de daarbij te gebruiken applicaties, waar deze gegevens zijn opgeslagen en; • welke medewerkers en derde partijen toegang hebben tot deze gegevens. Deze informatie is o.m. nodig om de verwerkingen te kunnen beschrijven (Register van verwerkingsactiviteiten) alsmede het kunnen maken van de verplichte afspraken met klanten en (sub)verwerkers.		
1.2	Benoem een FG of voorzie op andere wijze in de benodigde privacy en juridische kennis door het invullen van deze functie door samenwerking met andere organisaties of door gebruik te maken van de diensten van een derde partij. Derde partijen bieden een dergelijke functie in de vorm van een service aan. Een FG is niet vanzelfsprekend de Compliance-Officer, die verantwoordelijk is voor de compliance in het kader van de gedrags- en beroepsregels.	[**4.11**]	
1.3	Stel vast welke rol u als (MKB-)accountant in het kader van de AVG vervult bij de bij 1.1 geïnventariseerde verwerkingen (verwerkingsverantwoordelijk of verwerker). Deze informatie is nodig om in het kader van de dienstverlening met klanten / (sub)verwerkers de juiste afspraken te kunnen maken.	[**6.1**]	
1.4	Stel een overzicht van de (persoons)gegevens op: • gesplitst naar bijzondere persoonsgegevens, persoonsgegevens en overige gegevens; • de verwerkingen waar die (persoons)gegevens worden gebruikt; • de wijze van vastlegging en locatie van vastlegging; • de (logische) samenhang van de verschillende gegevens (data-architectuur).		
1.5	Breng het huidige IT- en applicatielandschap in kaart, incl. de diensten die door derde partijen (serviceproviders en sub-serviceproviders) worden geleverd. Mede in verband van het kunnen maken van afspraken.		
1.6	Breng in kaart met welke externe partijen / welke gegevens worden uitgewisseld (zowel ontvangen als verstrekt), op welk wijze de uitwisseling plaats vindt en waarom (doel van de registratie). Mede in verband van het kunnen maken van afspraken.		
1.7	Breng in kaart met welke contractpartijen zaken worden gedaan en wat de inhoud van deze zaken is. Denk hierbij aan softwareleveranciers, IT, kantoormiddelen, schoonmakers, onderhoud van apparatuur en pand, beveiliging, personeel (uitzendbureaus). Mede in verband van het kunnen maken van afspraken.		
1.8	Breng in kaart op welke wijze invulling kan worden gegeven aan de verantwoording over de doorlopende effectiviteit van ‘de passende maatregelen’.		
1.9	Analyseer op welke wijze het register van verwerkingsactiviteiten binnen de organisatie van verwerkingen vorm kan krijgen.	[**4.8**]	
1.10	Ingeval de MKB-accountant een rol vervult van verwerkingsverantwoordelijke, heeft die MKB-accountant een verantwoordelijkheid voor de gehele keten. Deze verantwoordelijkheid vraagt om actieve regie en actief toezicht.	[**6.1**]	

Stap	Maatregel	Verwijzing
	Evalueer de wijze waarop de verantwoordelijkheden in de keten als verwerkingsverantwoordelijke kan worden ingevuld, door audits, door een integraal ketenregister van verwerkingsactiviteiten (bijvoorbeeld met behulp van 'Sticky notes') of anderszins (bijvoorbeeld 'Smart contracts') een en ander contractueel te regelen, met behulp van een TTP.	
1.11	Voer een (initiële) analyse uit op het geformuleerde beleid, de (bestaande) procedures en de (bestaande) processen om de risico's met betrekking tot de informatiebeveiliging en privacybescherming te identificeren.	

Stap 2: Het invulling geven aan de AVG bepalingen

Indien sprake is van het verwerken van persoonsgegevens moet de MKB-accountant minimaal de volgende zaken geregeld hebben.

