Informatiebeveiliging & privacybescherming

Deel II achtergrondinformatie / hulpmiddelen

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

(december 2017)

DEEL II: Achtergrondinformatie / hulpmiddelen

Informatiebeveiliging & privacybescherming

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

December 2017

INHOUDSOPGAVE

H-1: DE BELANGRIJKSTE KENMERKEN VAN EEN MKB-KANTOOR

De diversiteit van de dienstverlening, alsmede de daaruit voortvloeiende complexiteit wordt geïllustreerd aan de hand van onderstaand overzicht van de belangrijkste kenmerken.

DIENSTENPAKKET

MKB-kantoren bieden vaak een uitgebreid dienstenpakket aan.

- Bij het aanbieden wordt gebruik gemaakt van een veelheid aan data, waaronder bedrijfsgevoelige data en persoonsgegevens;
- Diensten kunnen als zelfstandige eigen activiteit (eigen merk of label) of onder geassocieerd label worden aangeboden. Het aanbieden van de verschillende diensten onder een zelfde naam / label, maakt dat cyberinbreuken op een dienst een negatieve (commerciële) impact kunnen hebben op de andere diensten;
- Op de aangeboden diensten is vaak verschillende wet- en regelgeving van toepassing;
- Bij de uitvoering wordt vaak gebruik gemaakt van de diensten van derde partijen, zoals softwareleveranciers of deskundigen op fiscaal of juridisch terrein. Het samenwerken met derde partijen vereist afspraken en brengt afhankelijkheden mee wat betreft kwaliteit en naleving van wet- en regelgeving.

APPLICATIES / APPLICATIEARCHITECTUUR

- Meestal is sprake van het gebruik van standaard applicaties; vanuit de eigen omgeving of via het gebruik van diensten van derde partijen (serviceproviders / Cloudleveranciers);
- Er is voor een deel sprake van gemengd gebruik, applicaties worden zowel door de klanten als het MKB-kantoor gebruikt. Klanten hebben vaak toegang tot hun eigen boekhouding en salarisverwerking, die ook door de accountant in het kader van zijn administratieve dienstverlening, of mogelijk controle wordt gebruikt;
- Voor het uitvoeren van werkzaamheden zijn soms meerdere applicaties nodig. Bijvoorbeeld het samenstellen van aangiftes of jaarrekeningen, het goedkeuren daarvan door klanten en het verzenden naar het overheids- of bankenportaal;
- Voor de communicatie met klanten en derde partijen wordt gebruik gemaakt van publieke diensten, zoals het internet;
- De verschillende toepassingen worden vaak geleverd door verschillende leveranciers en beschikken over een eigen inlog-functie en onderhoudscyclus;
- Indien sprake is van maatwerk vereist dit extra aandacht wat betreft de functionaliteit en de koppeling met andere toepassingen;
- De functionaliteit van applicaties, alsmede de gebruikte dataformaten verschillen vaak wat de gegevensuitwisseling tussen de verschillende toepassingen kan bemoeilijken;
- Soms wordt om die reden gebruik gemaakt van tools voor de uitwisseling en opslag van gegevens. Voorbeelden hiervan zijn o.a. WeTransfer voor de uitwisseling en Dropbox, Google Drive of OneDrive voor de opslag van data. Elke aanbieder kent eigen voorwaarden ten aanzien van de beschikbaarheid (continuïteit), integriteit en vertrouwelijkheid van verwerkte/getransporteerde gegevens;
- In sommige vormen van dienstverlening wordt gebruik gemaakt van algoritmes die de advisering en/of besluitvorming ondersteunen. Bijvoorbeeld bij pensioen- of financieringsberekeningen;
- Vaak is er geen sprake van een geïntegreerde vorm van toegangsbeveiliging, inclusief centraal beheer van autorisaties en bevoegdheden;

- Veel kantoren maken gebruik van mobiele apparatuur (laptops, tablets en smartphones);
- De e-mailbox en de website van het kantoor staan open voor communicatie met derden. Daarnaast zijn applicaties soms gekoppeld met sociale media;
- Het komt ook voor dat actief van sociale media gebruik gemaakt wordt, wat eisen stelt aan het gebruik om betrokkenheid bij ongewenste uitingen te voorkomen.

De verscheidenheid aan applicaties en leveranciers vereist actieve afstemming en concrete afspraken omtrent de inhoud en kwaliteit van de dienstverlening. De variëteit van applicaties kan ook conflicten opleveren bij een geïntegreerd gebruik (bijvoorbeeld bij andere formaten van data). De verschillende inlog-functies kunnen een single sign-on bij de toegangsverlening in de weg staan.

TECHNISCHE INFRASTRUCTUUR

De applicaties functioneren vaak binnen een complexe technische infrastructuur waarin een grote variëteit aan componenten zijn te onderkennen, zoals:

- Verschillende (versies) van besturingssystemen en browsers, zoals Windows, Unix, Linux, Mac OSX, Android, iOS;
- Firewalls , anti-virus- e/o encryptie-software;
- Centrale servers voor de opslag en de verwerking van gegevens;
- Routers en switches voor de interne en externe datacommunicatie;
- Netwerken, inclusief Wifi;
- Communicatiefaciliteiten, zoals Citrix;
- Personal computer en mobiele apparatuur (laptops, tablets, smartphones) of zelfs wearables, zoals een Apple-watch;
- Printers en scanners;
- Software in apparaten (Internet of Things / IoT)) zoals in vervoermiddelen (koppelingen met navigatie-systemen of rittenregistratie), alarmsystemen, telefooncentrales;
- Back-up en recovery faciliteiten.

INHOUSE VERSUS UITBESTEED

De gegevensverwerking en -opslag, alsmede het functioneel en technische beheer kan intern worden verzorgd of zijn uitbesteed. Het in de eigen omgeving beheren van applicaties vereist de nodige deskundigheid maar ook beschikbaarheid. Het gebruik maken van derde partijen vereist duidelijke en actuele afspraken.

CONTRACTSPARTIJEN

Een MKB-kantoor heeft doorgaans met meerdere contractspartijen te maken, zoals:

- Softwareleveranciers en (cloud)serviceproviders;
- Leveranciers, zoals: IT en kantoormiddelen;
- Schoonmakers;
- Onderhoud van apparatuur, pand;
- Beveiliging;
- Uitzendbureaus.

TOEGANG TOT DATA / APPLICATIES

Er zijn verschillende mogelijkheden om de toegang tot en de uitwisseling van data te organiseren.

- Een centrale voorziening waarbij gebruikers op basis van een centrale toegangsschil (Single sign-on-software) toegang krijgen tot data / applicaties;
- Een toegang per applicatie/gegevensverzameling, wat in de praktijk betekent dat per toepassing de toegang moet worden geregeld en onderhouden.

Naast het verlenen van toegang aan gebruikers (natuurlijke personen) en voor informatiesystemen in de keten (geïntegreerde supply chain) moet ook het verlenen van toegang tot applicaties en apparatuur worden beheerd. Hierbij kun je denken aan applicaties die data verwerken of moeten goedkeuren of apparatuur voor de uitwisseling van data (USB sticks of andere portable gegevensdragers) of mobiele apparatuur.

Voorbeeld van BYOD

Indien gebruik wordt gemaakt van mobiele apparatuur op basis van BYOD (Bring Your Own Device) zal onderscheid moeten worden gemaakt tussen zakelijk en privé gebruik en zal voorkomen moeten worden dat zakelijke data via privégebruik of privé apps kunnen worden benaderd. Voor risico's en maatregelen, zie de NBA-publicatie: De mkb-accountant en Cloud Computing [**NBA-12**].

In het kader van de uitwisseling van data tussen applicaties, apparaten of gebruikers (natuurlijke personen) zullen maatregelen moeten worden getroffen om het ontvangen van data van o.a. klanten en het verstrekken van data aan klanten of derde partijen te beheersen.

Dit geldt ook voor de toegang van derde partijen tot de technische omgeving van het MKB-kantoor of de applicaties / data; hierbij te denken aan dienstverleners die het functioneel en technisch beheer van de IT verzorgen, maar ook onderhoud aan technische apparatuur, zoals telefoon- en alarminstallaties, klimaat-, toegangssystemen, etc.

In de praktijk kunnen data op verschillende plaatsen en mogelijk meerdere locaties zijn opgeslagen (eigen omgeving of bij een cloudleverancier).

ORGANISATIE EN DE MENS (DE GEBRUIKER)

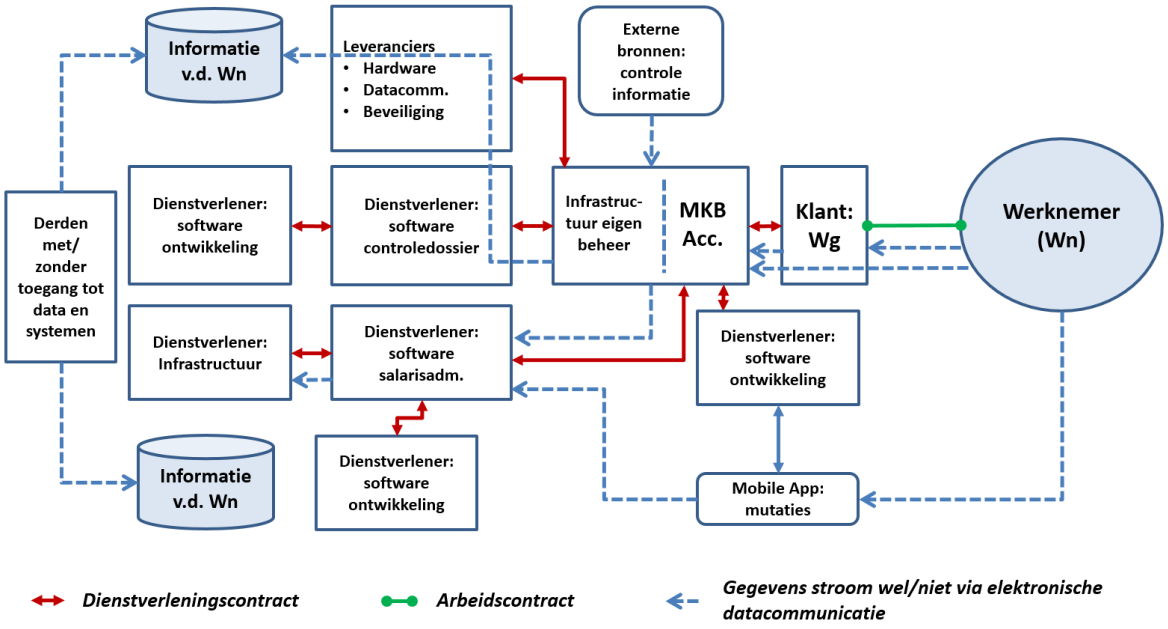
Een belangrijke factor is de mens. Bij het uitvoeren van zijn werkzaamheden heeft het MKB-kantoor met o.m. de volgende partijen te maken:

- Het personeel van klanten of mensen die namens of in opdracht van klanten handelen;
- De eigen en ingehuurde medewerkers met verschillende deskundigheden en vaardigheden en 'dienstverbanden' (accountants, IT-specialisten, medewerkers in opleiding, stagiaires, inhuurkrachten, buitenlandse werknemers, etc.);
- Personeel van leveranciers en dienstverleners;
- Medewerkers van publieke diensten, zoals het UWV, Belastingdienst, Deurwaarders, Justitie, etc.;
- Cybercriminelen.

In de praktijk worden vooral de MKB-kantoren geconfronteerd met de beperkte deskundigheid en beschikbaarheid van eigen medewerkers op het terrein van IT en informatiebeveiliging. Een oplossing is dan vaak het gebruik van derde partijen, wat een oplossing kan zijn voor het gebrek aan deskundigheid en beschikbaarheid, maar wel de afhankelijkheid van deze partijen en hun kwaliteit van dienstverlening vergroot.

VOORBEELD VAN COMPLEXITEIT

Dat complexiteit al snel in een organisatie tot uitdrukking kan komen wordt in het navolgende figuur geïllustreerd. Het MKB-kantoor voert de salarisadministratie voor klanten en verricht controlewerkzaamheden. Hierbij wordt gebruik gemaakt van door derden aangeboden software in de cloud en binnen het eigen netwerk. Bovendien mogen medewerkers van de verwerkingsverantwoordelijke (betrokkenen) rechtstreeks via een app gegevens aanleveren. Centraal staan vragen als, wie verricht welke verwerkingen en wie kan de garantie voor de doorlopende werking van de passende maatregelen leveren?



Afbeelding 11: Illustratie van mogelijke complexiteit bij slechts twee typen dienstverlening

H-2: OVERZICHT VAN DE BELANGRIJKSTE ARTIKELEN VAN DE AVG

In dit overzicht zijn de belangrijkste artikelen van de AVG voor het doorsnee MKB-kantoor opgenomen (artikelen 1 t/m 39). Niet opgenomen zijn de overwegingen en de artikelen die betrekking op:

- Afdeling 5: Gedragscodes en certificering (artikelen 40 t/m 43);
- Hoofdstuk V: Doorgiften van persoonsgegevens aan derde landen of internationale organisaties (artikelen 44 t/m 50);
- Hoofdstuk VI: Onafhankelijke toezichthoudende autoriteiten (artikelen 51 t/m 59);
- Hoofdstuk VII: Samenwerking en coherentie (tussen de toezichthouders) (artikelen 60 t/m 76);
- Hoofdstuk VIII: Beroep, aansprakelijkheid en sancties (artikelen 77 t/m 84);
- Hoofdstuk IX: Bepalingen in verband met specifieke situaties op het gebied va gegevensverwerking (artikelen 85 t/m 91);
- Hoofdstuk X: Gedelegeerde handelingen en uitvoeringshandelingen (artikelen 92 t/m 93);
- Hoofdstuk XI: Slotbepalingen (artikelen 94 t/m 99).

Artikel 1, AVG

1. Bij deze verordening worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens.
2. Deze verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens.
3. Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.

Artikel 2, AVG

1. Deze 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.
2. Deze verordening is niet van toepassing op de verwerking van persoonsgegevens: 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.
3. Op de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie is Verordening (EG) nr. 45/2001 van toepassing. Verordening (EG) nr. 45/2001 en andere rechtshandelingen van de Unie die van toepassing zijn op een dergelijke verwerking van persoonsgegevens worden overeenkomstig artikel 98 aan de beginselen en regels van de onderhavige verordening aangepast.
4. Deze verordening laat de toepassing van Richtlijn 2000/31/EG, en met name van de regels in de artikelen 12 tot en met 15 van die richtlijn betreffende de aansprakelijkheid van als tussenpersoon optredende dienstverleners onverlet.

Artikel 3, AVG

1. Deze verordening is van toepassing 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 in de Unie al dan niet plaatsvindt.

2. Deze verordening is van toepassing 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:
    a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist;
    b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.
3. Deze verordening is van toepassing op de verwerking van persoonsgegevens 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.

Artikel 4, AVG

Voor de toepassing van deze verordening wordt verstaan onder:

1) „persoonsgegevens”: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect 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;
2) „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;
3) „beperken van de verwerking”: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;
4) „profilering”: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;
5) „pseudonimisering”: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;
6) „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;
7) „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; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;
8) „verwerker”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
9) „ontvanger”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;
10) „derde”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, 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;

11) „toestemming" van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

12) „inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

13) „genetische gegevens": persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;

14) „biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

15) „gegevens over gezondheid": persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

16) „hoofdvestiging":

    a) met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd;

    b) met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;

17) „vertegenwoordiger": een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;

18) „onderneming": een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;

19) „concern": een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend;

20) „bindende bedrijfsvoorschriften": beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;

21) „toezichthoudende autoriteit": een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;

22) „betrokken toezichthoudende autoriteit": een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat:

    a) de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd;

b) de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of

c) bij die toezichthoudende autoriteit een klacht is ingediend;

23) „grensoverschrijdende verwerking”;

a) verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of

b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden;

24) „relevant en gemotiveerd bezwaar”: een bezwaar tegen een ontwerpbesluit over het bestaan van een inbreuk op deze verordening of over de vraag of de voorgenomen maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangetoond van de risico's die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;

25) „dienst van de informatiemaatschappij”: een dienst als gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (1);

26) „internationale organisatie”: een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.

Artikel 5, AVG

1. Persoonsgegevens moeten:

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie”);

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding”);

c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking”);

d) 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”);

e) 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; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking”);

f) 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”).

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht”).

Artikel 6, AVG

1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:
    a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
    b) 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;
    c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
    d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
    e) 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;
    f) 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.

De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

2. De lidstaten kunnen specifiekere bepalingen handhaven of invoeren ter aanpassing van de manier waarop de regels van deze verordening met betrekking tot de verwerking met het oog op de naleving van lid 1, punten c) en e), worden toegepast; hiertoe kunnen zij een nadere omschrijving geven van specifieke voorschriften voor de verwerking en andere maatregelen om een rechtmatige en behoorlijke verwerking te waarborgen, ook voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX.
3. De rechtsgrond voor de in lid 1, punten c) en e), bedoelde verwerking moet worden vastgesteld bij:
    a) Unierecht; of
    b) lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.

Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de in lid 1, punt e), bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX. Het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.

4. Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld niet berust op toestemming van de betrokkene of op een Unierechtelijke bepaling of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen houdt de verwerkingsverantwoordelijke bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld onder meer rekening met:
    a) ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;
    b) het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
    c) de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig artikel 9, en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig artikel 10;

d) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; e) het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

Artikel 7, AVG

1. Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.
2. Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.
3. 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.
4. Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

Artikel 8, AVG

1. Wanneer artikel 6, lid 1, punt a), van toepassing is in verband met 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.

De lidstaten kunnen dienaangaande bij wet voorzien in een lagere leeftijd, op voorwaarde dat die leeftijd niet onder 13 jaar ligt.

2. Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.
3. Lid 1 laat het algemene overeenkomstenrecht van de lidstaten, zoals de regels inzake de geldigheid, de totstandkoming of de gevolgen van overeenkomsten ten opzichte van kinderen, onverlet.

Artikel 9, AVG

1. Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.
2. Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan:
    a) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven;
    b) de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijk recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt;

c) de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;

d) de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;

e) de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;

f) de verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid;

g) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene;

h) de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;

i) de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim;

j) de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.

3. De in lid 1 bedoelde persoonsgegevens mogen worden verwerkt voor de in lid 2, punt h), genoemde doeleinden wanneer die gegevens worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden, of door een andere persoon die eveneens krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels tot geheimhouding is gehouden.

4. De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren.

Artikel 10, AVG

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid.

Artikel 11, AVG

1. Indien de doeleinden waarvoor een verwerkingsverantwoordelijke persoonsgegevens verwerkt, niet of niet meer vereisen dat hij een betrokkene identificeert, is hij niet verplicht om, uitsluitend om aan deze verordening te voldoen, aanvullende gegevens ter identificatie van de betrokkene bij te houden, te verkrijgen of te verwerken.
2. Wanneer de verwerkingsverantwoordelijke in de in lid 1 van dit artikel bedoelde gevallen kan aantonen dat hij de betrokkene niet kan identificeren, stelt hij de betrokkene daarvan indien mogelijk in kennis. In dergelijke gevallen zijn de artikelen 15 tot en met 20 niet van toepassing, behalve wanneer de betrokkene, met het oog op de uitoefening van zijn rechten uit hoofde van die artikelen, aanvullende gegevens verstrekt die het mogelijk maken hem te identificeren.

Artikel 12, AVG

1. De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking 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 met andere middelen bewezen is.
2. De verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene uit hoofde van de artikelen 15 tot en met 22. In de in artikel 11, lid 2, bedoelde gevallen mag de verwerkingsverantwoordelijke niet weigeren gevolg te geven aan het verzoek van de betrokkene om diens rechten uit hoofde van de artikelen 15 tot en met 22 uit te oefenen, tenzij de verwerkingsverantwoordelijke aantoont dat hij niet in staat is de betrokkene te identificeren.
3. De verwerkingsverantwoordelijke verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens de artikelen 15 tot en met 22 informatie over het gevolg dat aan het 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.
4. 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 een klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen.
5. Het verstrekken van de in de artikelen 13 en 14 bedoelde informatie, en het verstrekken van de communicatie en het treffen van de maatregelen bedoeld in de artikelen 15 tot en met 22 en artikel 34 geschieden kosteloos. Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de verwerkingsverantwoordelijke ofwel: a) 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 b) 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.
6. Onverminderd artikel 11 kan de verwerkingsverantwoordelijke, wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het verzoek indient als bedoeld in de artikelen 15 tot en met 21, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.
7. De krachtens de artikelen 13 en 14 aan betrokkenen te verstrekken 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 machineleesbaar.
8. De Commissie is bevoegd overeenkomstig artikel 92 gedelegeerde handelingen vast te stellen om te bepalen welke informatie de iconen dienen weer te geven en via welke procedures de gestandaardiseerde iconen tot stand dienen te komen.