Stap	Maatregel	Verwijzing	
2	**Invullen van de AVG verplichtingen**		
2.1	Zorg dat duidelijk is welke verwerkingen van (bijzondere) persoonsgegeven plaatsvinden en wat daarvan de wettelijke grondslag is.	[**4.2**]	

2.2	Zorg dat er procedures zijn ingericht die het mogelijk maken dat uw organisatie als verwerkingsverantwoordelijke invulling kan geven aan de rechten van betrokkene(n).
	Dit betekent in de praktijk:
	• Afspraken over de inhoud en vorm van communicatie met de betrokkene;
	• Het kunnen verstrekken van informatie wanneer en waarom persoonsgegevens bij betrokkenen zijn verzameld;
	• Het kunnen verstrekken van informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen, maar van een derde partij;
	• Het kunnen reageren op een verzoek om:
	  ○ inzage;
	  ○ rectificatie;
	  ○ bezwaar;
	  ○ beperking van de verwerking;
	  ○ vergetelheid;
	  ○ persoonsgegevens over te dragen aan een derde partij.
	• Het kunnen informeren van een ontvanger (kennisgeving).
		[**4.5**]	

2.3	Zorg dat er een protocol is en een procedure ingericht die het mogelijk maakt dat een beveiligingsincident kan worden beoordeeld, zodat binnen uiterlijk 72 uur een melding van een datalek kan worden gedaan bij de AP.
	Dit betekent in de praktijk:
	• De beschikbaarheid van een functionaris die in staat is en bevoegd om een beveiligingsincident te beoordelen en - zo nodig in samenspraak met anderen - te beslissen of er wel of geen melding bij de AP moet worden gedaan;
	• Dat de benodigde informatie over de persoonsgegevens, het incident, de verwerking, etc. beschikbaar moeten zijn;
	• Een aantal beslissingen moeten worden genomen, zoals:
	  ○ Of het beveiligingsincident betrekking heeft op persoonsgegevens;
	  ○ Of de organisatie in dit verband verwerkingsverantwoordelijk of verwerker is, dit i.v.m. de volgende beslissingen en acties;
		[**4.9**]
		[**II: H-6**]
		[**II: H-7**]
		[**II: H-8**]
		[**II: H-9**]
		[**II: H-10**]
			

Stap	Maatregel	Verwijzing	
	○ Of er een melding moet worden gedaan bij de AP of bij de verwerkingsverantwoordelijke; ○ Of de betrokkene(n) moet(en) worden geïnformeerd; ○ De feitelijke melding moet worden gedaan bij de AP of de verwerkingsverantwoordelijke; • Ook in het geval dat er geen sprake is van een datalek zal de registratie van beveiligingsincidenten / datalekken moeten worden bijgewerkt. Leg dit contractueel vast.		
2.4	Zorg voor passende technische en organisatorische maatregelen opdat de verwerking aan de eisen van de wet voldoet en de bescherming van de rechten van betrokkene(n) zijn gewaarborgd. Houd hierbij rekening van de verplichtingen in de AVG wat betreft Privacy by design en by default.	[**4.4**]	
2.5	Zorg dat in voorkomende gevallen een PIA wordt uitgevoerd.	[**4.10**] [**II: H-11**] [**NOREA-4**]	
2.6	Zorg dat er indien nodig een register van verwerkingsactiviteiten wordt bijgehouden.	[**4.8**] [**II: H-5**]	
2.7	Zorg dat met alle (sub)verwerker overeenkomsten zijn afgesloten.		
2.8	Sluit gegevensovereenkomsten voor de uitwisseling van persoonsgegevens.		
2.9	Zorg voor 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

Om passende beveiligingsmaatregelen te kunnen nemen is het van belang inzicht te hebben op welke gebieden uw kantoor de grootste risico's loopt. Dit inzicht kan worden verkregen door het uitvoeren van een risicoanalyse. Omdat het uitvoeren van een risicoanalyse veel tijd in beslag kan nemen, kan als eerste stap gebruik worden gemaakt van een QuickScan. Dit met als doel een eerste indruk te krijgen welke gebieden als eerste aandacht nodig hebben en waar maatregelen direct effectief kunnen zijn.

Deze stap kan ook worden overgeslagen en als wordt gekozen voor de baseline-aanpak die is gevolg bij het opstellen van het stappenplan.

Stap	Maatregel	Verwijzing	
2	**Risicoanalyse of QuickScan uit**		
2.1	Voer een risicoanalyse uit, of.	[**4.2**]	
2.2	Maak gebruik van een QuickScan om inzicht te krijgen in de aandachtsgebieden waar uw organisatie de meeste risico's loopt.	[**5.2**] [**II: H-13**]	
2.9	Zorg voor een gedragscode waarin is vastgelegd hoe om te gaan met gegevens binnen de eigen organisatie en in relatie met de klanten.		

Stap 4: Het invullen van de beveiligingsmaatregelen

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 in de praktijk, mede door hun

beperkte omvang (schaal) en gebrek aan deskundigheid, niet of moeilijk in staat zijn om de gewenste beveiligingsmaatregelen zelf te realiseren. Het gebruik maken van de diensten van derde partijen, kan in dat geval een oplossing bieden. Voorbeelden in dit kader zijn, het gebruik van toepassingen in de Cloud waardoor data op een veilige plaats wordt bewaard, het gebruik van beveiligde communicatie en mobiele apparaten. Dit natuurlijk onder de voorwaarde dat zaken wordt gedaan met betrouwbare partijen (zoals ook de privacywetgeving vereist) en het kantoor in staat is 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 een bedrijfs- en reputatierisico met zich meebrengen, worden beëindigd.

Stap	Maatregel	Verwijzing	
4	**Het treffen van maatregelen**		
4.1	**In de organisatie**		
4.1.1	Werk aan bewustwording en awareness door medewerkers te informeren over de belangrijkste verplichtingen van de (nieuwe) privacywet en voorkomende cyberdreigingen en datalekken. Wissel periodiek ervaringen uit.	[**AP-2**]	
4.1.2	Vraag van medewerkers een alerte houding bij onduidelijke, onverwachte of mogelijk potentieel bedreigende situaties en personen. Dit veronderstelt wel een 24/7 beschikbaarheid van een functie / functionaris die bevoegd is, indien nodig, actie te ondernemen. Een dergelijke functie / functionaris is ook nodig in het kader van een protocol voor het kunnen melden van een datalek.		
4.1.3	Maak, op basis van het geformuleerde beveiligings- en privacy-beleid, afspraken met uw medewerkers over wat van hen wordt verwacht. Hierbij passen concrete afspraken over wat wel en niet is toegestaan wat betreft toegang tot, het gebruik van, en het verstrekken van data aan derde partijen (incl. klanten). Voorts maak afspraken over het monitoren van het gedrag en eventuele sancties bij het niet nakomen van de gemaakte afspraken. Dit moet wel duidelijk en tijdig worden gecommuniceerd.	[**NEN-2**]	
4.1.4	Zorg voor een vorm van screening van uw bestaande / nieuwe medewerkers.		
4.1.5	Zorg voor een toegangsregeling tot het kantoor.	[**NEN-2**]	
4.1.6	Organiseer het beheer over het verlenen van (identiteits- en toegangsbeheer) door voor gebruikers bevoegdheden op basis van gebruikersprofielen toe te kennen en af te nemen. Dit vereist een beschikbaarheid van die gebruikersprofielen, onderhouden van die profielen en een beheerste toekenning/intrekking van bevoegdheden (inclusief vastleggingen). Dit is van toepassing op betrokkenen binnen de gebruikersorganisatie en binnen de IT-omgeving.	[**NEN-2**]	
4.2	**Met betrekking tot gegevens**		
4.2.1	Organiseer het beheer van gegevens (welke gegevens in relatie tot welke verwerkingen en de verantwoordelijke functionarissen), alsmede het changemanagement op wijzigingen in de te gebruiken / gebruikte gegevens als gevolg van bijvoorbeeld wijzigingen in het dienstenaanbod of wijzigingen in verwerkingen.	[**NEN-2**]	
4.2.2	Stel een beleid op om het opslaan en verwerken van persoonsgegevens tot een minimum te beperken en gegevens op een beheerste wijze te vernietigen (inclusief vastlegging).		