Artikel 13, AVG

1. Wanneer persoonsgegevens betreffende een betrokkene bij die persoon worden verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens al de volgende informatie:
    a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;
    b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;
    c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;
    d) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd; d) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
    e) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.
2. Naast de in lid 1 bedoelde informatie verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens de volgende aanvullende informatie om een behoorlijke en transparante verwerking te waarborgen:
    a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
    b) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
    c) wanneer de verwerking op artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
    d) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
    e) of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
    f) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
3. Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.
4. De leden 1, 2 en 3 zijn niet van toepassing wanneer en voor zover de betrokkene reeds over de informatie beschikt.

Artikel 14, AVG

1. Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie:
    a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;
    b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;
    c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking;

d) de betrokken categorieën van persoonsgegevens;

e) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;

f) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een ontvanger in een derde land of aan een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van de in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

2. Naast de in lid 1 bedoelde informatie verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie om ten overstaan van de betrokkene een behoorlijke en transparante verwerking te waarborgen:

a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

b) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd;

c) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens of om beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking van bezwaar te maken en het recht op gegevensoverdraagbaarheid;

d) wanneer verwerking op artikel 6, lid 1, punt a) of artikel 9, lid 2, punt a), is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;

e) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;

f) de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen;

g) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

3. De verwerkingsverantwoordelijke verstrekt de in de leden 1 en 2 bedoelde informatie:

a) 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;

b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of

c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

4. 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 bedoeld in lid 2.

5. De leden 1 tot en met 4 zijn niet van toepassing wanneer en voor zover:

a) de betrokkene reeds over de informatie beschikt;

b) het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen, of voor zover de in lid 1 van dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt de verwerkingsverantwoordelijke passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;

c) het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of

d) de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van

Artikel 15, AVG

1. 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 van die persoonsgegevens en van de volgende informatie:
    a) de verwerkingsdoeleinden;
    b) de betrokken categorieën van persoonsgegevens;
    c) de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
    d) indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
    e) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
    f) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
    g) wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
    h) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
2. Wanneer persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie, heeft de betrokkene het recht in kennis te worden gesteld van de passende waarborgen overeenkomstig artikel 46 inzake de doorgifte.
3. De verwerkingsverantwoordelijke verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt. Indien de betrokkene om bijkomende kopieën verzoekt, kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding aanrekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.
4. Het in lid 3 bedoelde recht om een kopie te verkrijgen, doet geen afbreuk aan de rechten en vrijheden van anderen.

Artikel 16, AVG

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken.

Artikel 17, AVG

1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:
    a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
    b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), berust, in, en er is geen andere rechtsgrond voor de verwerking;
    c) de betrokkene maakt overeenkomstig artikel 21, lid 1, bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking overeenkomstig artikel 21, lid 2;
    d) de persoonsgegevens zijn onrechtmatig verwerkt;

e) de persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

f) de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als bedoeld in artikel 8, lid 1.

2. Wanneer de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

3. De leden 1 en 2 zijn niet van toepassing voor zover verwerking nodig is:

a) voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;

b) voor het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;

c) om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9, lid 2, punten h) en i), en artikel 9, lid 3;

d) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, voor zover het in lid 1 bedoelde recht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;

e) voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Artikel 18, AVG

1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen indien een van de volgende elementen van toepassing is:

a) 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;

b) 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;

c) 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;

d) de betrokkene heeft overeenkomstig artikel 21, lid 1, 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.

2. Wanneer de verwerking op grond van lid 1 is beperkt, worden persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.

3. Een betrokkene die overeenkomstig lid 1 een beperking van de verwerking heeft verkregen, wordt door de verwerkingsverantwoordelijke op de hoogte gebracht voordat de beperking van de verwerking wordt opgeheven.

Artikel 19, AVG

De verwerkingsverantwoordelijke stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie of wissing 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.

Artikel 20, AVG

1. De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machineleesbare 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, indien:
    a) de verwerking berust op toestemming uit hoofde van artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), of op een overeenkomst uit hoofde van artikel 6, lid 1, punt b); en
    b) de verwerking via geautomatiseerde procedés wordt verricht.
2. Bij de uitoefening van zijn recht op gegevensoverdraagbaarheid uit hoofde van lid 1 heeft de betrokkene het recht dat de persoonsgegevens, indien dit technisch mogelijk is, rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere worden doorgezonden.
3. De uitoefening van het in lid 1 van dit artikel bedoelde recht laat artikel 17 onverlet. Dat recht geldt niet voor de verwerking die noodzakelijk is 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 verleend.
4. Het in lid 1 bedoelde recht doet geen afbreuk aan de rechten en vrijheden van anderen.

Artikel 21, AVG

1. De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens op basis van artikel 6, lid 1, onder e) of f), van artikel 6, lid 1, met inbegrip van profilering op basis van die bepalingen. De verwerkingsverantwoordelijke staakt de verwerking van de persoonsgegevens tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.
2. Wanneer persoonsgegevens ten behoeve van direct marketing worden verwerkt, heeft de betrokkene te allen tijde het recht bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens voor dergelijke marketing, met inbegrip van profilering die betrekking heeft op direct marketing.
3. Wanneer de betrokkene bezwaar maakt tegen verwerking ten behoeve van direct marketing, worden de persoonsgegevens niet meer voor deze doeleinden verwerkt.
4. Het in de leden 1 en 2 bedoelde recht wordt uiterlijk op het moment van het eerste contact met de betrokkene uitdrukkelijk onder de aandacht van de betrokkene gebracht en duidelijk en gescheiden van enige andere informatie weergegeven.
5. In het kader van het gebruik van diensten van de informatiemaatschappij, en niettegenstaande Richtlijn 2002/58/EG, mag de betrokkene zijn recht van bezwaar uitoefenen via geautomatiseerde procedés waarbij wordt gebruikgemaakt van technische specificaties.
6. Wanneer persoonsgegevens overeenkomstig artikel 89, lid 1, met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, heeft de betrokkene het recht om met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

Artikel 22, AVG

1. De betrokkene heeft het recht niet te 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.
2. Lid 1 geldt niet indien het besluit:
    a) noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
    b) is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
    c) berust op de uitdrukkelijke toestemming van de betrokkene.

3. In de in lid 2, punten a) en c), bedoelde gevallen treft de verwerkingsverantwoordelijke passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.
4. De in lid 2 bedoelde besluiten worden niet gebaseerd op de in artikel 9, lid 1, bedoelde bijzondere categorieën van persoonsgegevens, tenzij artikel 9, lid 2, punt a) of g), van toepassing is en er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene zijn getroffen.

Artikel 23, AVG

1. De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 20, worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:
    a) de nationale veiligheid;
    b) landsverdediging;
    c) de openbare veiligheid;
    d) 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;
    e) andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
    f) de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
    g) de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
    h) een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a), tot en met e) en punt g) bedoelde gevallen;
    i) de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
    j) de inning van civielrechtelijke vorderingen.
2. De in lid 1 bedoelde wettelijke maatregelen bevatten met name specifieke bepalingen met betrekking tot, in voorkomend geval, ten minste:
    a) de doeleinden van de verwerking of van de categorieën van verwerking,
    b) de categorieën van persoonsgegevens,
    c) het toepassingsgebied van de ingevoerde beperkingen,
    d) de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte,
    e) de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken,
    f) de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking,
    g) de risico's voor de rechten en vrijheden van de betrokkenen, en
    h) het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

Artikel 24, AVG

1. 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.
2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen.

Artikel 25, AVG

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en 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 welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.
2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om 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. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.
3. Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.

Artikel 26, AVG

1. 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 en hun respectieve verplichtingen om de in de artikelen 13 en 14 bedoelde informatie te verstrekken, door middel van een onderlinge regeling, tenzij en voor zover de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijken zijn vastgesteld bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijken van toepassing is. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.
2. Uit de in lid 1 bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.
3. Ongeacht de voorwaarden van de in lid 1 bedoelde regeling, kan de betrokkene zijn rechten uit hoofde van deze verordening met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

Artikel 27, AVG

1. Wanneer artikel 3, lid 2, van toepassing is, wijst de verwerkingsverantwoordelijke of de verwerker schriftelijk een vertegenwoordiger in de Unie aan.
2. De verplichting vervat in lid 1 van dit artikel geldt niet voor:

a) incidentele verwerking die geen grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, betreft noch verwerking van persoonsgegevens die verband houden met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10, en waarbij de kans gering is dat zij een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, rekening houdend met de aard, de context, de omvang en de verwerkingsdoeleinden; of

b) een overheidsinstantie of overheidsorgaan.

3. De vertegenwoordiger is gevestigd in een van de lidstaten waar zich de betrokkenen bevinden wier persoonsgegevens in verband met het hun aanbieden van goederen of diensten worden verwerkt, of wier gedrag wordt geobserveerd.
4. Teneinde de naleving van deze verordening te waarborgen, wordt de vertegenwoordiger door de verwerkingsverantwoordelijke of de verwerker gemachtigd om naast hem of in zijn plaats te worden benaderd, meer bepaald door de toezichthoudende autoriteiten en betrokkenen, over alle met de verwerking verband houdende aangelegenheden.
5. Het feit dat de verwerkingsverantwoordelijke of de verwerker een vertegenwoordiger aanwijzen, doet niet af aan de mogelijkheid om tegen de verwerkingsverantwoordelijke of de verwerker zelf vorderingen in te stellen.

Artikel 28, AVG

1. Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, 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.
2. De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. 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.
3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht 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 of andere rechtshandeling bepaalt met name dat de verwerker:

    a) de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;

    b) waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;

    c) alle overeenkomstig artikel 32 vereiste maatregelen neemt;

    d) aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;

    e) rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;

    f) rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;

g) na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;

h) de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt. Waar het gaat om de eerste alinea, punt h), stelt de verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

4. Wanneer een verwerker een andere verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in de in lid 3 bedoelde 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. 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.
5. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat voldoende garanties als bedoeld in de leden 1 en 4 van dit artikel worden geboden.
6. Onverminderd een individuele overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker kan de in de leden 3 en 4 van dit artikel bedoelde overeenkomst of andere rechtshandeling geheel of ten dele gebaseerd zijn op de in de leden 7 en 8 van dit artikel bedoelde standaardcontractbepalingen, ook indien zij deel uitmaken van de certificering die door een verwerkingsverantwoordelijke of verwerker uit hoofde van de artikelen 42 en 43 is verleend.
7. De Commissie kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure standaardcontractbepalingen vaststellen.
8. Een toezichthoudende autoriteit kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens het in artikel 63 bedoelde coherentiemechanisme standaardcontractbepalingen opstellen.
9. De in de leden 3 en 4 bedoelde overeenkomst of andere rechtshandeling wordt in schriftelijke vorm, waaronder elektronische vorm, opgesteld.
10. Indien een verwerker in strijd met deze verordening de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.

Artikel 29, AVG

Verwerking onder gezag van de verwerkingsverantwoordelijke of de verwerker De verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van de verwerkingsverantwoordelijke, tenzij hij Unierechtelijk of lidstaatrechtelijk tot de verwerking gehouden is.

Artikel 30, AVG

1. Elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:

    a) de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;

    b) de verwerkingsdoeleinden;

c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;

d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;

e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;

f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;

g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

2. De verwerker, en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register bevat de volgende gegevens:

a) de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de functionaris voor gegevensbescherming;

b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;

c) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;

d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

3. Het in de leden 1 en 2 bedoelde register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.

4. Desgevraagd stellen de verwerkingsverantwoordelijke of de verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker het register ter beschikking van de toezichthoudende autoriteit.

5. De in de leden 1 en 2 bedoelde verplichtingen zijn niet van toepassing op ondernemingen 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 bijzondere categorieën van gegevens, als bedoeld in artikel 9, lid 1, of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 betreft.

Artikel 31, AVG

De verwerkingsverantwoordelijke en de verwerker en, in voorkomend geval, hun vertegenwoordigers, werken desgevraagd samen met de toezichthoudende autoriteit bij het vervullen van haar taken.

Artikel 32, AVG

1. Rekening houdend 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, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) 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.

2. 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.
3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.
4. 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, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.

Artikel 33, AVG

1. Indien 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 overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, 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 toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.
2. De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
3. In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:
    a) 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;
    b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
    c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
    d) 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.
4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.
5. 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 toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

Artikel 34, AVG

1. 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.
2. 2.De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.
3. De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

a) 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;

b) de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

c) 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.

4. Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, 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 in lid 3 bedoelde voorwaarden is voldaan.

Artikel 35, AVG

1. Wanneer een soort 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 voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.
2. Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.
3. Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:
    a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
    b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of
    c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.
4. De toezichthoudende autoriteit stelt een lijst op van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling overeenkomstig lid 1 verplicht is, en maakt deze openbaar. De toezichthoudende autoriteit deelt die lijsten mee aan het in artikel 68 bedoelde Comité.
5. De toezichthoudende autoriteit kan ook een lijst opstellen en openbaar maken van het soort verwerking waarvoor geen gegevensbeschermingseffectbeoordeling is vereist. De toezichthoudende autoriteit deelt deze lijst mee aan het Comité.
6. Wanneer de in de leden 4 en 5 bedoelde lijsten betrekking hebben op verwerkingen met betrekking tot het aanbieden van goederen of diensten aan betrokkenen of op het observeren van hun gedrag in verschillende lidstaten, of op verwerkingen die het vrije verkeer van persoonsgegevens in de Unie wezenlijk kunnen beïnvloeden, past de bevoegde toezichthoudende autoriteit voorafgaand aan de vaststelling van die lijsten het in artikel 63 bedoelde coherentiemechanisme toe.
7. De beoordeling bevat ten minste:
    a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
    b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
    c) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en

d) 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.

8. Bij het beoordelen van het effect van de door een verwerkingsverantwoordelijke of verwerker verrichte verwerkingen, en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van de in artikel 40 bedoelde goedgekeurde gedragscodes naar behoren in aanmerking genomen.
9. 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.
10. Wanneer verwerking uit hoofde van artikel 6, lid 1, onder c) of e), haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is, de specifieke verwerking of geheel van verwerkingen in kwestie daarbij wordt geregeld, en er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een gegevensbeschermingseffectbeoordeling is uitgevoerd, zijn de leden 1 tot en met 7 niet van toepassing, tenzij de lidstaten het noodzakelijk achten om voorafgaand aan de verwerkingen een dergelijke beoordeling uit te voeren.
11. Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

Artikel 36, AVG

1. Wanneer uit een gegevensbeschermingseffectbeoordeling krachtens artikel 35 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 toezichthoudende autoriteit.
2. Wanneer de toezichthoudende autoriteit van oordeel is dat de in lid 1 bedoelde voorgenomen verwerking inbreuk zou maken op deze verordening, met name wanneer de verwerkingsverantwoordelijke het risico onvoldoende heeft onderkend of beperkt, geeft de toezichthoudende autoriteit binnen een maximumtermijn van acht weken na de ontvangst van het verzoek om raadpleging schriftelijk advies aan de verwerkingsverantwoordelijke en in voorkomend geval aan de verwerker, en mag zij al haar in artikel 58 bedoelde bevoegdheden uitoefenen. Die termijn kan, naargelang de complexiteit van de voorgenomen verwerking, met zes weken worden verlengd. Bij een dergelijke verlenging stelt de toezichthoudende autoriteit de verwerkingsverantwoordelijke en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van onder meer de redenen voor de vertraging. Die termijnen kunnen worden opgeschort totdat de toezichthoudende autoriteit informatie heeft verkregen waarom zij met het oog op de raadpleging heeft verzocht.
3. Wanneer de verwerkingsverantwoordelijke de toezichthoudende autoriteit uit hoofde van lid 1 raadpleegt, verstrekt hij haar informatie over:
    a) indien van toepassing, de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijke, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder voor verwerking binnen een concern;
    b) de doeleinden en de middelen van de voorgenomen verwerking;
    c) de maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van deze verordening;
    d) indien van toepassing, de contactgegevens van de functionaris voor gegevensbescherming;
    e) de gegevensbeschermingseffectbeoordeling waarin bij artikel 35 is voorzien; en
    f) alle andere informatie waar de toezichthoudende autoriteit om verzoekt.
4. De lidstaten raadplegen de toezichthoudende autoriteit bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel, of een daarop gebaseerde regelgevingsmaatregel in verband met verwerking.
5. Niettegenstaande lid 1 kunnen de verwerkingsverantwoordelijken lidstaatrechtelijk ertoe worden verplicht overleg met de toezichthoudende autoriteit te plegen en om haar voorafgaande toestemming te verzoeken wanneer

zij met het oog op de vervulling van een taak van algemeen belang verwerken, onder meer wanneer verwerking verband houdt met sociale bescherming en volksgezondheid.

Artikel 37, AVG

1. De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin:
    a) de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken;
    b) een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
    c) de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.
2. Een concern kan één functionaris voor gegevensbescherming benoemen, mits de functionaris voor gegevensbescherming vanuit elke vestiging makkelijk te contacteren is.
3. Wanneer de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie of overheidsorgaan is, kan één functionaris voor gegevensbescherming worden aangewezen voor verschillende dergelijke instanties of organen, met inachtneming van hun organisatiestructuur en omvang.
4. In andere dan de in lid 1 bedoelde gevallen kunnen of, indien dat Unierechtelijk of lidstaatrechtelijk is verplicht, moeten de verwerkingsverantwoordelijke of de verwerker of verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, een functionaris voor gegevensbescherming aanwijzen. De functionaris voor gegevensbescherming kan optreden voor dergelijke verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen.
5. De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen.
6. De functionaris voor gegevensbescherming kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten.
7. De verwerkingsverantwoordelijke of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de toezichthoudende autoriteit.

Artikel 38, AVG

1. De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
2. De verwerkingsverantwoordelijke en de verwerker ondersteunen de functionaris voor gegevensbescherming bij de vervulling van de in artikel 39 bedoelde taken 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.
3. De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken. Hij wordt door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft voor de uitvoering van zijn taken. De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.
4. Betrokkenen kunnen met de functionaris voor gegevensbescherming 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.
5. De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken overeenkomstig het Unierecht of het lidstatelijk recht tot geheimhouding of vertrouwelijkheid gehouden.

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

Artikel 39, AVG

1. De functionaris voor gegevensbescherming vervult ten minste de volgende taken:
    a) de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van deze verordening en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen;
    b) toezien op naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de 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 de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 35;
    d) met de toezichthoudende autoriteit samenwerken;
    e) optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 36 bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.
2. De functionaris voor gegevensbescherming 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.

H-3: INFORMATIE TE VERSTREKKEN AAN BETROKKENE(N)

TE VERSTREKKEN INFORMATIE WANNEER PERSOONSGEGEVENS BIJ DE BETROKKENE WORDEN VERZAMELD [ART. 13, AVG]

Wanneer persoonsgegevens betreffende een betrokkene bij die persoon worden verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens al de volgende informatie:

- de identiteit en de contactgegevens van de verwerkingsverantwoordelijke;
- in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;
- de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;
- de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking daarop is gebaseerd;
- in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een ontvanger in een derde land of aan een internationale organisatie.

Daarnaast verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens de volgende aanvullende informatie:

- de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
- dat de betrokkene het recht heeft op inzage, rectificatie, verwijdering of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;
- dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
- dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
- of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als eerder aangegeven. De eerder genoemde informatieverstrekking is niet nodig wanneer en voor zover de betrokkene reeds over de informatie beschikt.

TE VERSTREKKEN INFORMATIE WANNEER DE PERSOONSGEGEVENS NIET VAN DE BETROKKENE ZIJN VERKREGEN [ART. 14, AVG]

Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie:

- de identiteit en de contactgegevens van de verwerkingsverantwoordelijke;
- in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;
- de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking;
- de betrokken categorieën van persoonsgegevens;
- in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een ontvanger in een derde land of aan een internationale organisatie.