Stap	Maatregel	Verwijzing	
4.2.3	Stel regels en richtlijnen op voor de selectie van ontvangen persoonsgegevens, in het bijzonder voor niet gestandaardiseerde gegevensleveringen, zoals via e-mails en bijlagen.		
4.2.4	Stel vast dat ook in contracten met klanten en leveranciers voorkomen wordt dat 'overbodige' persoonsgegevens worden verstrekt en uitgewisseld.		
4.2.5	Betrek in de analyse en het beheer ook de gegevens die een rol vervullen in back-up & recoveryprocedures.	[**NEN-2**]	
4.3	**Met betrekking tot het dienstenpakket**		
4.3.1	Zorg voor passende Algemene voorwaarden, waarbij rekening is gehouden met de afspraken die u met uw klanten moet maken in het kader van de privacywetgeving.	[**4.6**] [**4.7**]	
4.3.2	Ga na of aangeboden diensten voldoende gestandaardiseerde (of geautomatiseerde) waarborgen bevatten voor het verwerken van persoonsgegevens (voorkomen 'verdwaalde' bestanden e.d.).		
4.3.3	Ga na welke effecten nieuwe diensten of beëindigde diensten hebben op de verwerkingen en de daarbij betrokken persoonsgegevens.	[**4.10**]	
4.4	**Met betrekking tot de applicaties / applicatie-architectuur**		
4.4.1	Implementeer nieuwe software- en beveiligingsupdates van de betrouwbare software partners direct omdat daarin de nieuwe beveiligingsmaatregelen zijn opgenomen ter voorkoming van het ongewenste verkrijgen van toegang.	[**NEN-2**]	
4.4.2	Zorg dat de juiste applicaties worden toegepast door onder meer toepassing van een effectief versiebeheer en changemanagement op software.	[**NEN-2**]	
4.4.3	Ga naar of er sprake is van onnodige complexiteit in gebruik van applicaties en de onderlinge uitwisseling van data en indien dat de situatie is, zorg dan dat deze complexiteit wordt opgelost.		
4.4.4	Stel vast dat of in de applicatiearchitectuur legacy-systemen zijn opgenomen die tot verhoogde risico's kunnen leiden.		
4.4.5	Stel vast dat de leverancier van softwarediensten voldoet aan de eisen van de AVG.	[**4.4**] [**4.7**]	
4.5	**Met betrekking tot de technische infrastructuur**		
4.5.1	Zorg voor toereikend (configuratie) beheer van de verschillende systeemcomponenten (hardware, software, datacommunicatie e.d.): • start met de identificatie en vastlegging van de bestaande systeemcomponenten; • ontwikkel het wijzigingsbeheer. Dit betreft het changemanagement op aanpassingen in de infrastructuur door aanpassingen (nieuw, buitengebruik, vervanging etc.) van de verschillende systeemcomponenten; incl. de vastleggingen daarvan.	[**NEN-2**]	
4.5.2	Zorg voor een toereikende beveiliging tegen bedreigingen van buitenaf door het gebruik van firewalls en virusscanners.	[**NEN-2**]	
4.5.3	Breng waar mogelijk en zinvol scheiding aan in de infrastructuur, zodat een mogelijk beveiligingsprobleem niet het hele IT-infrastructuur kan besmetten.	[**NEN-2**]	