Daarnaast verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens de volgende aanvullende informatie:

- de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking daarop is gebaseerd;
- dat de betrokkene het recht heeft op inzage, rectificatie, verwijdering of beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking van bezwaar te maken en het recht op gegevensoverdraagbaarheid;
- dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
- dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
- de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

H-4: INHOUD VERWERKERSOVEREENKOMST

De volgende afspraken moeten in de overeenkomst worden opgenomen [**art. 28, lid 3, AVG**] en [**overweging 081**]:

- Met betrekking tot de gegevens en de verwerking:
  - Het onderwerp en de duur van de verwerking;
  - De aard en het doel van de verwerking;
  - Het soort persoonsgegevens en de categorieën van betrokkenen;
  - De rechten en verplichtingen van de verwerkingsverantwoordelijke;
  - De opdrachtgever (verwerkingsverantwoordelijke) beschikt over de toestemming van de betrokkene of een andere rechtmatige grondslag voor verwerking van de persoonsgegevens van deze betrokkene(n).

    Voorts dient rekening gehouden te worden met de specifieke taken en verantwoordelijkheden van de verwerker in het kader van de te verrichten verwerking (bijvoorbeeld in het kader van het samenstellen / controleren van een jaarrekening, de vrijheid van de accountant om daarin zelf zijn activiteiten / werkzaamheden te bepalen) en de rechten en vrijheden van de betrokkene;
- De verwerker de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een wettelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;
- De verwerker waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
- De verwerker passende technische en organisatorische maatregelen neemt en de effectiviteit daarvan ook kan aantonen. Dit houdt ook in dat van een verwerker in een andere lidstaat of buiten Unie wordt verwacht dat deze de beveiligingsmaatregelen naleeft, zoals die zijn gedefinieerd door de wetgeving van de staat waarin de verwerker is gevestigd;
- De verwerker geen andere verwerker (subverwerker) in dienst neemt zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke [**art. 28, lid 2, AVG**];
- De verwerker de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de rechten van de betrokkene te beantwoorden en de effectiviteit daarvan kan aantonen;
- De verwerker de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de beveiliging van verwerkingen en het melden van datalekken. In dit kader is het van belang om in de overeenkomst met de verwerker de volgende zaken te regelen:
  - dat de verwerker alle relevante incidenten (beveiligingslekken) meldt;
  - dat de verwerker eventueel zelf meldingen doet aan de AP (en zo nodig aan betrokkene) en zo ja, in welke concrete situaties. De verwerkingsverantwoordelijke blijft ook in dit geval eindverantwoordelijk voor de melding. Dit betekent dat de verwerker de verwerkingsverantwoordelijke op de hoogte stelt als hij een datalek meldt aan de AP;
  - dat de verwerkingsverantwoordelijke per incident (beveiligingslek / datalek) alle informatie ontvangt die hij nodig heeft;

- op welke manier de verwerkingsverantwoordelijke wordt geïnformeerd over een incident en de tijdigheid daarvan;
- dat de verwerkingsverantwoordelijke op de hoogte wordt gehouden van eventuele nieuwe ontwikkelingen rond het incident, en van de maatregelen die de verwerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen;
- op welke wijze de verwerkingsverantwoordelijke kan vaststellen dat hij daadwerkelijk op de hoogte wordt gesteld van alle relevante incidenten, en dat de verstrekte informatie klopt;

- De verwerker na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens wettelijk is verplicht;
- De verwerker de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de overeengekomen afspraken aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt. De verwerker stelt de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

H-5: REGISTER VAN VERWERKINGSACTIVITEITEN

VERWERKINGSREGISTER VOOR DE VERWERKINGSVERANTWOORDELIJKE

Dit register bevat alle volgende gegevens:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de FG;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- wie toegang heeft tot deze gegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in [**art. 49, lid 1, tweede alinea**], bedoelde doorgiften, de documenten inzake de passende waarborgen;
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in [**art. 32, lid 1 AVG**].

VERWERKINGSREGISTER VOOR DE (SUB)VERWERKER

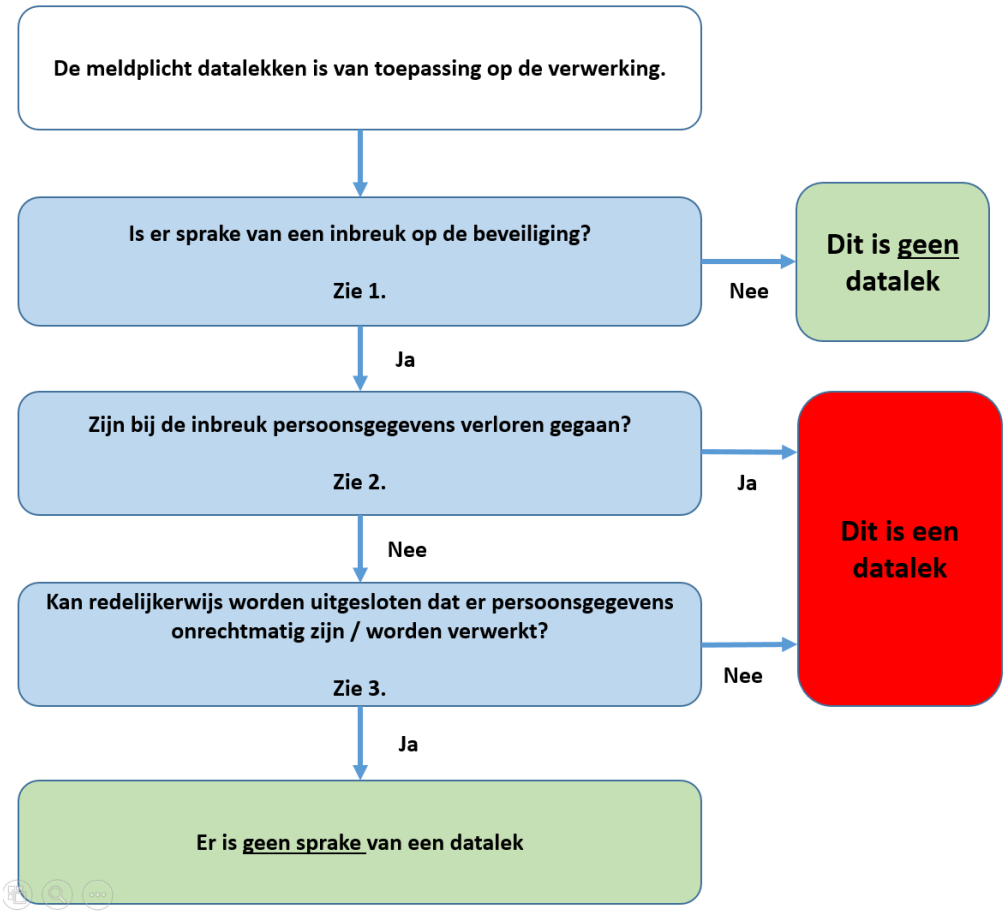
Dit register bevat de volgende gegevens [**art. 30, lid 2, AVG**]:

- de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de FG;
- de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke **zijn uitgevoerd**;
- wie toegang heeft tot deze gegevens;
- indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in [**art. 49, lid 1, tweede alinea**], bedoelde doorgiften, de documenten inzake de passende waarborgen.
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in [**art. 32, lid 1 AVG**], mede met als doel om de naleving van de verordening aan te kunnen tonen. De toezichthouder kan naar deze registratie van verwerkingsactiviteiten vragen tonen [**overweging 082, AVG**].

H-6: WANNEER IS ER SPRAKE VAN EEN DATALEK

Het onderstaande schema en beslissingstabel zijn gebaseerd op de [**art, 33 en 34, AVG**] en de publicatie van de AP inzake meldplicht datalekken [**AP-1**], en geeft de vragen weer die u moet beantwoorden om vast te stellen of sprake is van een datalek. Uitgangspunt is dat de meldplicht datalekken van toepassing is op de verwerking waarover het gaat. Mocht nog niet duidelijk zijn of dat het geval is, doorloop dan [**II, H-6**].

Het is belangrijk dat onderstaande beslistabel onderdeel uitmaakt van een protocol datalekken, omdat een datalek binnen 72 uur bij de AP moet worden gemeld.



Afbeelding 12

1. IS ER SPRAKE VAN EEN INBREUK OP DE BEVEILIGING?

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die u eventueel heeft getroffen waren niet toereikend om dit te voorkomen.

Bij beveiligingsincidenten waar sprake kan zijn van een inbreuk op de beveiliging van persoonsgegevens kan zijn:

- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;

- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Kenmerkend voor een inbreuk op de beveiliging is verder dat het beveiligingsincident daadwerkelijk gevolgen heeft voor de persoonsgegevens die u verwerkt. Er zijn persoonsgegevens verloren gegaan, of u kunt niet redelijkerwijs uitsluiten dat er persoonsgegevens onrechtmatig zijn verwerkt. De repressieve maatregelen en de herstelmaatregelen die u eventueel heeft getroffen waren niet voldoende om deze gevolgen geheel weg te nemen.

Een inbreuk op de beveiliging van persoonsgegevens moet ruim worden geduid. Het is niet van belang of u passende technische of organisatorische maatregelen heeft getroffen of niet. Een datalek kan zich in beide situaties voordoen.

2. ZIJN BIJ DE INBREUK PERSOONSGEGEVENS VERLOREN GEGAAN?

Verlies houdt in dat u de persoonsgegevens niet meer heeft. Bij het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan, en u beschikt niet over een complete en actuele reservekopie van de gegevens. In deze situatie is er sprake van een datalek.

Voorbeeld wel / geen datalek (verlies van persoonsgegevens)

Een database met persoonsgegevens is vernietigd als gevolg van een menselijke fout van een systeembeheerder. Van de database is een complete, actuele back-up beschikbaar, op basis waarvan de database direct weer wordt opgebouwd. In deze situatie is er geen sprake van een datalek.

De aard van het beveiligingsincident is niet relevant voor de vraag of er al dan niet sprake is van een datalek. Er is ook sprake van een datalek als de persoonsgegevens verloren zijn gegaan als gevolg van een calamiteit en er geen actuele reservekopie beschikbaar is.

3. KAN REDELIJKERWIJS WORDEN UITGESLOTEN DAT ER PERSOONSGEGEVENS ONRECHTMATIG ZIJN / WORDEN VERWERKT?

Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. Als u redelijkerwijs niet kunt uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet u de inbreuk beschouwen als een datalek.

Voorbeeld wel / geen datalek (onrechtmatige verwerking van persoonsgegevens)

Een werknemer geeft aan een derde de gebruikersnaam en het wachtwoord die toegang geven tot alle klantgegevens van alle klanten van het bedrijf waar hij werkt.

Na ontdekking van het gebeurde past het bedrijf het wachtwoord van het betreffende account aan, zodat de derde geen toegang meer heeft.

Daarna onderzoekt het bedrijf of de derde daadwerkelijk toegang heeft gezocht tot de klantgegevens. Bij dit onderzoek maakt het bedrijf gebruik van logbestanden, waarin per gebruikersnaam is vastgelegd welke acties er op welk tijdstip zijn uitgevoerd met welke klantgegevens.

Als op basis van de logbestanden redelijkerwijs kan worden uitgesloten dat er door middel van het betreffende account toegang is verkregen tot de klantgegevens, dan is er uitsluitend sprake van een beveiligingslek en niet van een datalek.

Bij een malware-besmetting moet u ervan uitgaan dat er sprake kan zijn van een datalek. Bepaalde typen malware doorzoeken de besmette apparatuur op waardevolle persoonsgegevens zoals e-mailadressen, gebruikersnamen en wachtwoorden en creditcardgegevens, om de gevonden gegevens vervolgens weg te sluizen naar een server die in handen is van de aanvaller. Een dergelijke malware-besmetting stelt de getroffen persoonsge-

gevens dus bloot aan onbevoegde kennisname en andere vormen van onrechtmatige verwerking. Andere typen malware maken bestanden ontoegankelijk voor de rechtmatige eigenaar door ze te blokkeren ('ransomware') of te versleutelen ('cryptoware'). Door deze vormen van malware worden de getroffen persoonsgegevens dus blootgesteld aan onbevoegde aantasting of wijziging.

H-7: WELKE GEGEVENS VASTLEGGEN OVER EEN INBREUK / DATALEK

De verwerkingsverantwoordelijke is alle inbreuken in verband met persoonsgegevens te documenteren, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen [**Art. 33, lid 5, AVG**]. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

In de AVG is geen gedetailleerd overzicht opgenomen van de te documenten gegevens. Maar het is mogelijk dat een op enig moment op grond terechte gronden niet gemelde inbreuk (datalek) toch nog kan leiden tot aanzienlijke schade. Dit betekent dat deze inbreuk alsnog aanleiding kan geven tot een melding aan de AP en mogelijk aan betrokkene(n).

Dit laatste kan zich bijvoorbeeld voordoen als u bij diefstal van een versleutelde dataset eerder heeft besloten om een melding aan de AP en de kennisgeving aan de betrokkene achterwege te laten. U moet zich er in een dergelijke situatie van bewust zijn dat de komst van nieuwe technieken nieuwe risico's kan inhouden, en dat er met grote regelmaat nieuwe kwetsbaarheden in breed gebruikte versleutelingsalgoritmen worden ontdekt. Dit houdt in dat u, met de diefstal van de versleutelde dataset in het achterhoofd, over een langere periode alert moet zijn op deze risico's. Bij signalen van mogelijke ontsleuteling zult u alsnog de afweging moeten maken of u deze inbreuk bij de AP moet melden en de betrokken persoon/personen moet informeren.

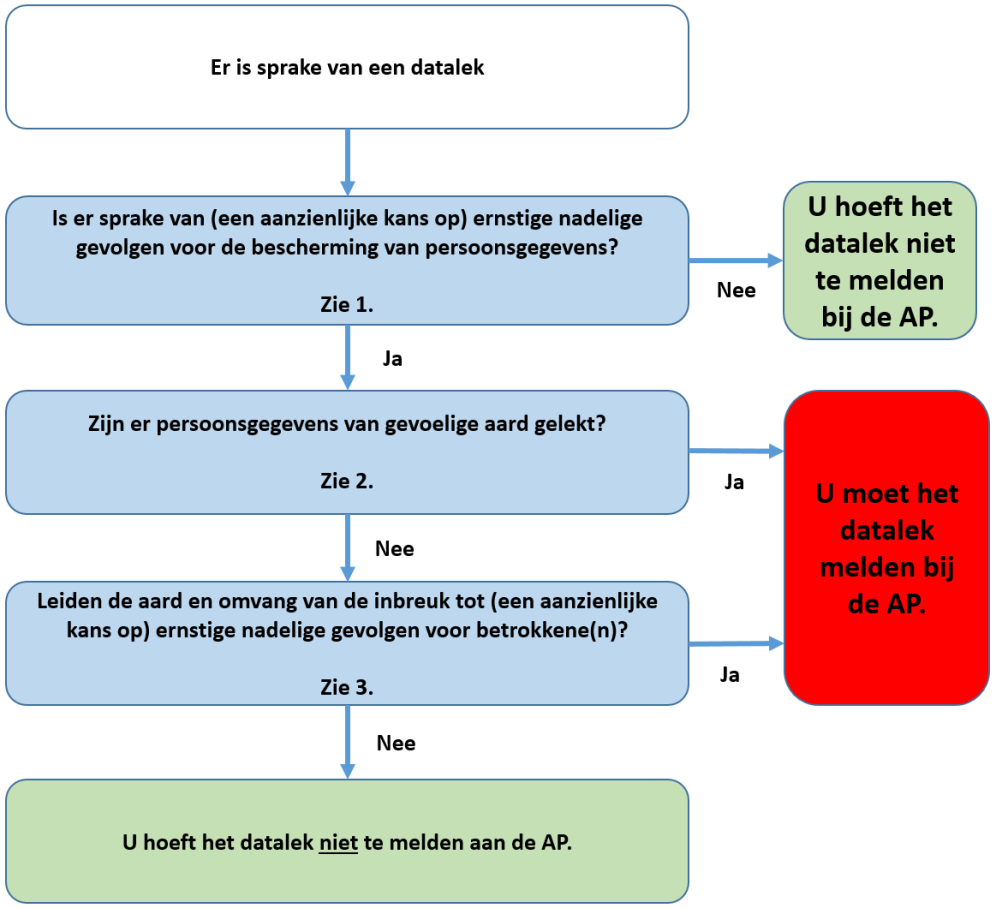
Houdt u er verder rekening mee dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat u waar dat aan de orde is het bewijsmateriaal moet verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Mede om die reden is het van belang dat de registratie van inbreuken alle informatie bevat die in een melding aan de AP moeten worden opgenomen, zie in dit verband [**II, H-9**].

H-8: MELDEN VAN EEN DATALEK AAN DE AP

Het onderstaande schema en beslissingstabel zijn gebaseerd op de [**art. 33** en **34, AVG**] en de publicatie van de AP inzake meldplicht datalekken [**AP-1**], en geeft de vragen weer die u moet beantwoorden om vast te stellen of u een specifiek datalek moet melden aan de Autoriteit Persoonsgegevens. Iedere vraag uit het onderstaande schema correspondeert met een paragraaf uit het vervolg. Uitgangspunt is dat er een gebeurtenis heeft plaatsgevonden waarvan u al heeft vastgesteld dat het gaat om een datalek. Mocht u dit nog niet hebben vastgesteld, doorloop dan eerst de vragen in [**II, H-8**].

Het is belangrijk dat onderstaande beslistabel onderdeel uitmaakt van een protocol datalekken, omdat een datalek binnen 72 uur bij de AP moet worden gemeld.



Afbeelding 13

1. IS ER SPRAKE VAN (EEN AANZIENLIJKE KANS OP) ERNSTIGE NADELIGE GEVOLGEN VOOR DE BESCHERMING VAN PERSOONSGEGEVENS?

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat u een inbreuk alleen hoeft te melden als deze leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (**art. 33, lid 1, AVG**).

Bij het beantwoorden van de vraag of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, moet u in ieder geval kijken naar de aard van de getroffen gegevens.

Voorbeelden van datalekken die moeten worden gemeld aan de Autoriteit Persoonsgegevens[1]

Intern wordt binnen een ziekenhuis gesignaleerd dat door een haperende beveiliging (technische storing) medische gegevens zijn ingezien door onbevoegden.

Een journalistiek programma confronteert een bedrijf met het feit dat als gevolg van een beveiligingslek onder andere persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen, bankgegevens en wachtwoorden) van werknemers op de server van het bedrijf door onbevoegden zijn ingezien.

Een medewerker verliest een laptop met onversleutelde, financiële klantgegevens.

Een bedrijf krijgt te maken met een hack waarbij klantgegevens en wachtwoorden zijn ontvreemd.

Een overheidsdatabase met gevoelige persoonsgegevens wordt gehackt waardoor onbevoegden toegang hebben gekregen tot deze gegevens.

Vier laptops zijn gestolen bij een gezondheidscentrum voor kinderen. De laptops bevatten gevoelige gegevens over gezondheid en welzijn en andere persoonsgegevens van meer dan 2000 kinderen.

Bij een levensverzekeraar zijn persoonsgegevens ongeoorloofd in te zien als gevolg van een kwetsbaarheid in een webapplicatie. Van 700 personen kunnen naam, adres en formulieren met medische gegevens worden ingezien.

Een medewerker van een internetprovider heeft zijn login/wachtwoordgegevens aan een derde partij gegeven die daardoor nagenoeg onbeperkt bij alle klantgegevens (meer dan 100.000) kon komen.

Een envelop met creditcardbetalingsgegevens van 800 personen was per ongeluk niet versnipperd, maar in een vuilnisbak gegooid. Een derde persoon haalde de gegevens uit de vuilniscontainer op straat en verstrekte ze aan andere personen.

De versleutelde laptop van een financieel adviseur is uit de auto gestolen. Financiële gegevens (hypotheken, salarissen, leningen) van 1000 personen waren betrokken. Hoewel het wachtwoord van de laptop niet gecompromitteerd is, was er geen back-up voorhanden.

Op de website van een telefoonbedrijf kunnen klanten inloggen en hun financiële gegevens en belgegevens inzien. Een derde partij heeft toegang gekregen tot de database met inlognamen en bijbehorende verhaspelde (onleesbaar gemaakte) wachtwoorden. Het is echter mogelijk dat bepaalde wachtwoorden achterhaald kunnen worden.

Een internetprovider biedt de gebruikers de mogelijkheid om details van hun account te zien, zoals onder andere historische zoekgegevens en vaak bezochte websites. Door een fout in de website had eenieder via een simpele truc de mogelijkheid om de accounts van andere gebruikers vrijelijk in te zien. Zonder een sluitende logging is hier niet vast te stellen of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd.

Voorbeelden van gebeurtenissen die niet onder de meldplicht vallen

Een brief met daarin persoonsgegevens wordt naar een foutief adres gestuurd, en wordt ongeopend retour gezonden.

Iemand laat een koffer met daarin persoonsgegevens achter in de trein. De koffer is voorzien van een deugdelijk slot, en komt via 'gevonden voorwerpen' ongeopend terug bij de rechtmatige eigenaar.

Het zoekraken of hacken van de ledenadministratie van een sportvereniging zal doorgaans leiden tot het nodige ongemak voor verenging en leden, maar zal niet snel aanleiding geven tot een melding bij het CBP.19 Dit kan overigens anders liggen als de sportvereniging zich bijvoorbeeld richt op personen met een specifieke levensovertuiging of seksuele geaardheid, of als er fraudegevoelige gegevens gelekt zijn.

Als ziekenhuispersoneel gebruik maakt van het wachtwoord van een arts om toegang te krijgen tot medische persoonsgegevens, dan is er niet zo zeer sprake van een datalek, als van schending van interne voorschriften. In eerste instantie liggen dan disciplinaire maatregelen voor de hand.

[1] Alle bovengenoemde voorbeelden zijn ontleend aan de parlementaire geschiedenis. De laatstgenoemde voorbeelden zijn oorspronkelijk afkomstig uit Advies 03/2014 van de Artikel 29-Werkgroep. In een aantal van deze voorbeelden wordt grote aantallen betrokkenen genoemd. Echter: de meldplicht kan ook van toepassing zijn op een datalek dat slechts betrekking heeft op de gegevens van één persoon.

2. ZIJN ER PERSOONSGEGEVENS VAN GEVOELIGE AARD GELEKT?

Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn? Bij dit laatste moet u bijvoorbeeld denken aan gegevens over betalingsachterstanden.

Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits)fraude. Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend:

- Bijzondere persoonsgegevens zoals bedoeld in [**art. 9, AVG**]. Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- Gegevens over de financiële of economische situatie van de betrokkene Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene Hieronder vallen bijvoorbeeld 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 gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen (bijvoorbeeld het medisch beroepsgeheim) moeten tot de persoonsgegevens van gevoelige aard worden gerekend.

Voorbeeld persoonsgegevens van gevoelige aard bij hack

Een hacker weet op de website van een lokale sportvereniging door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een twintigtal abonnees op een nieuwsbrief.

Normaal gesproken gaat het hier niet om persoonsgegevens van gevoelige aard. Dit wordt anders als de sportvereniging of de nieuwsbrief zich richt op mensen met, bijvoorbeeld, een specifieke levensovertuiging, politieke voorkeur of seksuele geaardheid.

3. LEIDEN DE AARD EN OMVANG VAN DE INBREUK TOT (EEN AANZIENLIJKE KANS OP) ERNSTIGE NADELIGE GEVOLGEN VOOR BETROKKENE(N)?

De aard en omvang van de getroffen verwerking is mede bepalend zijn voor de beantwoording van de vraag of er bij een datalek sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de bescherming van persoonsgegevens. Een datalek bij instellingen als de Belastingdienst, de Sociale Verzekeringsbank (SVB) of bij een commerciële bank of verzekeraar kan leiden tot financieel nadeel voor de betrokkene of tot het compromitteren van gegevens die beschermd worden door een geheimhoudingsplicht. Beveiligingslekken in de omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt kunnen ook zeer grote gevolgen hebben voor de betrokkenen.

Afgezien van de gevoelige aard van de verwerkte gegevens, die in de voorgaande paragraaf al aan de orde kwam, is voor de kans op ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens verder het volgende relevant:

- De omvang van de hierboven beschreven verwerkingen betekent dat het bij datalekken kan gaan om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen. Deze beide factoren maken een gelekte dataset aantrekkelijk voor misbruik in het criminele circuit. De kans dat de gelekte dataset wordt doorverkocht wordt daardoor ook groter, met als gevolg dat de betrokkenen langer last houden van het datalek.
- Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen van verlies en onbevoegde wijziging van de gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden.
- Bij omvangrijke verwerkingen van de overheid is vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken.

Als de aard en omvang van de getroffen verwerking voldoen aan het bovenstaande, dan moet u ervan uitgaan dat er (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aanwezig kan zijn.

Behalve voor de aard en de omvang van de getroffen verwerking, wordt in de parlementaire geschiedenis ook aandacht gevraagd voor de positie van kwetsbare groepen. Voor betrokkenen in kwetsbare groepen kan verlies of onrechtmatige verwerking van persoonsgegevens extra risico's met zich meebrengen. De gevolgen van onbevoegde toegang tot NAW-gegevens zullen bijvoorbeeld voor de meeste mensen beperkt zijn, maar dit ligt anders voor mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven. Voor bepaalde categorieën van betrokkenen, zoals kinderen en mensen met een verstandelijke handicap, kan het moeilijker zijn om adequaat om te gaan met de gevolgen van een datalek. Zo zullen zij mogelijk eerder ingaan op pogingen tot phishing of oplichting.

Als u weet dat u gegevens verwerkt van mensen in kwetsbare groepen, bijvoorbeeld omdat de verwerking zich specifiek richt op betrokkenen die hiertoe behoren, dan moet u ervan uitgaan dat bij een datalek (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aanwezig kan zijn.

Voorbeeld kwetsbare groepen

Een hacker weet op de website van een buurthuis door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een twintigtal abonnees op een elektronische nieuwsbrief. De nieuwsbrief richt zich op buurtbewoners van 65 jaar en ouder die bij het buurthuis een cursus volgen om vertrouwd te raken met het gebruik van computers en het internet. De aard van de doelgroep leidt hier tot extra risico's voor de betrokkenen. Gezien de onervarenheid van de betrokkenen met digitale communicatie bestaat er een aanzienlijk risico dat zij in zullen gaan op pogingen tot phishing of oplichting.

Bij een datalek als gevolg van een (niet-ethische) hack (art. 138ab van het Wetboek van Strafrecht), is van belang wat de aard van de gelekte persoonsgegevens is, en wat de risico’s van misbruik van deze persoonsgegevens voor de betrokkene zijn. Bij een hack zal melding al snel gepast zijn gelet op de risico’s van misbruik van persoonsgegevens. Bij een hack ligt ook aangifte bij de politie in de rede in verband met opsporing van de daders.

H-9: VRAGEN / GEGEVENS IN MELDING VAN EEN DATALEK AAN DE AP

Deze bijlage bevat een overzicht van de vragen die u moet beantwoorden en de informatie die u moet verstrekken bij een melding van een datalek aan de AP[2].

Een nieuwe melding doen

Voor het melden van een datalek vult u onderstaand formulier in.

Lees ook onze informatie over datalekken.

Nadat u een melding heeft gedaan, krijgt u een meldingsnummer te zien ter bevestiging. Registreer dit nummer voor verdere communicatie met de Autoriteit Persoonsgegevens.

Nieuwe of bestaande melding

- Gaat het om een nieuwe of bestaande melding?

Wettelijk kader van de melding

- Op grond van welke wettelijke bepaling doet u deze melding?

Algemene informatie en contactpersoon

- Over welke organisatie of welk bedrijf gaat het?
- Naam van het bedrijf of de organisatie
- Adres (bezoekadres)
- Postcode
- Vestigingsplaats
- Registratienummer bij de Kamer van Koophandel
- In welke sector is de organisatie of het bedrijf actief?
- Overige sector, te weten: ……

Wie meldt het datalek?

- Naam
- Functie
- E-mailadres
- Telefoonnummer
- Tweede telefoonnummer

[2] Dit overzicht is gebaseerd op de huidige melding via de website van de AP d.d. 5 mei 2017, in het kader van de Wbp. De onderzoekers verwachten dat de melding in het kader van de AVG dezelfde gegevens zal bevatten.

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

- De melder is contactpersoon?
- Naam contactpersoon
- Functie contactpersoon
- E-mailadres contactpersoon
- Telefoonnummer contactpersoon
- Tweede telefoonnummer contactpersoon

Gegevens over het datalek

- Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?
- Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest: ……
- Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie?
- Naam van de organisatie waaraan de verwerking is uitbesteed
- Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
- Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
- Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk: ……
- Is bekend wanneer de inbreuk was?
- Is de exacte datum bekend wanneer de inbreuk was?
- Exacte datum waarop de inbreuk was
- Startdatum van de periode waarbinnen de inbreuk was
- Einddatum van de periode waarbinnen de inbreuk was
- Wanneer werd de inbreuk ontdekt?

Wat is de aard van de inbreuk?

(Selecteer één of meerdere opties)

- Lezen (vertrouwelijkheid)
- Kopiëren
- Veranderen (integriteit)
- Verwijderen of vernietigen (beschikbaarheid)
- Diefstal
- Nog niet bekend

Om welk type persoonsgegevens gaat het?

(Selecteer één of meerdere opties en geef, indien van toepassing, een toelichting)

- Naam-, adres- en woonplaatsgegevens
- Telefoonnummers
- E-mailadressen of andere adressen voor elektronische communicatie

- Toegangs- of identificatiegegevens
- Financiële gegevens
- Burgerservicenummer (BSN)
- Paspoortkopieën of kopieën van andere legitimatiebewijzen
- Geslacht, geboortedatum en/of leeftijd

Bijzondere persoonsgegevens [art. 9, AVG])

- Over iemands godsdienst of levensovertuiging
- Over iemands ras
- Over iemands politieke gezindheid
- Over iemands gezondheid
- Over iemands seksuele leven
- Over het lidmaatschap van een vakvereniging
- Strafrechtelijke persoonsgegevens
- Over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag
- Overige / onbekend: ……

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

(Selecteer één of meerdere opties)

- Stigmatisering of uitsluiting
- Schade aan de gezondheid
- Blootstelling aan (identiteits)fraude
- Blootstelling aan spam of phishing
- Andere gevolgen, namelijk: ……

Vervolgacties naar aanleiding van het datalek

- Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen? : ……
- Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
- Wanneer heeft u het datalek gemeld aan de betrokkenen?
- Wanneer gaat u het datalek melden aan de betrokkenen?
- Wat is de inhoud van de melding aan de betrokkenen? : ……
- Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?
- Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren? : ……
- Waarom ziet u af van het melden van het datalek aan de betrokkenen?
- Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkenen, want: ……
- Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: …….

- Anders, namelijk: ……

Technische beschermingsmaatregelen

- Waren de persoonsgegevens op het moment van het ontdekken van het datalek versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?
- Deels, namelijk: ……
- Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?

Internationale aspecten

- Heeft de inbreuk betrekking op personen in andere EU-landen?
- Ja, namelijk: ……
- Heeft uw organisatie of bedrijf, het datalek gemeld bij toezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?
- Toezichthouder(s) van andere landen waar het datalek is gemeld: ……

Vervolgmelding

- Is naar uw mening deze melding compleet?

Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen en dat de in de melding verstrekte informatie juist is.

H-10: MELDEN VAN DATALEK AAN BETROKKENE

Het onderstaande schema en beslissingstabellen zijn gebaseerd op de [**art. 33** en **34, AVG**] en de publicatie van de AP inzake meldplicht datalekken [**AP-1**], en geeft de vragen weer die u moet beantwoorden om vast te stellen of u een specifiek datalek moet melden aan de betrokkene(n). Iedere vraag uit het onderstaande schema correspondeert met een paragraaf uit het vervolg. Uitgangspunt is dat er een gebeurtenis heeft plaatsgevonden waarvan u al heeft vastgesteld dat het gaat om een datalek dat u moet melden aan de AP. Mocht u dit nog niet hebben vastgesteld, doorloop dan eerst de vragen in [**II, H-10**].

Het is belangrijk dat onderstaande beslistabel onderdeel uitmaakt van een protocol datalekken, omdat een datalek binnen 72 uur bij de AP moet worden gemeld.

Afbeelding 16

Als u het datalek niet meldt aan de betrokkene kan de Autoriteit Persoonsgegevens, indien deze van oordeel is dat de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, van u verlangen dat u alsnog een kennisgeving doet aan de betrokkenen. Dit staat gelijk aan een bindende aanwijzing. Bij het niet nakomen van een bindende aanwijzing kan de AP een bestuurlijke boete opleggen.

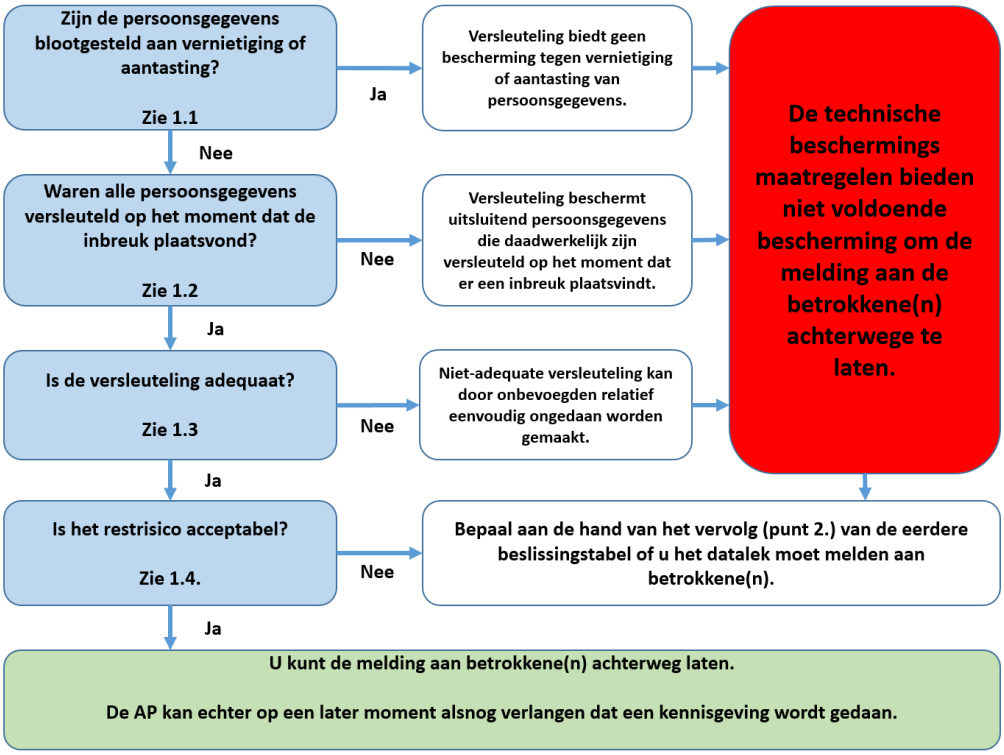
1. BIEDT DE CRYPTOGRAFIE DIE IS TOEGEPAST VOLDOENDE BESCHERMING OM DE MELDING AAN DE BETROKKENE(N) ACHTERWEGE TE LATEN?

Indien u passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, dan kunt u de melding aan de betrokkene achterwege laten.

Uit de wetsgeschiedenis komt de toepassing van cryptografie naar voren als het voornaamste voorbeeld van een technische beschermingsmaatregel. Deze paragraaf gaat in op het gebruik van cryptografie als technische beschermingsmaatregel om persoonsgegevens onbegrijpelijk of ontoegankelijk te maken voor onbevoegden. Andere technische beschermingsmaatregelen worden behandeld in het vervolg van de toelichting bij de beslissingstabel.

Deze toelichting gaat in op twee cryptografische bewerkingen: encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code). Kenmerkend voor encryptie is dat deze bewerking omkeerbaar is: door gebruik van de juiste sleutel kan de oorspronkelijke informatie worden verkregen (decryptie). Encryptie wordt onder meer gebruikt om gegevens te beveiligen die zijn opgeslagen op draagbare apparatuur en op verwijderbare media zoals USB-sticks. Hashing is een bewerking die van informatie, ongeacht de lengte, een unieke hashcode maakt die altijd even lang is (de lengte is afhankelijk van de gebruikte hashingmethode). Hashing wordt onder meer gebruikt bij de opslag en verwerking van wachtwoorden: op het moment dat de gebruiker een (nieuw) wachtwoord kiest, wordt de bijbehorende hashcode opgeslagen. Wanneer de gebruiker vervolgens inlogt, wordt de hashcode van het ingevoerde wachtwoord vergeleken met de opgeslagen hashcode en krijgt de gebruiker toegang tot het informatiesysteem als de codes overeenkomen.

Als door de cryptografische bewerkingen die u heeft toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kunt u de melding aan de betrokkene achterwege laten. Dit is een strenge norm, die u van geval tot geval toe moet passen op basis van de actuele stand van de techniek. Als u twijfelt over de adequaatheid van de technische beschermingsmaatregelen die u heeft getroffen, dan moet u het datalek melden aan de betrokkene. Doel van het vervolg van deze toelichting is om u bij deze afweging te ondersteunen.



Afbeelding 15

Iedere vraag uit het bovenstaande schema correspondeert met een van de onderstaande paragrafen.

1.1 Zijn de persoonsgegevens blootgesteld aan vernietiging of aantasting

Persoonsgegevens die adequaat zijn versleuteld kunnen bij een datalek nog steeds worden vernietigd, en ook aantasting of onbevoegde wijziging is nog steeds mogelijk (bijvoorbeeld door zogenoemde 'cryptoware', die de

reeds versleutelde gegevens nogmaals versleutelt met een sleutel die de verantwoordelijke uitsluitend tegen betaling in zijn bezit kan krijgen.)

Een datalek waarbij adequaat versleutelde persoonsgegevens niet alleen zijn blootgesteld aan onbevoegde kennisname, maar ook aan verlies of aan andere vormen van onrechtmatige verwerking, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan hem of haar worden gemeld.

Voorbeeld technische beschermingsmaatregelen bij verlies van persoonsgegevens

De versleutelde laptop van een financieel adviseur is gestolen uit de kofferbak van zijn auto. Op de laptop staan de financiële dossiers – met daarin onder meer details over hypotheken, salarissen en aanvragen van leningen – van 1000 betrokkenen.

Door de diefstal zijn deze gegevens blootgesteld aan onbevoegde kennisname. De financieel adviseur komt tot de conclusie dat alle gegevens op de harde schijf adequaat versleuteld zijn, en dat het restrisico acceptabel is. In principe zou hij de melding aan de betrokkene dus achterwege kunnen laten.

Echter: de financieel adviseur beschikt niet over een back-up (reserve-kopie) van de persoonsgegevens op de harde schijf. Dat betekent dat er in dit geval niet alleen sprake is van blootstelling aan onbevoegde kennisname, maar ook van het verlies van de getroffen persoonsgegevens.

Aangezien de financieel adviseur de gegevens niet meer heeft, zal hij ze opnieuw bij de betrokkenen op moeten vragen. De vertraging die hierdoor ontstaat, kan ertoe leiden dat deadlines voor de indiening van documenten of aanvragen niet worden gehaald, wat voor de betrokkenen uiteindelijk kan leiden tot boetes, derving van inkomsten of verwachte winst, beëindiging van koopovereenkomsten of andere ingrijpende gevolgen.

In dit geval ligt het, ondanks de genomen technische beschermingsmaatregelen, voor de hand om het datalek te melden aan de betrokkenen. De melding omvat in ieder geval het verzoek om de gegevens opnieuw aan de financieel adviseur te verstrekken en een uitleg van de potentiële consequenties en negatieve gevolgen van de inbreuk.

1.2 WAREN ALLE PERSOONSGEGEVENS VERSLEUTELD OP HET MOMENT DAT DE INBREUK PLAATSVOND?

Versleuteling beschermt uitsluitend persoonsgegevens die daadwerkelijk versleuteld zijn op het moment dat er een inbreuk plaatsvindt. Een datalek waarbij (ook) niet versleutelde persoonsgegevens zijn gelekt, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan hem of haar worden gemeld.