Stap	Maatregel	Verwijzing	
	Zorg dat gegevens die niet direct toegankelijk behoeven te zijn, zoals het archief en het accountantsdossier van afgesloten opdrachten, niet toegankelijk zijn via de huidige infrastructuur, maar geplaatst op een aparte omgeving in de eigen locatie of bij derden.		
4.5.4	Zorg voor de 24/7 beschikbaarheid van de functie 'Incident en probleemmanagement', zodat direct kan worden gereageerd op beveiligingsincidenten of berichten / vragen van medewerkers.	[**NEN-2**]	
4.5.5	Stel vast dat technische opzet en beveiliging van de website, het portaal en de e-mailserver effectieve waarborgen bevatten om inbreuken door derden te detecteren, af te handelen en te registreren.	[**NCSC-1**]	
4.5.6	Ga na, waarschijnlijk in samenwerking met derde partijen, welke IoT apparatuur aan uw netwerk is gekoppeld, of dit noodzakelijk is en zo ja, of deze apparatuur toereikend is beveiligd voor inbreuken.	[**NCSC-4**] [**NCSC-5**]	
4.5.7	Zorg voor maatregelen om bij calamiteiten de continuïteit (op korte en op langere termijn) te kunnen waarborgen en back-up & recovery van te gebruiken / gebruikte gegevens.	[**NEN-2**]	
4.5.8	Buitengebruik gestelde apparatuur (computers, servers, mobiele apparaten, harde schijven) worden via een beheerst proces geschoond voor data en vernietigd inclusief de vastlegging daarvan. Met externe partijen worden afspraken gemaakt over de vernietiging inclusief de verantwoording daarover.		
4.5.9	Stel vast dat de leverancier van de systeemcomponenten blijvend voldoet aan de eisen van de AVG.	[**4.4**] [**4.7**]	
4.6	**Met betrekking tot derde partijen / (sub)verwerkers**		
4.6.1	Organiseer het ketenbeheer. Dit betreft beleidsmatig en operationeel beheer van de samenhang van de verschillende contractpartijen in de ketens van informatievoorziening (bijvoorbeeld van cliënten via MKB-kantoor naar cloudleveranciers).		
4.6.2	Zorg voor een beheerste inzet van (sub)verwerkers door een proces van screening en selectie bij de keuze van nieuwe derde partijen.	[**4.4**] [**4.7**]	
4.6.3	Sluit schriftelijke overeenkomsten af met (sub)verwerkers met minimaal de vereiste onderwerpen (AVG); onder meer over de uitbestede verwerkingen en de betrokken persoonsgegevens alsmede de verantwoording over de doorlopende effectiviteit van de passende set van maatregelen.	[**4.4**] [**4.6**] [**4.7**] [**II: H-4**]	
4.6.4	Maak afspraken met andere dienstverleners.		
4.6.5	Stel vast dat de (sub)verwerker blijvend voldoet aan de eisen van de AVG.	[**4.7**]	
4.7	**Met betrekking tot de toegang en de uitwisseling van data**		
4.7.1	Beperk de toegang tot persoonsgegevens door minimalisering hoeveelheid gegevens, beperking van gegevensuitwisseling en van bevoegdheden om verwerkingen met gegevens te verrichten.	[**NEN-2**]	
4.7.2	Toegang tot de (persoons-) gegevens vindt plaats op basis van het 'Need to Know' principe, wat betekent dat alleen medewerkers / derde partijen toegang hebben, als dat noodzakelijk is om hun werk (binnen het doel van gegevensverwerking en opslag) te kunnen uitvoeren.	[**NEN-2**]	

Stap	Maatregel	Verwijzing	
	De toegang tot data wordt aan personen en applicaties verleent op basis van een sterke identificatie en authenticatie, alsmede autorisatie (bevoegdheden). De toegang (beveiliging) tot de data is altijd up to date. Iedere gebruiker/applicatie heeft een eigen user-ID, waaraan de persoon/applicatie en zijn bevoegdheden zijn gekoppeld. Gebruik van elkaars user-ID's is niet toegestaan. Er wordt een strikt wachtwoordbeleid gehanteerd, waarbij gebruikers door het systeem gedwongen worden om maandelijks hun wachtwoord te wijzigen. Aan het wachtwoord zijn eisen gesteld die voorkomt dat eenvoudige wachtwoorden kunnen worden geraden en hergebruikt. Inactief na verloop van beperkte tijd en toegangspogingen.		
4.7.3	Informatie (gegevens) wordt alleen verstrekt aan 'bekende' organisaties of personen, die bevoegd zijn om deze informatie te ontvangen.	[**NEN-2**]	
4.7.4	Met klanten worden afspraken gemaakt de uitwisseling (verstrekking en ontvangst) van klantdata; bijvoorbeeld dat • gegevensuitwisseling alleen plaats vindt via beveiligde en beveiligde (encrypte) verbindingen; • het verstrekken van gegevens plaats vindt door het beschikbaar stellen van deze gegevens op het eigen portaal. Het ophalen van deze gegeven, alsmede de verdere verwerking, is de verantwoordelijkheid van de ontvanger; • geen gebruik gemaakt van e-mail of USB-sticks, of publieke datatransfer programma's.	[**NEN-2**]	
4.7.5	Gegevens (bestanden), die van derden worden ontvangen, worden als eerst stap geplaatst op een aparte omgeving (computer), waar zij indien nodig worden uitgepakt en gescreend op persoonsgegevens, virussen, etc.		
4.7.6	Betrek in de toegangsregeling ook de remote-toegang waardoor gebruikers op afstand toegang kunnen verkrijgen; software kan deze toegang beheerst laten verlopen.	[**NEN-2**]	
4.7.7	Beperk de toegang van de functie Incident en probleemmanagement (helpdesk) tot wat noodzakelijk is, en zorg dat achteraf verantwoording wordt afgelegd over uitgevoerde acties.		
4.7.8	Stel van dat er geen leveringen van persoonsgegevens plaatsvinden aan een land buiten de Europese Economische Ruimte, tenzij er sprake van een 'passend beschermingsniveau'.	[**art. 44, AVG**]	

4.8	**Met betrekking tot het gebruik van mobiele apparatuur**		
4.8.1	Communicatie vindt alleen plaats via beveiligde (encrypte) verbindingen, zowel binnen als buiten de organisatie.	[**NCSC-2**]	
4.8.2	Organiseer een scheiding tussen zakelijk en privé gebruik. Smartphones kunnen worden voorzien van MDM (Mobile Device Management) software, waardoor de toegang tot de data wordt beveiligd en een scheiding kan worden aangebracht tussen privé en zakelijk gebruik. Op deze wijze kan het zakelijk gebruik worden beperkt tot toegestane apps en afgeschermd van in privé gebruikte apps. Bij verlies of diefstal kan het apparaat onbruikbaar worden gemaakt. Een andere optie is mobiele apparatuur die door de eigen organisatie wordt verstrekt en alleen maar zakelijk mag worden gebruikt. Deze apparatuur moet natuurlijk ook zijn voorzien van goede beveiliging.	[**NCSC-2**]	

Stap	Maatregel	Verwijzing
4.8.3	Organiseer de toegang tot en opslag van gegevens op laptops. Laptops kunnen worden voorzien van toegangsbeveiliging en de data kan encrypted worden opgeslagen. Daarnaast kan het gebruik van programmatuur worden beperkt, alsmede de opslag van klantdata. Laptops van de organisatie mogen niet privé worden gebruikt en onbeheerd achtergelaten.	[**NCSC-2**] 

Stap 5: Evaluatie, monitoring en bijstelling

In deze afsluitende stap worden maatregelen ingevoerd die de organisatie in staat stellen om het functioneren van ingevoerde maatregelen te evalueren, te monitoren, en desgewenst bij te stellen. Daarnaast maatregelen om het gedrag te monitoren en het niet naleven van afspraken tijdig te signaleren (detectie). Maar ook maatregelen en procedures gericht op een juiste afhandeling van incidenten en verstoringen.

Stap	Maatregel	Verwijzing
5	**Operationele / periodieke activiteiten**	
5.1	**Verwerkingsregistratie**	
5.1.1	Organiseer “accountability’ door een gedegen administratie te voeren met betrekking tot verwerkingen en opslag van data. Inzichtelijk moet worden gemaakt dat de passende maatregelen doorlopend effectief zijn geweest en adequaat voor de afwikkeling van een datalek. De gedegen administratie moet een sluitende registratie van alle verwerkingen omvatten om eventuele inbreuken zelfstandig te kunnen detecteren en bij een claim van een benadeelde te kunnen aantonen welke verwerking onder welke omstandigheden is uitgevoerd.	[**4.8**] [**II: H-5**]
5.1.2	Tref waarborgen rond de verwerkingsregistratie die moeten voorkomen dat aan de juistheid en volledigheid van de registraties kan worden getwijfeld (ter vergelijking: eisen aan een financiële of inkoopadministratie).	
5.2	**Incident- en probleembeheer**	
5.2.1	Organiseer het beheer van de operationele beveiliging. Dit betreft het operationeel doorlopend inventariseren en adresseren van de risico’s (beschikbaarheid, integriteit en vertrouwelijkheid) die van toepassing zijn op de informatievoorziening en in het bijzonder op de verwerkingen van persoonsgegevens.	[**NEN-2**]
5.2.2	Zorg voor awareness bij betrokkenen van het belang van het signaleren, vastleggen en rapporteren van incidenten en verstoringen.	[**NEN-2**]
5.2.3	Stel procedures op voor een juiste afhandeling van incidenten en verstoringen.	[**NEN-2**]
5.2.4	Organiseer beheerste computer operaties. Dit betreft het binnen de gestelde eisen operationeel houden van de IT-diensten op de afgesproken dienstenniveau ’s.	[**NEN-2**]
5.2.5	Organiseer de continuïteit van de bedrijfsvoering (bedrijfscontinuïteitbeheer). Dit betreft het beheer van voorzieningen om na het optreden van een calamiteit of incident de bedrijfsvoering wordt hersteld en voortgezet van in overeenstemming met afgesproken dienstenniveau ‘s en de gestelde eisen (AVG).	[**NEN-2**]