Voorbeeld persoonsgegevens die niet waren versleuteld op het moment dat de inbreuk plaatsvond

Op de harde schijf van een laptop staat een bestand met persoonsgegevens. Het bestand zelf is niet versleuteld. De laptop wordt automatisch vergrendeld als deze enige tijd niet wordt gebruikt, en bij de automatische vergrendeling wordt de inhoud van de harde schijf versleuteld. De laptop is in handen gekomen van een aanvaller die met technische middelen gebruik van het toetsenbord simuleert, en daardoor voorkomt dat de automatische vergrendeling in werking treedt en de gegevens op de harde schijf worden versleuteld.

Voorbeeld waarin niet alle getroffen persoonsgegevens waren versleuteld, en de resterende persoonsgegevens niet waren versleuteld op het moment van de inbreuk.

Een werknemer geeft aan een derde de gebruikersnaam en het wachtwoord dat toegang geeft tot alle klantgegevens van alle klanten van het bedrijf waar hij werkt. Het gaat onder meer om namen, adressen, e-mailadressen, telefoonnummers, toegangs- en andere identificatiegegevens (gebruikersnamen, gehashte wachtwoorden en klantnummers) en versleutelde betaalgegevens (waaronder rekeningnummers en creditcardgegevens). Om twee redenen moet de verantwoordelijke dit datalek melden aan de betrokkene:

- slechts een deel van de persoonsgegevens is versleuteld (de wachtwoorden en de betaalgegevens);

- de betaalgegevens zijn weliswaar versleuteld opgeslagen, maar als de derde met de verstrekte gegevens inlogt krijgt hij via de gebruikersinterface toegang tot de onversleutelde gegevens.

1.3 IS DE VERSLEUTELING ADEQUAAT?

Het is in eerste instantie aan u om te beoordelen of de versleuteling sterk genoeg is, en op de juiste wijze wordt uitgevoerd.

Zowel encryptie als hashing zijn in principe te 'kraken', wat inhoudt dat onbevoegden toegang kunnen krijgen tot de oorspronkelijke gegevens. Kraken wordt tegengegaan door het gebruik van (combinaties van) moderne cryptografische technieken en door toepassing van zogenoemde salts (extra informatie die bij hashing wordt toegevoegd aan het oorspronkelijke gegeven om het kraken van de hashcode te bemoeilijken). Dit terrein ontwikkelt zich voortdurend en het is zeer goed mogelijk dat een cryptografische bewerking die in de huidige situatie veilig genoeg is dat over enige tijd niet meer is. Bij gebruik van cryptografische bewerkingen beoordeelt u daarom periodiek of deze nog steeds voldoende bescherming bieden.

De Europese verordening 611/2013 geeft een nadere invulling aan adequate versleuteling. Volgens deze verordening mag u gegevens als onbegrijpelijk beschouwen als ze:

- op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of
- zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.35

Aandachtspunten bij de beoordeling zijn:

- Het algoritme zelf, of de wijze waarop u dit toepast, kunnen kwetsbaarheden vertonen waardoor de encryptie of de hashing niet de bescherming biedt die u daarvan verwacht.
- Encryptie is omkeerbaar. Een onbevoegde die over de juiste sleutel beschikt, of deze zonder al te veel moeite kan vinden, kan de gelekte gegevens ontsleutelen.
- Hashing is herhaalbaar. Als er bij hashing geen salt is toegepast, of als een onbevoegde over de gebruikte salt beschikt of deze zonder al te veel moeite kan vinden, kan hij de gebruikte hashingmethode toepassen op een lijst met veelgebruikte waarden en daardoor bijvoorbeeld gestolen wachtwoorden achterhalen.

Algemene informatie over algoritmen en toepassingen daarvan vindt u onder meer in de publicaties van het European Union Agency for Network and Information Security (ENISA) en het Nationaal Cyber Security Centrum (NCSC). Bij het opstellen van deze beleidsregels was de meest recente publicatie van ENISA op dit gebied het 'Algoritms, key sizes and parameters report – 2014' dat werd gepubliceerd in november 2014 [**ENISA-1**].

Behalve het gebruikte algoritme zelf, is voor adequate versleuteling ook van belang dat u dit op de juiste wijze toepast. Een beoordeling door een deskundige kan hier uitsluitsel over bieden. Bij voorkeur vindt deze beoordeling plaats voordat er een datalek heeft plaatsgevonden zodat u, op het moment dat zich een datalek voordoet, gemakkelijk kunt bepalen of de encryptie of de hashing die u heeft toegepast voldoende bescherming biedt.

Als laatste is van belang dat de gebruikte sleutel c.q. salt niet is gelekt. Dit zult u van geval tot geval vast moeten stellen.

1.4 IS HET RESTRISICO ACCEPTABEL?

Door de beantwoording van de voorgaande vragen heeft u, als het goed is, een beeld gekregen van de mate waarin de technische beschermingsmaatregelen die u heeft genomen de gelekte persoonsgegevens beschermen tegen onbevoegde kennisname. Per concreet geval zult u moeten beoordelen of de geboden bescherming voldoende is om de kennisgeving aan de betrokkene achterwege te kunnen laten.

Behalve met wat hierboven is aangegeven, moet u ook meewegen welke gevolgen het voor de persoonlijke levenssfeer van de betrokkene kan hebben als een aanvaller er nu of in de toekomst alsnog in slaagt om kennis te nemen van de getroffen persoonsgegevens.

Voorbeeld achterwege laten melding betrokkene bij encryptie

Een laptop, met op de harde schijf een bestand met persoonsgegevens, is gestolen. De verantwoordelijke onderzoekt het incident, en komt tot de conclusie dat hij op grond van het zesde lid van artikel 34a Wbp af mag zien van de melding aan de betrokkene. Zijn overwegingen daarbij zijn:

- bij de versleuteling van het bestand is gebruik gemaakt van combinatie van algoritme en sleutellengte die door het ENISA in een actuele (niet door een recentere publicatie achterhaalde) handreiking wordt beoordeeld als 'toekomst-vast voor de komende 10 tot 50 jaar;
- met betrekking tot het gebruikte algoritme en de implementatie daarvan zijn geen kwetsbaarheden bekend;
- de implementatie is met goed gevolg beoordeeld door een deskundige;
- het bestand zelf was versleuteld, dus de versleuteling was niet afhankelijk van automatische vergrendeling die in het specifieke geval mogelijk niet heeft gewerkt;
- de sleutel is niet gelekt;
- gezien de aard van het datalek, de verwerking en de gelekte gegevens is het restrisico acceptabel.

2. BIEDEN DE ANDERE TECHNISCHE BESCHERMINGSMAATREGELEN DIE ZIJN GENOMEN VOLDOENDE BESCHERMING OM DE MELDING AAN DE BETROKKENE(N) ACHTERWEGE TE LATEN?

Naast encryptie vermeldt de Nederlandse wetsgeschiedenis nog een andere technische beschermingsmaatregel waarmee persoonsgegevens kunnen worden beschermd tegen onbevoegde kennisname: het op afstand wissen van de gegevens die op een apparaat staan (remote wiping). Door de gegevens te wissen worden deze ontoegankelijk voor onbevoegden, aangezien na een geslaagde remote wipe een eventuele aanvaller nog wel de beschikking heeft over het apparaat waarop de gegevens stonden, maar niet meer over de gegevens zelf. Een remote wipe heeft echter uitsluitend kans van slagen als er aan een aantal randvoorwaarden wordt voldaan. De eerste randvoorwaarde is dat de remote wipe tijdig in gang wordt gezet, zodat een eventuele aanvaller nog geen kans heeft gehad om kennis te nemen van de gegevens. Verder moet op dat moment het apparaat waar het om gaat nog intact zijn en werken, zodat het in staat is om de remote wipe uit te voeren en de gegevens te wissen. Ook moet de toepassing die voor het wissen van de gegevens wordt gebruikt correct werken, zodat alle gegevens waar het om gaat daadwerkelijk worden verwijderd en er ook geen sporen achterblijven waaruit de oorspronkelijke gegevens kunnen worden gereconstrueerd.

Als u gebruik maakt van remote wiping, dan zult u op basis van de specifieke omstandigheden van het geval vast moeten stellen of er wordt voldaan aan de strenge beveiligingseisen [**art. 32, AVG**]. De voorgaande paragrafen kunt u daarbij gebruiken als leidraad.

Ook als de gelekte gegevens gepseudonimiseerd zijn zult u op basis van de specifieke omstandigheden van het geval vast moeten stellen of er aan de norm beveiligingseisen wordt voldaan. Pseudonimisering wil zeggen dat u technische maatregelen heeft genomen om te voorkomen dat de persoonsgegevens worden gekoppeld aan

de oorspronkelijke identiteit van de betrokkene. Geslaagde pseudonimisering maakt de persoonsgegevens waarover het gaat tot op zekere hoogte onbegrijpelijk voor onbevoegden en de kans dat een datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene wordt als gevolg daarvan verlaagd. Onvolkomenheden in de wijze waarop de persoonsgegevens zijn gepseudonimiseerd kunnen er echter toe leiden dat onbevoegden de oorspronkelijke identiteit van de betrokkenen alsnog kunnen achterhalen, eventueel met gebruikmaking van andere gegevens die ze reeds in hun bezit hadden of alsnog in hun bezit krijgen.

Net als bij remote wiping zult u dus ook bij blootstelling van gepseudonimiseerde gegevens aan onbevoegde kennisname op basis van de specifieke omstandigheden van het geval moeten vaststellen of er wordt voldaan aan de strenge beveiligingseisen. De onderstaande paragrafen kunt u daarbij gebruiken als leidraad. Verder is aan te bevelen om bij de beoordeling gebruik te maken van het advies over anonimiseringstechnieken dat de samenwerkende Europese toezichthouders in 2014 hebben uitgebracht.

3. ZAL HET DATALEK WAARSCHIJNLIJK ONGUNSTIGE GEVOLGEN HEBBEN VOOR DE PERSOONLIJKE LEVENSSFEER VAN DE BETROKKENE(N)?

Het datalek moet aan de betrokkene worden gemeld indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer [**art. 34, AVG**].

Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn. Bij dit laatste moet u bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen.

Het is aan u om te beoordelen of u een datalek aan de betrokkene moet melden.

Indien er persoonsgegevens van gevoelige aard zijn gelekt, dan moet u er van uitgaan dat u het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene. Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of (identiteits)fraude.

In alle overige gevallen zult u op basis van de omstandigheden van het geval een afweging moeten maken.

Het informeren van de betrokkene over een opgetreden datalek is met name noodzakelijk in situaties waarin er voor hem of haar daadwerkelijk ongunstige gevolgen voor de persoonlijke levenssfeer te duchten zijn. Door de kennisgeving is de betrokkene alert op de mogelijke gevolgen van het datalek en kan hij of zij zich, voor zover dat mogelijk is, daartegen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen (zoals vervanging van een wachtwoord) of door diensten of producten van een andere marktpartij af te nemen.

Voorbeelden van datalekken die moeten worden gemeld aan de betrokkene

1. Vier laptops zijn gestolen bij een gezondheidscentrum voor kinderen. De laptops bevatten gevoelige gegevens over gezondheid en welzijn en andere persoonsgegevens van meer dan 2000 kinderen. Gelet op de mogelijke gevolgen van het datalek is kennisgeving aan de betrokkenen geboden. Daarbij is het wel belangrijk om rekening te houden met de leeftijd en de rijpheid van de betrokkenen. Naast de kennisgeving aan het kind zelf, voor zover deze passend is, kan het in dit geval juister zijn om een ouder of voogd, die al actief betrokken is bij de medische verzorging van het kind, op de hoogte te brengen. Door de kwijtgeraakte gegevens kan de integriteit van de medische dossiers worden aangetast, wat de behandeling van de kinderen kan verstoren. Als de ouders of verzorgers op de hoogte zijn van het datalek dan kunnen ze hier alert op zijn, en kunnen ze bij eventuele afwijkingen in de medische zorg voor hun kinderen contact opnemen met de betreffende zorgverlener.
2. Bij een levensverzekeraar waren persoonsgegevens ongeoorloofd ingezien als gevolg van een kwetsbaarheid in een webapplicatie. Van 700 personen konden naam, adres en formulieren met medische gegevens worden

ingezien. Als de aanvaller buitgemaakte gegevens op internet zet kan dat er bijvoorbeeld toe leiden dat betrokkenen moeilijker een baan kunnen vinden, als gevolg van het bekend worden van informatie over gezondheidsproblemen, zwangerschap, etc. Betrokkenen kunnen ook te maken krijgen met phishing of identiteitsfraude. Het datalek heeft waarschijnlijk negatieve gevolgen voor de betrokkenen, die er daarom van in kennis moeten worden gesteld.

3. Een medewerker van een internetprovider heeft zijn login/wachtwoordgegevens aan een derde partij gegeven die daardoor nagenoeg onbeperkt bij alle klantgegevens (meer dan 100.000) kon komen. Het kan niet redelijkerwijs worden uitgesloten dat er daadwerkelijk persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. De derde partij had onder meer toegang tot betaalgegevens (waaronder creditcardinformatie) en hashwaarden van wachtwoorden van klanten. Misbruik van de betaalgegevens kan financiële gevolgen hebben voor de klanten. Ook is het mogelijk dat de onbevoegde derde op basis van de buitgemaakte hashwaarden de oorspronkelijke wachtwoorden van de klanten kan achterhalen. Het datalek heeft waarschijnlijk negatieve gevolgen voor de betrokkenen, die er daarom van in kennis moeten worden gesteld. Als de wachtwoorden niet meer veilig zijn, dan moet de verantwoordelijke de klanten op een veilige manier verplichten om een nieuw wachtwoord aan te maken. Hij moet daarbij zorgen dat de nieuwe wachtwoorden worden aangemaakt door legitieme gebruikers, en niet door derden die de inloggegevens hebben bemachtigd. Hij moet daarbij ook aangeven wat de reden is voor de vervanging van het wachtwoord.

4. Een envelop met creditcardbetalingsgegevens van 800 personen was per ongeluk niet versnipperd, maar in een vuilnisbak gegooid. Een derde persoon haalde de gegevens uit de vuilniscontainer op straat en verstrekte ze aan andere personen. Het datalek kan financiële consequenties hebben voor de betrokkenen, als hun kaartgegevens nog geldig zijn en worden misbruikt. De betrokkenen moeten daarom van het datalek in kennis worden gesteld.

5. De versleutelde laptop van een financieel adviseur is uit de auto gestolen. Financiële gegevens (hypotheken, salarissen, leningen) van 1000 personen waren betrokken. Hoewel het wachtwoord van de laptop niet gecompromitteerd is, was er geen back-up voorhanden. Aangezien de verantwoordelijke niet meer beschikt over de persoonsgegevens die op de laptop stonden, zullen deze opnieuw door de betrokkenen moeten worden verstrekt. Op zich heeft dit slechts beperkte negatieve gevolgen voor de betrokkenen: er is hooguit sprake van frustratie en tijdverspilling omdat ze alle informatie nogmaals moeten verzamelen. In sommige gevallen kunnen ook deadlines voor de indiening van documenten of aanvragen worden overschreden, wat kan leiden tot financiële schade voor de betrokkenen. De betrokkenen moeten van het datalek in kennis worden gesteld. In de kennisgeving moet worden aangegeven dat de gegevens opnieuw aan de financieel adviseur moeten worden verstrekt, en moet uitleg worden gegeven over de potentiële consequenties en mogelijke negatieve gevolgen van het datalek.

6. Op de website van een telefoonbedrijf kunnen klanten inloggen en hun financiële gegevens en belgegevens inzien. Een derde partij heeft toegang gekregen tot de database met inlognamen en bijbehorende hashwaarden van wachtwoorden. Bij het hashen van de wachtwoorden is gebruik gemaakt van een verouderd algoritme dat onvoldoende bescherming biedt tegen kennisname door onbevoegden. Gevolg is dat een derde partij de oorspronkelijke wachtwoorden zonder al te veel moeite zal kunnen achterhalen. [Dit voorbeeld heeft betrekking op de telecomsector, en valt dus niet onder de meldplicht datalekken uit de Wbp. De overwegingen bij het informeren van de betrokkenen kunnen echter ook buiten de telecomsector worden toegepast.] De derde partij kan de wachtwoorden van alle abonnees achterhalen. Hij beschikt ook over de inlognamen, en kan zich daardoor toegang verschaffen tot alle accounts. Veel mensen gebruiken voor het inloggen op meerdere websites dezelfde combinatie van inlognaam en wachtwoord. Dit betekent dat de derde zich met de buitgemaakte gegevens mogelijk ook toegang kan verschaffen tot andere accounts van sommige betrokkenen, waaronder mogelijk ook e-mailaccounts. Dit datalek heeft waarschijnlijk negatieve gevolgen voor de betrokkenen, en kennisgeving is vereist. De klanten moeten op de hoogte worden gesteld van het datalek, met daarbij het dringende advies om voor alle accounts waar ze hetzelfde wachtwoord gebruiken, dit wachtwoord aan te passen. Ze moeten bij het inloggen op de website in kwestie ook worden gedwongen om hun wachtwoord voor de kwestie aan te passen. Daarbij moet worden gezorgd dat de nieuwe wachtwoorden worden aangemaakt door legitieme gebruikers, en niet door derden die de inloggegevens hebben bemachtigd.

7. Een internetprovider biedt de gebruikers de mogelijkheid om details van hun account te zien, zoals onder andere historische zoekgegevens en vaak bezochte websites. Door een fout in de website had eenieder via een simpele truc de mogelijkheid om de accounts van andere gebruikers vrijelijk in te zien. Zonder een sluitende logging is hier niet vast te stellen of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd. [Dit voorbeeld heeft betrekking op de telecomsector, en valt dus niet onder de meldplicht datalekken uit de Wbp. De overwegingen bij het informeren van de betrokkenen kunnen echter ook buiten de telecomsector worden toegepast.] De gegevens kunnen worden gebruikt voor het versturen van spam aan de betrokkenen of voor telefonische verkoop of phishing. De buitgemaakte gegevens kunnen mogelijk ook worden gebruikt om profielen van de klanten op te stellen of hun gedragingen in kaart te brengen, wat gevoelige informatie aan het licht zou kunnen brengen. Dit datalek heeft waarschijnlijk negatieve gevolgen voor de betrokkenen, en moet daarom aan hen worden gemeld.

4. ZIJN ER ZWAARWEGENDE REDENEN OM DE MELDING AAN BETROKKENE(N) ACHTERWEG TE LATEN?

U mag de melding aan de betrokkene achterwege laten, als daarvoor zwaarwegende redenen aanwezig zijn [**art. 34, AVG**]. Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit noodzakelijk is met het oog op de belangen die worden genoemd in dit artikel.

Het melden van datalekken aan de betrokkenen brengt administratieve lasten met zich mee, maar op zichzelf is dat geen reden om de melding achterwege te laten. Alleen als u aannemelijk kunt maken dat de administratieve lasten die zijn gemoeid met het melden van het datalek aan de betrokkene zodanig disproportioneel zijn, kunt u een beroep doen op [**art. 34 lid 3.c, AVG**] om een melding aan de betrokkene achterwege te laten. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

In de kennisgeving aan de betrokkene vermeldt u in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in [**art. 33, lid 3 onder b), c) en d), AVG**] bedoelde gegevens en maatregelen.

Bij het beschrijven van de aard van de inbreuk kunt u doorgaans met een algemene omschrijving volstaan. U neemt uw contactgegevens op zodat de betrokkene u kan bereiken als hij of zij vragen heeft over het datalek. Verder geeft u aan wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken. U moet daarbij denken aan het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn. Het staat u vrij om meer informatie toe te voegen aan de kennisgeving, maar dit is niet verplicht.

Voorbeeld melding aan de betrokkene en vervolgacties

Een energieleverancier biedt zijn klanten een online account aan waarop ze kunnen inloggen om recente facturen en verbruiksinformatie te raadplegen. Het bedrijf ontdekt dat een derde zich illegaal toegang heeft verschaft tot de database met gebruikersnamen en wachtwoorden van de website. De wachtwoorden zijn niet adequaat versleuteld.

De energieleverancier onderneemt de volgende acties:

- hij informeert zijn klanten over het datalek. Hij beveelt daarbij aan om, voor alle accounts waar de klant hetzelfde wachtwoord gebruikt, dit wachtwoord te wijzigen;
- hij reset alle wachtwoorden en dwingt alle gebruikers om een nieuw wachtwoord op te geven. Hij doet dit op een veilige manier zodat hij zeker weet dat het zijn klanten zijn die een nieuw wachtwoord aanmaken, en niet een onbevoegde derde, en hij geeft hierbij ook aan waarom de klant een nieuw wachtwoord aan moet maken;
- hij past zijn systemen aan, zodat alle gebruikte wachtwoorden op een adequate manier worden versleuteld.