Stap	Maatregel	Verwijzing
5.3	**Monitoring (detectie)**	
5.3.1	Stel vast dat de geformuleerde uitgangspunten voor het beveiligings- en privacy-beleid en de daaruit voortvloeiende waarborgen zijn nageleefd.	[**NEN-2**]
5.3.2	Stel vast dat opgeslagen persoonsgegevens niet langer dan noodzakelijk worden opgeslagen; indien mogelijk verwijder (waaronder terugzending naar opdrachtgever) persoonsgegevens en leg dit vast.	
5.4	**Evaluatie van beveiligingsmaatregelen (vorm van risicoanalyse)**	
5.4.1	Draag zorg voor project-voortgangsverslagen over de voorbereidingen van de invoering van de te treffen “passende maatregelen”.	
5.4.2	Organiseer een rapportage over het functioneren van de informatiebeveiliging waaruit tot uitdrukking komt in welke mate wordt voldaan aan de informatie- en privacybescherming. Dit conform de reguliere planning- en control en verantwoordingscyclus voor de leiding van het MKB kantoor.	
5.4.3	Stel vast dat de verwerkingsregistratie voldoet aan de daaraan te stellen eisen van ‘accountability’.	
5.4.4	Stel ten minste vast dat de contractspartijen een verklaring kunnen overleggen waaruit blijkt dat zij accountable zijn voor de wet AVG en daarmee verklaren doorlopend effectieve maatregelen getroffen te hebben.	
5.5	**Check op naleving**	
5.5.1	Stel vast dat de bestuurlijk verantwoordelijke informatie- en privacybescherming op de agenda van de leiding van het MKB-kantoor plaatst door middel van nieuwe inzichten en periodieke rapportages.	
5.5.2	Stel vast dat de FG over de door de wet gestelde onderwerpen heeft geadviseerd en opinions heeft afgegeven. Stel vast dat deze uitingen op een zorgvuldige wijze zijn betrokken in het besluitvormingsproces.	[**4.11**]
5.5.3	Stel vast dat de organisatie een verantwoordingsdocument heeft opgesteld, dat is gebaseerd op een ‘accountable’-grondslag en waaruit blijkt dat de passende maatregelen effectief zijn gebleken.	

8. ADVISERING / ONDERSTEUNING VAN KLANTEN

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

Voorwaarde hiervoor is wel dat de MKB-accountant beschikt over de benodigde technische en juridische kennis. Indien hij daarover niet zelf beschikt, kan dit worden verkregen door inhuur van specialisten of samenwerking met andere partijen, die wel over deze deskundigheid beschikken. Voorbeeld is het MKB-kantoor dat IT-specialisten inhuurt en/of samenwerkt met derde partijen, waaronder IT-juristen.

Bij de advisering / ondersteuning van klanten is het van belang dat de MKB-accountant uitgaat van de bedrijfsvoering van de desbetreffende organisatie en de daarbij behorende (bedrijfs)risico's. 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 waar welke maatregelen moeten getroffen, naast de maatregelen en procedures die de AVG verplicht stelt. Denk hierbij, naast 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, 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?

Dit rapport is niet zonder meer geschikt voor advisering van klanten, omdat het uitgaat van de bedrijfsvoering / dienstverlening van de MKB-accountant. Dit rapport is echter wel een goede basis, omdat het praktische informatie bevat in de vorm van beslissingstabellen, beveiligingsstandaarden en normen-/beheersingskaders, alsmede nadere informatie over verplichtingen in het kader van de (vernieuwde) privacywetgeving. Het gepresenteerde Stappenplan kan ook voor klanten een goede eerste stap zijn.

DEEL II: INHOUDSOPGAVE

Correspondentieadres
NEMACC, Kamer H 13-05
Postbus 1738, 3000 DR Rotterdam