U doet de kennisgeving aan de betrokkene op zo'n manier dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

In veruit de meeste gevallen zult u als verantwoordelijke beschikken over de contactgegevens van de betrokkenen, en zult u in staat zijn om de betrokkenen individueel te informeren.

Bij meer omvangrijke incidenten kunt u kiezen voor een combinatie van algemene voorlichting en het op individuele basis informeren van betrokkenen. Bijvoorbeeld:

- U stuurt een e-mail naar de betrokkenen waarin u kort aangeeft wat er is gebeurd en wat de betrokkene zelf kan doen om de negatieve gevolgen tegen te gaan.
- In de e-mail aan de betrokkenen verwijst u naar meer uitgebreide informatie op uw website. Daar licht u de aard van de inbreuk en de maatregelen die de betrokkene zelf kan treffen waar nodig nader toe.
- Verder verwijst u in de e-mail naar een centraal informatiepunt (e-mail, telefoonnummer) waar de betrokkene nadere informatie kan verkrijgen.

Het belangrijkste is, dat u zo veel mogelijk betrokkenen bereikt met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaal gesproken niet bereikt.

U moet het datalek onverwijld melden aan de betrokkene [**art. 34, lid 1, AVG**].

Het onverwijld melden houdt in dat u, na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek zodat u de betrokkene op een behoorlijke en zorgvuldige manier kunt informeren. Wel moet u er rekening mee houden 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.

Net als bij de melding aan de AP kunt u er eventueel voor kiezen om de betrokkene in eerste instantie te informeren op basis van de informatie waarover u op dat moment beschikt, zodat deze alvast maatregelen kan gaan treffen om zich te beschermen tegen de gevolgen van het datalek, en om deze informatie in tweede instantie op basis van nader onderzoek aan te vullen. Een voorbeeld van een dergelijke situatie is dat u weet dat onbevoegden toegang hebben gehad tot een database met inloggegevens, maar dat u nog aan het onderzoeken bent of de onbevoegden ook andere persoonsgegevens hebben ingezien. U kunt in een dergelijk geval meteen al beginnen met het resetten van de getroffen wachtwoorden en met het informeren van de betrokkenen, waarbij u aangeeft dat betrokkenen, als zij elders dezelfde inloggegevens gebruiken, deze moeten wijzigen.

In de melding aan de AP moet u aangeven of u het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer u dat gaat doen. De termijn die u in de melding aan de AP aangeeft, moet u ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat u dit aan de AP weten door middel van een aanpassing van de melding.

H-11: PRIVACY IMPACT ASSESSMENT (PIA) [NOREA-4]

Een PIA maakt de privacy-risico's zichtbaar in nieuwe maar ook bestaande verwerkingen van persoonsgegevens en draagt bij aan het vermijden of verminderen van deze privacy-risico's. Op basis van een PIA wordt op systematische wijze inzichtelijk gemaakt hoe groot de kans is dat de privacy van de betrokken personen van wie gegevens worden verwerkt wordt geschaad, waar deze risico's zich voordoen en welke gevolgen daaraan voor hen verbonden zijn. Op basis van de uitkomsten van een PIA kunnen gerichte acties ondernomen worden om deze risico's te verminderen.

Met het van kracht worden van de AVG op 25 mei 2018 is een PIA verplicht bij het gebruik van nieuwe technologieën bij het verwerken van persoonsgegevens [**art. 35, AVG**]. Het verdient daarom aanbeveling een PIA onderdeel te laten uitmaken van de privacy strategie en het kwaliteitssysteem van een organisatie alsmede van de kwaliteitsbeheersing van projecten waardoor verwerking van persoonsgegevens tot stand komt.

Een PIA kent een aantal doelen. Het belangrijkste doel is:

1. Het voorkomen van kostbare aanpassingen in processen, herontwerp van systemen of stopzetten van een project door vroegtijdig inzicht in de belangrijkste privacy-risico's.

   Daarnaast kunnen nog de volgende doelen worden onderscheiden:
2. Het verminderen van de gevolgen van toezicht en handhaving.
3. Het verbeteren van de kwaliteit van gegevens.
4. Het verbeteren van de dienstverlening.
5. Het verbeteren van de besluitvorming.
6. Het verhogen van het privacy bewustzijn binnen een organisatie.
7. Het verbeteren van de haalbaarheid van een project.
8. Het verstevigen van het vertrouwen van de klanten, werknemers of burgers in de wijze waarop persoonsgegevens worden verwerkt en privacy wordt gerespecteerd.
9. Het verbeteren van de communicatie over privacy en de bescherming van persoonsgegevens.

Een PIA kan gebruikt worden door alle typen organisaties.

Een PIA bedoeld voor opdrachtgevers en opdrachtnemers van projecten en andere belanghebbenden. In het algemeen kan worden gezegd dat het zinvol is een PIA uit te voeren bij een nieuw project of grote wijziging van een bestaand systeem of proces waarbij persoonsgegevens worden verwerkt. Een PIA kan uiteraard ook op bestaande verwerkingen van persoonsgegevens worden toegepast, indien dat nog niet eerder is geschiedt.

Een PIA kan het beste gestart worden in een zeer vroeg stadium van een project. Vervolgens kan de verdere uitwerking van een PIA aansluiten bij de verdere uitwerking van het project. Op die manier helpt een PIA u om het privacybelang structureel mee te nemen in het project. Daarmee wordt een PIA een belangrijk onderdeel van het ontwerp proces.

Ook aanpassingen of wijzigingen van bestaande verwerkingen van persoonsgegevens rechtvaardigen een PIA. Op die manier kunt u voorkomen dat later kostbare aanpassingen nodig zijn om alsnog de noodzakelijke beheersmaatregelen met betrekking tot privacy te implementeren. Ook wanneer de omstandigheden van een project tijdens de looptijd veranderen, is het raadzaam een PIA te herhalen en/of te evalueren bij de afsluiting van een project. Een PIA is geen nalevingsinstrument, maar een risicoanalyse-instrument waarmee privacy-risico's kunnen worden geïdentificeerd en gelokaliseerd. Zie voor een nadere invulling de genoemde handreiking [**NOREA-4**].

H-12:SOORTEN BEVEILIGINGSMAATREGELEN

In de praktijk zijn verschillende vormen van beveiligingsmaatregelen te onderscheiden.

MAATREGELEN TE ONDERSCHEIDEN NAAR HUN SOORT

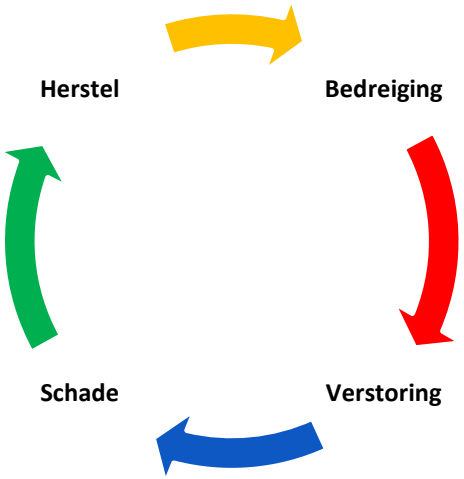
Maatregelen kunnen worden onderscheiden naar hun soort (verschijningsvorm). Een voorbeeld waar de drie hieronder genoemde soorten maatregelen van toepassing zijn, is de toegangsbeveiliging die wij op dit moment bij veel organisaties, maar ook op stations tegenkomen.

- **Organisatorische maatregelen**: In de organisatie is afgesproken wie bevoegd is tot het verlenen van toegang en op welke wijze deze toegang wordt verleend, alsmede de procedure om deze toegangsrechten te implementeren en te onderhouden. Andere voorbeelden zijn een duidelijk verdeling van taken/bevoegdheden/verantwoordelijkheden (functiescheiding) en duidelijke afspraken hoe wordt omgegaan met mobiele apparatuur, wachtwoorden en email.
- **Fysieke maatregelen**: Bijvoorbeeld de bekende toegangsspoortjes bij panden, maar ook het afsluiten van ruimtes of het beschermen van locaties door hekken in combinatie met water.
- **Logische maatregelen**: Dit zijn maatregelen die in de besturings- en applicatiesoftware worden getroffen. In dit voorbeeld de toegangspasjes in combinatie met de lezers in de beveiligingspoortjes, die bepalen of iemand wel of geen toegang krijgt tot het pand.

De keuze en het samenstel van maatregelen is sterk afhankelijk van de situatie, maar ook van de mogelijkheden die de techniek biedt. Gegevens de technische ontwikkelingen zien wij een verschuiving van fysieke naar meer logische maatregelen. De beveiliging van de NS-stations is daar een voorbeeld van, maar ook de paspoortcontrole op Schiphol, die gebruik maakt van een irisscan of een vingerafdruk bij het vaststellen of men te maken heeft met de juiste persoon.

MAATREGELEN TE ONDERSCHEIDEN NAAR HUN DOEL

Maatregelen kunnen ook worden onderscheiden naar hun doel en zijn gericht op een bepaald moment van de incidentencyclus, zie onderstaand figuur.



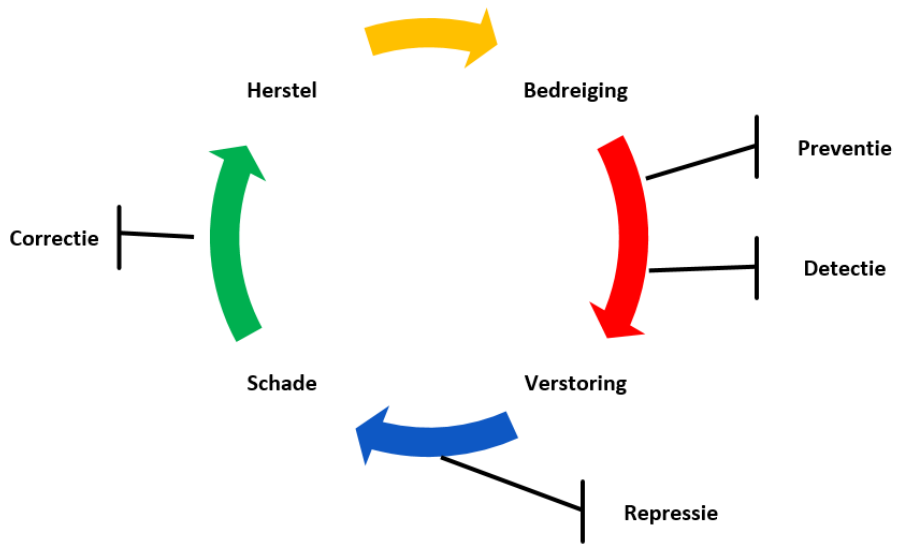
Afbeelding 16: De incidentencyclus

In de incidentencyclus worden achtereenvolgens vier stappen onderscheiden. Allereerst is er een **bedreiging**: iets dat zou kunnen gebeuren. Als dit verwezenlijkt wordt, spreken wij van een **verstoring**, oftewel een beveiligingsincident. Een beveiligingsincident is een incident die de betrouwbaarheid van een systeem, proces of data

aantast. Door dit incident ontstaat mogelijk **schade**, die vraagt om actie tot beperking van deze schade en daarna **herstel** van de schade.

Analoog aan de incidentencyclus kunnen wij de beveiligingsmaatregelen als volgt indelen. Hierbij is de brandbeveiliging van een pand als voorbeeld genomen.

- **Preventieve maatregelen**, met als doel het voorkomen dat bedreigingen leiden tot inbreuken (verstoring) en schade. Een voorbeeld in dit verband is het gebruik van onbrandbaar materiaal of het segmenteren van ruimtes (fysieke maatregelen), maar ook een rookverbod in bepaalde ruimtes (organisatorische maatregel).
- **Detectieve maatregelen**, met als doel het tijdig signaleren dat een bedreiging toch geleid heeft tot een incident, maar ook het registreren van activiteiten / handelingen. Een voorbeeld in dit verband zijn brand- en rookmelders of andere vormen van signalering.
- **Repressieve maatregelen**, met als doel de mogelijke schade, die door een bedreiging die niet is voorkomen, maar wel (tijdig) gesignaleerd schade, te beperken. Een voorbeeld in dit verband is de aanwezigheid van een sprinklerinstallatie of andere blusmiddelen (fysieke maatregelen).
- **Correctieve maatregelen**, met als doel de opgetreden schade weet te kunnen herstellen. Een voorbeeld in dit verband is de mogelijkheid om de verloren gegane goederen weer snel te kunnen vervangen (organisatorische maatregel).



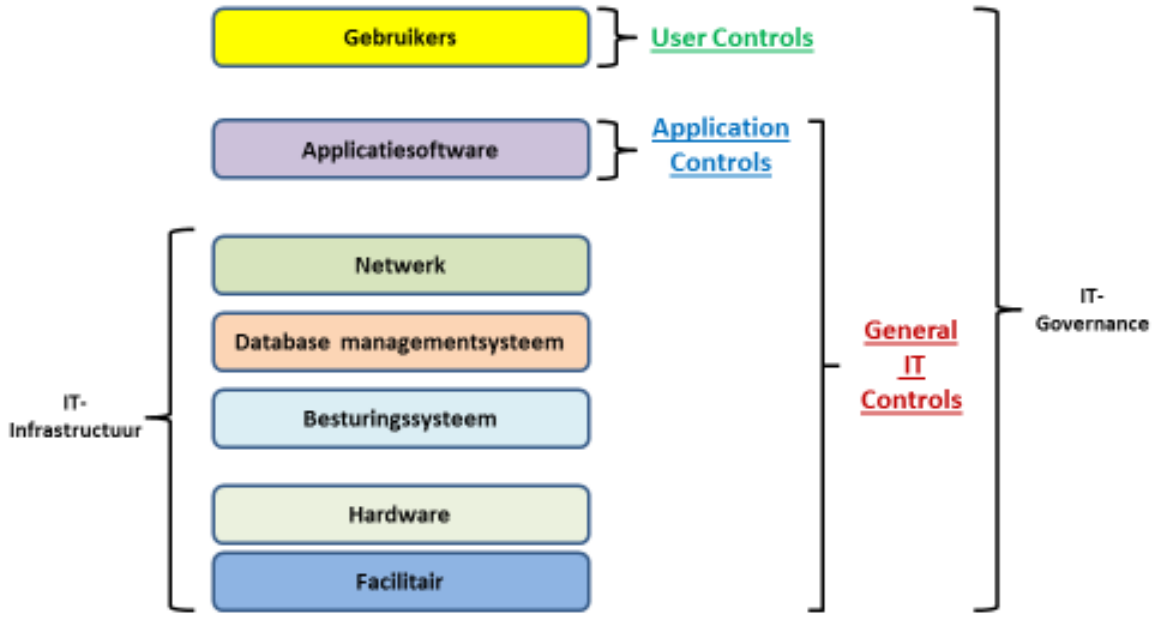
Afbeelding 17: Beveiligingscyclus

Het kan zijn dat een feitelijke maatregel meerder doelstellingen kan realiseren. Een voorbeeld daarvan is een snelheids- of bewakingscamera, die zowel een preventieve (voorkomende / afschrikwekkende) als een detectieve (signalering en registratie) werking heeft.

In het kader van informatiebeveiliging heeft het voorkomen van beveiligingsincidenten nog steeds een grote prioriteit, maar ook is duidelijk dat incidenten niet altijd kunnen worden voorkomen, dus is het zaak is dat de organisatie in staat is om inbreuken tijdig te kunnen detecteren, om daarna maatregelen te kunnen nemen om mogelijke schade te voorkomen of te beperken en daarna te herstellen. Dit vereist dus een samenstel van de vier genoemde soorten maatregelen.

MAATREGELEN TE ONDERSCHEIDEN NAAR HUN PLAATS

Maatregelen kunnen op verschillende plaatsen in de organisatie, systemen en processen worden getroffen. In de onderstaande figuur zij de verschillende vormen van maatregelen zichtbaar gemaakt.



Afbeelding 18: Plaats van maatregelen (Controls) in de organisatie, systemen en processen

- **User Controls** zijn maatregelen die in de gebruikersorganisatie worden getroffen. Voorbeelden zijn activiteiten die gebruikers moeten uitvoeren, zoals het vaststellen van verbanden, of het reageren op signaleringen.
- **Application Controls** zijn maatregelen die in de applicaties (toepassingen) worden getroffen. Voorbeelden zijn controles gericht op invoer (juistheid, volledigheid, bestaan of redelijkheid), verwerking (volgorde van handeling of verbanden) of uitvoer (totalen).
- **General IT Controls** zijn maatregelen gericht op de IT-infrastructuur als basis voor de applicaties. Voorbeelden zijn:
    - Het doorvoeren van functiescheidingen door middel van een toegangsbeveiligingssysteem dat gebruikers identificeert, hun identiteit controleert en op basis van autorisaties toegang verschaft tot processen en data;
    - Scheiding tussen de systeemontwikkeling / aanschaf / onderhoud en productie;
    - Back-up en recovery en continuity planning (korte en lange termijn);
    - Change management van zowel de applicaties als de IT-infrastructuur[3];
    - Probleem- en incident-management, de helpdeks die problemen oplost.

[3] Bij de cyberaanvallen in mei en juni 2017 bleken ondernemingen o.a. niet de geadviseerde patches (updates) van hun besturingssystemen te hebben doorgevoerd waardoor zij kwetsbaar waren voor dit virus en hun bedrijfsvoering ernstig werd verstoord en soms zelfs stilgelegd (o.a.: zestien Britse medische instellingen, de Spaanse telecomaanbieder Telefónica, de containerterminals van havenbedrijf APM, de parkeergarages van Q-Park, pakjesbezorger TNT Express als onderdeel van FedEx.

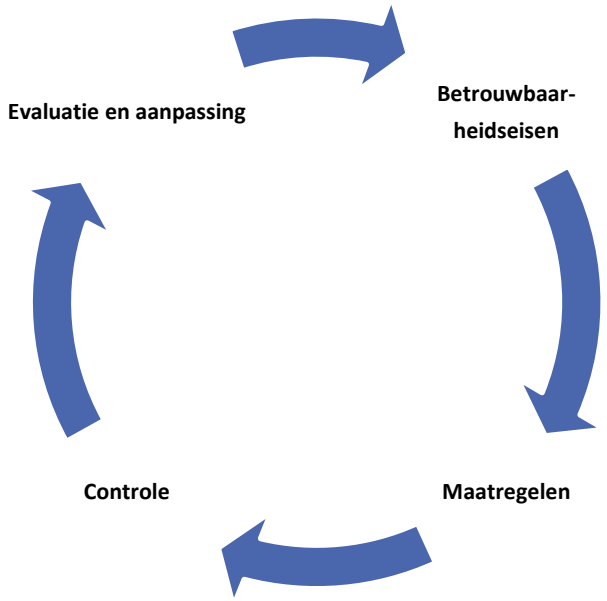
H-13: RISICOANALYSE

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

- Het een samenspel is van gebruikers, toepassingen (applicaties) en technische systemen;
- 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 Cloudcomputing);
- 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.

De **Plan >>> Do >>> Check >>> Act** cyclus of kwaliteitscirkel stelt de verantwoordelijke voor de informatiebeveiliging in staat om tot een blijvend passend beveiligingsniveau te komen. Het onderstaande schema geeft deze cyclus weer.



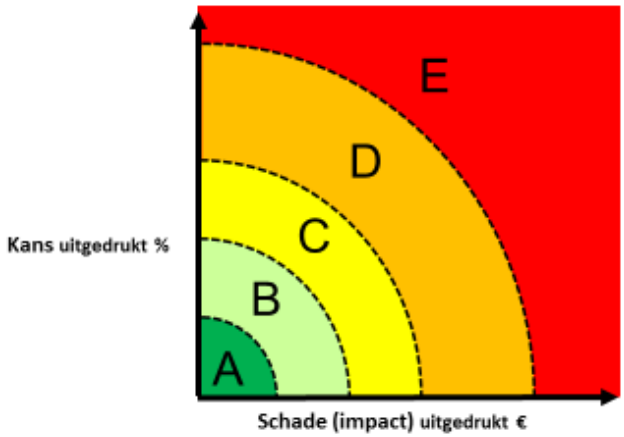
Afbeelding 19: Plan >>> Do >>> Check >>> Act cyclus

Vanuit de **Plan >>> Do >>> Check >>> Act** cyclus leidt dat tot de volgende vragen:

- Aan welke eisen of kwaliteitscriteria moet worden voldaan?
- Welke risico's worden onderkend en welke maatregelen kunnen hiertegen worden getroffen om het risico te mitigeren (verminderen)?
- Welke maatregelen zijn nodig om (doorlopend) de effectiviteit van de getroffen maatregelen vast te kunnen stellen?
- Op welke wijze wordt evaluatie ingevuld om waar nodig gerichte actie te kunnen nemen om de maatregelen aan te passen aan de gewijzigde omstandigheden, waardoor een blijvend passend beveiligingsniveau wordt bereikt en in stand gehouden?

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 passende maatregelen te treffen die een passend beveiligingsniveau garanderen. Onderstaand schema geeft de belangrijkste elementen uit de risicoanalyse weer, met daarbij de verschillende typen maatregelen die de verantwoordelijke kan treffen om de risico's af te dekken.



Afbeelding 20: Risicoanalyse

Risico is de **kans** dat een potentieel gevaar resulteert in een daadwerkelijk incident en de **schade** die dit tot gevolg heeft. Bij risicoanalyse wordt op basis van een analyse van mogelijke bedreigingen een inschatting gemaakt van de kans dat de betreffende bedreiging kan voorkomen en de mogelijke schade die daarvan het gevolg kan zijn. Vaak wordt dit uitgedrukt in bedrag in euro's. De dreigingen kunnen onder meer samenhangen met de specifieke kenmerken van de verwerking en de gebruikte technologie. Bij verwerking via internet is bijvoorbeeld hacking een dreiging waarmee rekening moet worden gehouden; bij verwerking op draagbare computers en opslag op draagbare geheugenmedia zijn vermissing en diefstal dreigingen die de verantwoordelijke in de risicoanalyse moet betrekken.

Een analyse van mogelijke bedreigingen (oorzakenanalyse) kan in hoofdlijn op verschillende wijzen worden ingevuld:

- Het inventariseren van mogelijke bedreigingen (scenario's) en toetsen welke impact die bedreigingen hebben op de realisatie van de kwaliteitseisen (bijvoorbeeld: wat zijn de mogelijke gevolgen van een ransomware-aanval, phishing-mails of brand in serverruimte?
- Bij elk (nieuw) component in de informatievoorziening bepalen wat de mogelijke impact is van de component op de gehele informatievoorziening ten aanzien van de kwaliteitseisen (Bijvoorbeeld: wat als gebruik gemaakt gat worden van een nieuwe Cloudleverancier).

Om een oorzakenanalyse uit te kunnen voeren is het noodzakelijk om de duidelijk beeld te hebben van de actuele inrichting van de informatievoorziening:

- Met welke soorten van gegevens (bedrijfsgegevens en (bijzondere) persoonsgegevens wordt door het MKB-kantoor gewerkt;
- Zijn er echt essentiële gegevens te onderkennen (kroonjuwelen) die nadrukkelijk om bescherming vragen (bijvoorbeeld inkomensgegevens van een publiek bekende cliënt);
- Op welke locaties/hardware worden welke gegevens vastgelegd en verwerkt. Bijvoorbeeld op lokale servers, mobiele laptops, USB-stick en/of in de Cloud;
- Met welke toepassingen (applicaties) wordt gewerkt en in welke samenhang (ketens);
- Met welke technische componenten wordt gewerkt;

- Welke stromen van gegevens zijn aanwezig en welke criteria worden daaraan gesteld (wel/niet encrypted, wel/niet geformaliseerd, transacties/gegevensverzamelingen);
- Wie heeft toegang tot welke gegevens en applicaties toegang en past dit binnen het 'Need to know' beleid;
- Over welke competenties beschikt de organisatie als het gaat om informatievoorziening en beveiliging van informatie;
- Welke wet- en regelgeving is op de informatievoorziening van toepassing. Dit is mede afhankelijk van het dienstenpakket en het terrein waarop het accountantskantoor werkzaam is. Bijvoorbeeld de zorgsector heeft eigen eisen voor informatiebeveiliging.

Het volledig wegnemen van risico's is in de praktijk onmogelijk. Daarnaast kunnen organisaties een verschillende niveau van risico-acceptatie hebben. Indien het ingeschatte risico (kans dat een bedreiging optreedt x mogelijke schade) te hoog is, kunnen maatregelen worden getroffen om het risico te verlagen. In het geval van het risico **E**, kan de kans verlaagd worden door het treffen van **preventieve** maatregelen in combinatie met **detectieve** maatregelen. De mogelijke schade kan worden verlaagd door het treffen van **detectieve** maatregelen in combinatie met **repressieve** maatregelen. De combinatie met **detectieve** maatregelen is essentieel, omdat deze signaleren dat ondanks de getroffen preventieve maatregelen een incident niet is voorkomen en actie vereist is om de schade te voorkomen of beperken.

Het verlagen van de kans hangt sterk af van de mogelijkheid om deze te beïnvloeden. Als voorbeeld een cyberaanval van buiten de organisatie. De kans dat een hacker binnendringt in de organisatie kan worden verlaagd door het treffen van preventieve maatregelen, zoals een goede toegangsbeveiliging, inclusief firewall. De ervaring leert dat niet alle aanvallen kunnen worden voorkomen, vandaar dat detectieve maatregelen, zoals intrusion detectie en monitoring van activiteiten op het netwerk, inbreuken tijdig kunnen signaleren. Een repressieve maatregel om de schade te beperken kan zijn het tijdelijk uitschakelen of afschakelen van onderdelen van het netwerk.

H-14: BEVEILIGINGSSTANDAARDEN & NORMEN-/BEHEERSINGSKADERS

In onderstaand overzicht zijn standaarden en normen-/beheersingskaders gericht op informatiebeveiliging en privacybescherming opgenomen. Deze zijn bruikbaar in het kader van dit rapport en doelgroep (MKB) en bieden praktische handvaten bij de invulling van informatiebeveiliging en privacybescherming.

STANDAARDEN GERICHT OP INFORMATIEBEVEILIGING

CODE VOOR INFORMATIEBEVEILIGING

Een zeer veel gebruikte beveiligingsstandaard is de Code voor Informatiebeveiliging: NEN-ISO/IEC 27001+C11+C1+C2:2015 (nl) [**NEN-1**] en NEN-ISO/IEC 27002+C1+C2:2015 (nl) [**NEN-2**]. Deze standaard is onderdeel van een groep onderling samenhangende standaarden voor het initiëren, implementeren, handhaven en verbeteren van de informatiebeveiliging in een organisatie. Voor de zorgsector is de Code voor Informatiebeveiliging nader uitgewerkt in de standaard NEN 7510 [**NEN-3**]. De Code voor Informatiebeveiliging en NEN 7510 zijn beveiligingsstandaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken. Het zijn algemene, technologie neutrale standaarden, wat betekent dat ze niet ingaan op de maatregelen die moeten worden getroffen bij een specifiek type verwerking of bij het gebruik van een specifieke technologie.

BEVEILIGINGSSTANDAARD VOOR CREDITCARDBETALINGEN

Er zijn ook beveiligingsstandaarden die dit wel doen. Voorbeelden zijn de Data Security Standard van de Payment Card Industry voor de veilige afhandeling van creditcardbetalingen [**PCI-1**].

BEVEILIGING VAN WEBAPPLICATIES

Voor de beveiliging van webapplicaties zijn er de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie [**NCSC-1**].

BEVEILIGING VAN MOBIELE APPARATEN

Voor de beveiliging van mobiele apparaten zijn er de beveiligingsrichtlijnen voor mobiele apparaten van het NCSC [**NCSC-2**].

BEVEILIGING VAN INDUSTRIËLE CONTROLESYSTEMEN

Industriële controlesystemen worden gebruikt voor de automatische monitoring en besturing van fysieke processen. Voorbeelden zijn de productie, het transport en de distributie binnen onze energie- en drinkwatervoorziening, de productieprocessen van raffinaderijen, de chemische, voedingsmiddelen en farmaceutische industrie. Maar ook camerabewakings-, klimaatregel- en andere gebouwbeheersystemen. Deze systemen blijken vaak direct vanaf internet bereikbaar te zijn. Veel organisaties zijn zich niet bewust van de risico's die dit met zich meebrengt. Daarnaast ontbreekt bij veel organisaties een actueel overzicht van alle systemen die met internet zijn verbonden. Hierdoor wordt niet altijd een gedegen inschatting van de risico's gemaakt en worden niet altijd de juiste maatregelen getroffen [**NCSC-4**] en [**NCSC-5**].

CLOUDCOMPUTING

Voor de beveiliging van cloudcomputing is er de standaard van het Amerikaanse National Institute of Standards and Technology [**NIST-1**]. Daarnaast hebben NEMACC en de NBA in 2014 twee publicaties gericht op de MKB-

accountant: De gevolgen van cloudcomputing voor de werkzaamheden van de mkb-accountant, een uitgebreid onderzoek (januari 2014) [**NEMACC-1**] en De mkb-accountant en Cloud Computing (november 2014) [**NBA-12**].

CYBERSECURITY

In opdracht van president Obama (Executive Order) heeft het Amerikaanse National Institute of Standards and Technology specifiek voor cybersecurity, een Framework for Improving Critical Infrastructure Cybersecurity [**NIST-2**] (februari 2014) opgesteld. Voor Critical infrastructure wordt een ruime definitie gehanteerd "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.". Het framework is opgebouwd volgens de lijn Identify – Protect – Detect – Respond – Recover en maakt gebruik van vele eerdere standaarden.

SOC FOR CYBERSECURITY

De Amerikaanse accountantsorganisatie AICPA heeft in april 2017 een Cybersecurity risk management reporting framework [**AICPA-1**] gepubliceerd. Het framework moet organisaties in staat stellen efficiënt te communiceren over de reikwijdte en de effectiviteit van de getroffen maatregelen in het kader van cyber security risk management. In aanvulling op de beschrijving geeft het management een bevestiging (Management's assertion). De controlerend accountant kan na attestatie de effectiviteit evalueren en daarover rapporteren.

VOLWASSENHEIDSMODEL INFORMATIEBEVEILIGING

In 2016 heeft de NBA-Ledengroep Intern en Overheidsaccountants (NBA LIO) en Handreiking bij Volwassenheidsmodel Informatiebeveiliging gepubliceerd, met als doel de interne audit afdelingen alsmede de directies van organisaties een leidraad en handvaten te geven waarmee zij doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging [**NBA-13**].

RISICOMANAGEMENT

NEN-ISO 31000 (2009) Risicomanagement - Principes en richtlijnen, geeft een kader voor integraal risicomanagement [**NEN-4**].

TOETSINGSKADER INFORMATIEBEVEILIGING

In 2017 heeft DNB het Toetsingskader Informatiebeveiliging voor DNB onderzoek 2017 gepubliceerd, dat zich richt op de wettelijke eisen voor de beveiliging van geautomatiseerde gegevensverwerking bij financiële instellingen [**DNB-1**].

BASELINE INFORMATIEBEVEILIGING NEDERLANDSE GEMEENTEN

De Nederlandse gemeenten hebben in 2016 een Strategische baseline informatiebeveiliging [**VNG-1**] en een Tactische-Baseline-Informatiebeveiliging [**VNG-2**] gepubliceerd. Deze baseline, die mede is gebaseerd op NEN-ISO 27001 en 27002 en biedt een uitgebreid overzicht van te treffen beveiligingsmaatregelen.

STANDAARDEN GERICHT OP PRIVACYBESCHERMING

PRIVACY-AUDIT-PROOF [NOREA-1]

In 2005 hebben de NBA en NOREA, in nauwe samenwerking met de AP (destijds het Cbp) en een aantal accountantskantoren een viertal producten ontwikkeld die bedrijven in staat stelt zelf na te gaan in hoeverre men voldoet aan de privacywetgeving. Daarnaast wordt ook de mogelijkheid geboden voor een externe beoordeling en

certificering. Van deze mogelijkheid wordt op dit moment door een aantal overheidsorganisaties gebruik gemaakt. Het eerder opgesteld normenkader is inmiddels via een addendum aangepast aan de nieuwe privacywetgeving. De volgende publicaties zijn beschikbaar:

- Richtlijn 3600 [**NOREA-2**]
- Addendum bij Richtlijn 3600n [**NOREA-3**]
- Raamwerk Privacy Audit [**CBP-3**]
- Handreiking bij het Raamwerk Privacy Audit [**CBP-7**]
- Instemming met richtlijn door Cbp [**CBP-6**]
- Richtsnoeren voor de beveiliging van persoonsgegevens [**CBP-2**]

Genoemde publicaties bieden een goede basis voor de inrichting van privacybescherming.

PRIVACY IMPACT ASSESSMENT (PIA)

Voor het kunnen uitvoeren van een Privacy Impact Assessment (PIA), zoals de nieuwe privacywet voorschrijft, heeft NOREA een handreiking gepubliceerd: Privacy Impact Assessment (PIA), Introductie, handreiking en vragenlijst, Versie 1.2 - November 2015 [**NOREA-4**].

AUTORITEIT PERSOONSGEGEVENS (AP)

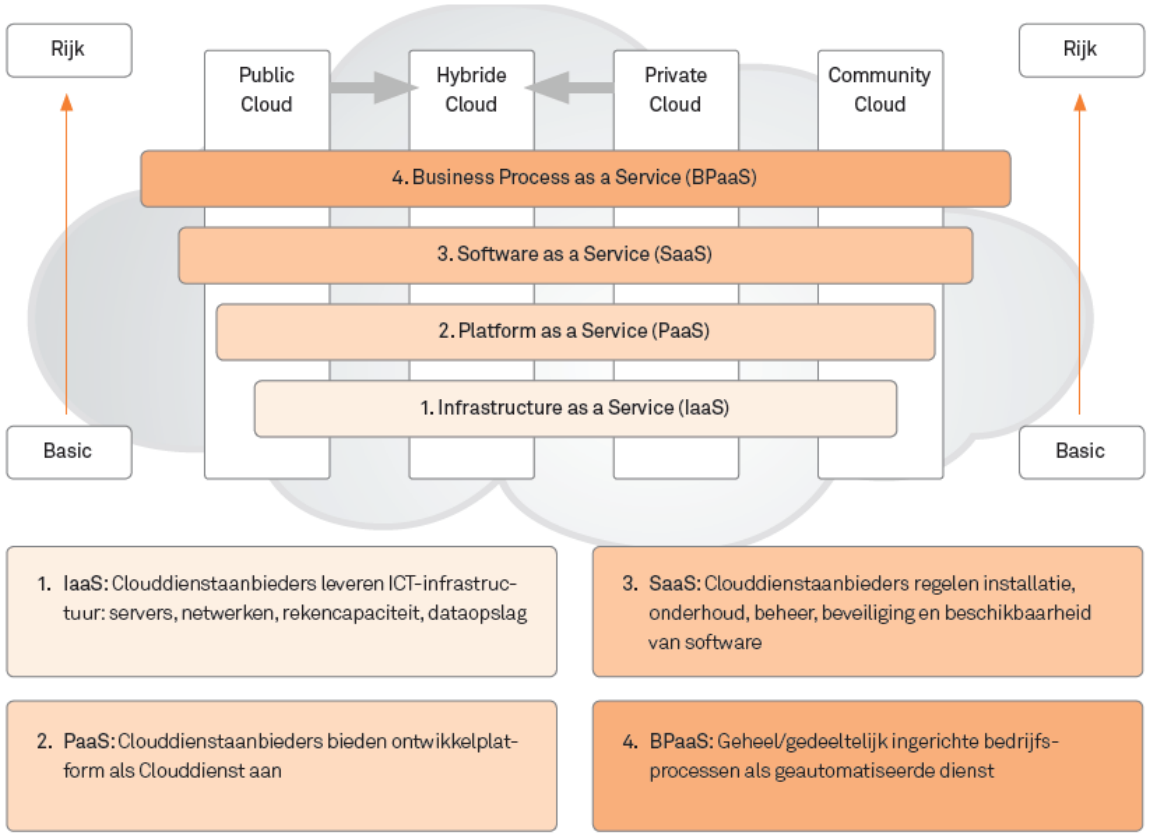
De Autoriteit Persoonsgegevens biedt via haar website praktische adviezen over interpretatie en invulling van de huidige en de nieuwe privacywetgeving (AVG) [**AP-5**].

MELDPLICHT DATALEKKEN

Naar aanleiding van de invoering van de meldplicht datalekken op 1 januari 2017, heeft de AP praktische informatie gepubliceerd hoe in de praktijk om te gaan met meldplicht datalekken [**AP-1**] en geeft zij periodiek inzicht in het aantal en soort gemelde datalekken [**AP-4**]. In mei 2017 heeft NOREA de handreiking “Werkprogramma ‘Meldplicht Datalekken’, Versie 1.0 – Mei 2017” gepubliceerd [**NOREA-5**].

H-15: DIENSTEN VAN DERDE PARTIJEN / CLOUDCOMPUTING

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



Afbeelding 21: Bron NBA-publicatie over Cloud computing

De ‘klassieke’ uitbesteding van de verwerking en opslag van gegevens kwalificeert in dit model als een IaaS 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.

Veel MKB-accountantskantoren maken gebruik van SaaS toepassingen, in de vorm van een Public Cloud. In dat geval is de cloudaanbieder verantwoordelijk voor het functioneel en technisch beheer, 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.

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 taak-/verantwoordelijkheidsverdeling. Dit om vast te kunnen stellen welke beveiligingsmaatregelen zijn organisatie moet treffen, en welke maatregelen hij mag verwachten bij de derde partij.

Onderstaand is een overzicht van de verschillende dienstconcepten en toepassingsmodellen, alsmede de daarbij behorende risico’s en interne beheersingsmaatregelen opgenomen [**NBA-12**].

DIENSTCONCEPTEN (OOK WEL 'SERVICES' GENOEMD)

INFRASTRUCTURE AS A SERVICE (IAAS)

IaaS is de meest kale, basic vorm van cloudcomputing. De clouddienstaanbieder biedt ICT infrastructuurcomponenten aan in de vorm van servers, netwerken, rekencapaciteit en dataopslag. De afnemer van deze clouddienst:

- is volledig vrij om eigen systemen en diensten te ontwikkelen en kan ook zelf zijn besturingssysteem kiezen;
- kan de systemen voor zijn eigen organisatie gebruiken of deze ter beschikking stellen aan derden in de vorm van een clouddienst;
- is zelf verantwoordelijk voor de functionaliteit, de verwerking en de opslag van data.

De clouddienstaanbieder is dus alleen verantwoordelijk voor de onderliggende infrastructuur, zoals servers en systemen voor dataopslag. Afhankelijk van de gemaakte afspraken tussen de clouddienstaanbieder en de afnemer is één van beiden verantwoordelijk voor de toegang, back-up en recovery van de opgeslagen data. De clouddienstaanbieder biedt vaak een basisvoorziening aan, maar de afnemer zal zelf moeten bepalen of deze voor hem toereikend is. Voorbeelden van (internationale) aanbieders: Microsoft (Azure), Rackspace en Amazon. Enkele lokale spelers bieden dergelijke services ook aan.

PLATFORM AS A SERVICE (PAAS)

Er zijn ook aanbieders van clouddiensten die een ontwikkelplatform aanbieden met een verzameling standaarddiensten (besturings- en datamanagementsysteem, ontwikkeltools). Op basis daarvan kan de gebruiker snel eigen toepassingen ontwikkelen. De afnemer is zelf verantwoordelijk voor de uiteindelijke applicatie. Het onderliggende platform (services, verwerkings- en opslagcapaciteit) is de verantwoordelijkheid van de aanbieder van de clouddienst. Voorbeelden van aanbieders van PaaS: Microsoft, Amazon, Google, Open Text Cordys, Mendix en WordPress.

SOFTWARE AS A SERVICE (SAAS)

Als de aanbieder van een clouddienst zorgt voor installatie, onderhoud en beheer, beveiliging en beschikbaarheid van de software, gaat het om Software as a Service (SaaS). De SaaS-aanbieder is daarbij verantwoordelijk voor de toepassingsmogelijkheden en alle onderliggende hard- en software. De afnemer gebruikt de standaardfunctionaliteit die de aanbieder van de SaaS-dienst hem aanbiedt en kan daar doorgaans niets aan wijzigen. Soms biedt de aanbieder de gebruiker de mogelijkheid om de aangeboden standaardfunctionaliteit - binnen de mogelijkheden van de dienst - naar eigen wens vorm te geven en te koppelen met toepassingen die in de eigen omgeving van de gebruiker draaien. Bekende voorbeelden van SaaS-toepassingen: Microsoft Office 365, de online boekhoudpakketten van Exact, Reeleezee, Twinfield, UNIT4, PM Software, Cash, Davilex, Muis, Yob, AccountView, maar ook LinkedIn, Facebook, Gmail van Google en Hotmail van Microsoft. Andere bekende voorbeelden zijn de opslagdiensten Dropbox, Google Drive, Microsoft OneDrive of Apple iCloud, waarmee de gebruiker data kan opslaan in de vorm van tekst, foto's, films, muziek, etc. Deze toepassingen zijn vaak te gebruiken via apps.

BUSINESS PROCESS AS A SERVICE (BPAAS)

Bij Business Process as a Service worden geheel of gedeeltelijk ingerichte bedrijfsprocessen aangeboden als een geautomatiseerde dienst. BPaaS is een recente ontwikkeling, waarbij de processen door de diensten van meerdere clouddienstaanbieders worden vormgegeven. Voorbeelden van BPaaS zijn: salaris- en factuurverwerkingsprocessen (inclusief betaalbaarstelling en betaling), human resources management, maar ook ons elektro-

nisch betaalsysteem, vormgegeven door de betaalfunctie in boekhoudsoftware gecombineerd met het elektronische betaalsysteem van de banken. Een ander bekend voorbeeld is iDEAL, waarmee klanten van een webwinkel in hun aankoopproces via hun eigen bank(rekening) de betaling van een product afhandelen. Bij een BPaaS-dienst zijn dus meerdere partijen verantwoordelijk voor de functionaliteit, het beheer, het onderhoud, de beveiliging en de continuïteit van de keten. Wanneer een van de schakels in de keten niet naar behoren functioneert, levert dit een risico op voor de gehele keten. Concreet voorbeeld daarvan is een grote storing bij iDEAL, waardoor webwinkels de betalingen van hun klanten niet konden verwerken. Dit werkte onmiddellijk negatief door in hun omzetten.

TOEPASSINGSMODELLEN CLOUDCOMPUTING

PUBLIC CLOUD

De Public Cloud is de meest vergaande vorm van cloudcomputing. Public clouddiensten zijn voor iedereen toegankelijk en worden vaak aangeboden door grote internationaal opererende bedrijven. Maar ook kleine nationaal opererende bedrijven kunnen dergelijke diensten aanbieden. Voor de afnemer is de aangeboden infrastructuur onzichtbaar. Deze bevindt zich - ergens ter wereld - op een locatie van de aanbieder of een onderaannemer en wordt ook gedeeld met andere gebruikers. De gebruiker heeft feitelijk geen invloed op de functionaliteit of de kwaliteit van de aangeboden dienst. Voorbeelden van aanbieders: Microsoft (IaaS, PaaS, SaaS), Google (IaaS, SaaS), Apple (SaaS), Open Text Cordys (PaaS), Amazon (IaaS), Salesforce voor CRM (PaaS, SaaS), WordPress voor de ontwikkeling en het onderhoud van websites (PaaS), maar ook Rackspace (IaaS).

PRIVATE CLOUD

Bij een Private Cloud werkt de gebruiker op een infrastructuur en met toepassingen die specifiek zijn ingericht voor zíjn organisatie. De functionaliteit en infrastructuur worden niet gedeeld met andere organisaties. Bij dit toepassingsmodel heeft de gebruiker meer zeggenschap en controle over de data, de beveiliging en de kwaliteit van de dienst. Het onderhoud van de Private Cloud ligt - afhankelijk van het gekozen dienstconcept - bij de aanbieder en/of de gebruiker.

HYBRIDE CLOUD

Voor sommige clouddiensten wordt gekozen voor de combinatie van de Public Cloud met een Private Cloud. Zo kunnen bijvoorbeeld toepassingen binnen de Public Cloud een Private Cloud ondersteunen wanneer er sprake is van een piekbelasting.

COMMUNITY CLOUD

Binnen een Community Cloud worden clouddiensten aangeboden voor een groep organisaties met een gemeenschappelijk belang. De Community Cloud is aangepast aan de specifieke eisen die de deelnemende organisaties aan de clouddienst stellen, zoals datalocatie, beveiliging en architectuurkeuzes. De hardware staat bij één of meer van de deelnemende organisaties of een derde partij, wat het risico van inbreuk op de beschikbare data beperkt. Voorbeelden van organisaties met een gemeenschappelijk belang die in een Community Cloud werken, zijn onderwijsorganisaties, overheidsinstellingen en zorginstellingen. Een clouddienst (bijvoorbeeld een administratieve toepassing) die zich richt op een specifieke groep gebruikers in een bepaald gebied is ook te beschouwen als dienstconcept binnen een Community Cloud. Voorbeelden in die context, van op Nederland gerichte clouddiensten op het terrein van de financiële administratie, zijn: Twinfield, Reeleezee, UNIT4, Exact Online en Pro Management.

VOORBEELDEN VAN BEVEILIGINGSRISICO'S GERELATEERD AAN CLOUDCOMPUTING

- Ontoereikende logische en fysieke beveiliging van data en processen bij de clouddienstaanbieder (verder: CDA);
- Onvoldoende back-up en recovery voor herstel van services bij storingen bij de CDA, inclusief disaster recovery en uitwijk;
- Ontoereikende beveiliging van dataverkeer over het internet;
- Ontoereikend intern beheer en interne beheersing bij CDA (bijvoorbeeld bij toepassen virtualisatie en multi-tenancy);
- Ontoereikend changemanagement van applicaties en infrastructuur bij de CDA;
- Ontoereikend incidentenbeheer CDA;
- Ontbreken van voldoende toepassingsgerichte interne beheersingsmaatregelen (Application controls) op invoer, verwerking, uitvoer en opslag);
- Onvoldoende mogelijkheid om via een audit-trail de goede werking van processen en opslag, inclusief incidentmanagement, vast te stellen;
- Faillissement of overname van de CDA door een andere partij;
- Onduidelijkheid over juridisch eigenaarschap data;
- Onduidelijkheid over fysieke locatie/omstandigheden waaronder data worden opgeslagen en bewaard;
- Onvoldoende duidelijkheid over wet- en regelgeving waaronder de clouddienst wordt aangeboden en de CDA functioneert;
- Onduidelijkheid over de aansprakelijkheid voor beschikbaarheid dienstverlening, performance, etc.;
- Onduidelijkheid over de mogelijkheid om te kunnen voldoen aan wet- en regelgeving, waaronder privacyregelgeving, maar ook fiscale regelgeving;
- Vendor lock-in; de gebruiker kan in technische zin zijn data en/of programma's/processen niet overbrengen naar een andere CDA. Dit in verband met het recht van de betrokkene op dataportabiliteit [**art. 20, AVG**].

H-16:THIRD PARTY REPORTS

ASSURANCE-RAPPORTEN

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 van dienstverlening of dat periodiek een assurance-rapport kan worden overlegd. Een assurance-rapport kan ook als een vorm van verantwoording in het contract met een derde partij worden opgenomen. Wat betreft assurance-rapporten zijn er twee mogelijkheden:

- Een assurance-rapport gebaseerd op Standaard 3000. Deze rapportage is vaak bedoeld voor een ruimere doelgroep. De rapportage richt zich niet alleen op zaken die van belang zijn voor de controle van de financiële verantwoording, maar er wordt ook gekeken of de dienstverlening en de interne beheersingsmaatregelen van de clouddienstaanbieder voldoen aan een algemeen aanvaard kwaliteitsniveau.
- Een assurance-rapport gebaseerd op de International Standard on Assurance Engagements (ISAE) 3402 (Standaard 3402) of de Amerikaanse variant SSAE 16. Dit rapport is primair bedoeld voor de controlerend accountant van de gebruiker van de dienstverlening van de clouddienstaanbieder. De rapportage kent twee varianten: een rapportage gericht op de opzet van de interne beheersingsmaatregelen van de clouddienstaanbieder op een bepaald moment (type 1) en een rapportage die naast de opzet ook het bestaan en de werking van de beheersingsmaatregelen gedurende een bepaalde periode omvat (type 2).

ISO-CERTIFICERING

Ook is het mogelijk dat een organisatie beschikt over een ISO 27001- of ISO 27002-certificering. De standaarden ISO 27001 en 27002 hebben beide betrekking op de invulling van informatiebeveiliging. Zij zijn de opvolgers van ISO 17799 (voorheen de Code voor Informatiebeveiliging). ISO 27001 is normatief van opzet en bevat harde eisen waaraan de organisatie moet voldoen om gecertificeerd te worden. Deze eisen worden beschreven op het niveau van maatregelen die de organisatie moet treffen. ISO 27002 is niet-normatief van opzet en bevat ‘best practices’ voor de implementatie van informatiebeveiliging. Beide standaarden richten zich primair op de beheersing van informatiebeveiliging. Dit kan weliswaar raakvlakken hebben met de beheersing van de integriteit van de data en het waarborgen van de vertrouwelijkheid, maar dat is niet de primaire focus. Om die reden leveren certificaten die gebaseerd zijn op ISO 27001 of ISO 27002 onvoldoende controlebewijs voor een accountant. Een accountant die wil weten in welke mate bepaalde risico’s zijn afgedekt, dient de ‘verklaring van toepasselijkheid’ (‘statement of applicability’) in te zien.

KEURMERK ZEKER-ONLINE[4]

Medio 2013 is het keurmerk ‘Zeker-Online’ actief geworden. Dit is een onafhankelijk en transparant keurmerk voor online administratieve diensten, ofwel clouddiensten. Het keurmerk staat daarmee voor betrouwbaarheid, veiligheid en continuïteit, kwaliteit in functionaliteit en juridische zekerheid van de cloud. De Belastingdienst, het Electronic Commerce Platform Nederland (ECP) en aanbieders van clouddiensten hebben samen bijgedragen aan de ontwikkeling van ‘Zeker-Online’. Hun missie is daarbij: een kwaliteitsgarantie kunnen bieden aan gebruikers van clouddiensten. De kwaliteitseisen voor het keurmerk zijn gedefinieerd en vastgelegd in het ‘Normenkader Zeker-Online’. Hierbij werkten de hiervoor genoemde partijen nauw met elkaar samen, daarbij ondersteund door een groep auditors. Binnen het normenkader is met een kwaliteitsbril gekeken naar

[4] https://www.zeker-online.nl/

de technische infrastructuur, de administratieve structuur en verwerkingswijze (generieke en specifieke maatregelen in de applicatie), en naar de juridische infrastructuur. De Stichting Zeker-Online verleent het (nieuwe) keurmerk, dat zichtbaar maakt welke clouddienstaanbieders diensten leveren die voldoen aan belangrijke online securityvereisten. Daarin hebben de beveiligingsrichtlijnen van het National Cyber Security Center een belangrijke rol gespeeld. Wil een clouddienstaanbieder in aanmerking komen voor het keurmerk? In dat geval zal hij, en zijn eventuele onderaannemers, moeten voldoen aan hoge kwaliteitseisen die een betrouwbare, continue verwerking van transacties waarborgen. Dat geldt niet alleen voor de applicatie die de administratieve gegevens verwerkt en waaruit financiële informatie voortkomt. Voor het totaalpakket van de dienstverlening door de aanbieder die het keurmerk voor zijn oplossing heeft verworven, geldt dit óók. Is het keurmerk toegekend, dan mag de klant erop vertrouwen dat de dienstverlening voldoet aan de relevante wet- en regelgeving, waaronder privacywetgeving.

OVERZICHT VAN RELEVANTE VERSCHILLEN TUSSEN THIRD PARTY RAPPORTEN

Standaard	Toepassing	Inhoud	Inhoud v/h rapport
Standaard 3402	Communicatiemiddel tussen accountants in het kader van de controle van de jaarrekening over de interne beheersing bij een serviceorganisatie aan wie de controlecliënt diensten heeft uitbesteed.	Het rapport geeft aan in hoeverre het door de serviceorganisatie gedefinieerd stelsel van interne beheersmaatregelen in opzet/bestaan op enig moment in de tijd aanwezig is en functioneert over een aangegeven periode (werking). Het is aan de accountant van de uitbestedende organisatie om na te gaan welk stelsel van interne beheersing in het onderzoek is betrokken (scope) en of het niveau van interne beheersing van het beoordeelde stelsel van maatregelen procedures voor hem van voldoende niveau is om daarop in zijn controle te kunnen steunen. In dat kader zal hij moeten vaststellen: • Alle voor zijn controle van belang zijnde maatregelen in de beoordeling van het stelsel zijn meegenomen; • De uitgevoerde controlewerkzaamheden voldoende bewijs hebben om de conclusie (oordeel van de onafhankelijke auditor) te onderbouwen. Van belang voor de controlerende accountant van de gebruiker van de dienstverlening van de serviceorganisatie.	Twee typen rapportages zijn mogelijk: • Type I rapport heeft betrekking op de opzet/het bestaan op enig moment in de tijd; • Type 2 rapport heeft naast opzet/bestaan ook betrekking op het functioneren gedurende aangegeven periode.
Standaard 3000	Assurance-rapport ten behoeve van een ruime doelgroep.	Certificaat geeft aan in hoeverre een organisatie voldoet aan de in de standaard aangegeven eisen. Het rapport biedt de serviceorganisatie de mogelijkheid om publiekelijk aan te geven dat de door de serviceorganisatie te definiëren dienstverlening, inclusief interne beheersing, aan algemeen aanvaarde kwaliteitsnormen voldoet.	Twee typen rapportages zijn mogelijk: • Een assurance-rapport dat betrekking heeft op de opzet/het bestaan op enig moment in de tijd; • Een assurance-rapport dat ook betrekking heeft op het functioneren van

Standaard	Toepassing	Inhoud	Inhoud v/h rapport
		Ook hier is het aan de lezer na te gaan of het beoordeelde stelsel en de gehanteerde normen voor hem van voldoende niveau zijn en of alle voor hem van belang zijnde maatregelen in de beoordeling van het stelsel zijn meegenomen. Van belang voor gebruikers van de dienstverlening van de beoordeelde serviceorganisatie.	het beoordeelde stelsel gedurende de aangegeven periode.
ISO 27001/2	Basis voor het afgeven van een certificaat. Richt zich met name op informatiebeveiliging.	Het certificaat heeft aan in hoeverre de beoordeelde organisatie voldoet aan de in de standaard aangegeven eisen. Hierbij moet worden aangetekend dat de in de standaard opgenomen eisen ruimte laten voor interpretatie door de uitvoerend auditor en zijn deze afhankelijk van de beleidsdoelstellingen van de organisatie.	Certificaat waarin is aangeven in hoeverre een organisatie voldoet aan de in de standaard opgenomen eisen.
SOC 1 Amerikaanse regelgeving	Richt zich op de interne beheersingsmaatregelen van belang in het kader van controle van de jaarrekening.	Problematiek vergelijkbaar met Standaard 3402. Van belang voor de controlerende accountant van de gebruiker van de dienstverlening van de serviceorganisatie.	Problematiek vergelijkbaar met Standaard 3402.
SOC 2 Amerikaanse regelgeving	Assurance-rapport ten behoeve van een ruime doelgroep.	Problematiek vergelijkbaar met Standaard 3000. Als normenkader voor de beoordeling wordt vaak gebruik gemaakt van de 'Trust Services Principles' die zich richten op Beveiliging (inclusief betrouwbaarheid), Beschikbaarheid (inclusief continuïteit), Verwerkingsintegriteit, Vertrouwelijkheid en Privacy. Van belang voor gebruikers van de dienstverlening van de beoordeelde serviceorganisatie.	Problematiek vergelijkbaar met Standaard 3000.

Standaard	Toepassing	Inhoud	Inhoud v/h rapport
SOC 3 Amerikaanse regelgeving	Assurance-rapport ten behoeve van publiekelijk gebruik, veelal in de vorm van een extern gericht keurmerk.	Problematiek vergelijkbaar met Standaard 3000. Als normenkader voor de beoordeling wordt vaak gebruik gemaakt van de 'Trust Services Principles' die zich richten op Beveiliging (inclusief betrouwbaarheid), Beschikbaarheid (inclusief continuïteit), Verwerkingsintegriteit, Vertrouwelijkheid en Privacy. Van belang voor gebruikers van de dienstverlening van de beoordeelde serviceorganisatie.	Publiekelijk gericht keurmerk dat verwijst naar achterliggend assurance-rapport.
Zeker-OnLine	Keurmerk inzake de kwaliteit van IT-dienstverlening	Beoordeling is gebaseerd op een uitgebreid normenstelsel. Van belang voor gebruikers van de dienstverlening van cloudaanbieders.	Publiekelijk gericht keurmerk dat verwijst naar achterliggend assurance-rapport (3402).

H-17: RECENT ONDERZOEK NAAR CYBERCRIME EN NON-COMPLIANCE

Recent onderzoek naar cybercrime en privacy (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. Afgelopen periode zijn de volgende onderzoeken in het kader van dit rapport van belang.

ONDERZOEK NAAR CYBERCRIME

NBA: Bij de aankondiging van de Accountantsdag 2017 is bij het thema Cybersecurity een overzicht van 7 Crazy facts opgenomen [**NBA-14**]. De belangwekkendste zijn:

- De jaarlijkse schadepost voor de NL samenleving wordt geschat op 9 miljard euro. Nederland wordt hiermee relatief hard getroffen, in de EU ligt de gemiddelde schade op 0,41% van het BBP (Bron: ABN AMRO).
- Het duurt gemiddeld 252 dagen voordat een hack wordt ontdekt. Controle of je daadwerkelijk bent gehackt neemt in 82 % van de gevallen slechts 1 minuut in beslag. Maar slechts 6 % van de hacks wordt ontdekt door de IT-afdeling (Bron: Emerce).
- De wereldwijde markt voor cyber security was in 2016 ongeveer 75 miljard dollar. Naar verwachting groeit deze markt door tot 170 miljard dollar in het jaar 2020 (Bron: FD).
- De schattingen van de opbrengst voor de criminelen lopen enorm uiteen. De laagste schatting is een opbrengst van 300 miljard terwijl de hoogste van het dubbele uitgaat (Bron: FD).
- 55 % van de mensen gebruikt maar 1 wachtwoord voor alle plekken waar zij moeten inloggen. Het meest voorkomende wachtwoord is 123456 (Bron: NRC / Deloitte).

NCSC 2017: het Cybersecuritybeeld Nederland (CSBN) 2017 van Nationaal Cyber Security Centrum (NCSC) [**NCSC-3**] biedt inzicht in de belangen, dreigingen en weerbaarheid en daarmee samenhangende ontwikkelingen op het gebied van cybersecurity. CSBN 2017 richt zich primair op Nederland, over de periode mei 2016 tot en met april 2017. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid gepubliceerd en komt tot stand in samenwerking met publieke en private partners. De kernbevindingen zijn:

- Beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan;
- Digitale aanvallen worden gebruikt om democratische processen te beïnvloeden;
- De kwetsbaarheid van het Internet of Things (IoT) heeft tot verstorende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven;
- Veel organisaties zijn afhankelijk van een beperkt aantal buitenlandse aanbieders van digitale infrastructuurdiensten waardoor de maatschappelijke impact bij verstoring groot is;
- Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging.

De belangrijkste dreigingen zijn:

- Het Internet of Things (IoT) is het afgelopen jaar ingezet voor cyberaanvallen. Onvoldoend beveiligde IoT-apparatuur levert een belangrijke bijdrage aan de stijging van de omvang van DDoS-aanvallen. Distributed Denial of Service-aanvallen (DDoS- of 'cyberaanvallen'), is het platleggen van een server door het sturen van een grote hoeveelheid data, waardoor organisaties, zoals een webwinkel niet meet bereikbaar zijn.
- Het gebruik van ransomeware (gijzelsoftware) waarmee organisaties worden gechanteerd door data te versleutelen en deze pas na betaling vrij te geven. Door de aanvallen in mei en juni 2017 werden

wereldwijd meer dan 200.000 computers. Bij o. m. zestien Britse medische instellingen, de Spaanse telecomaanbieder Telefónica, de containerterminals van havenbedrijf APM, de parkeergarages van Q-Park en pakjesbezorger TNT Express werd de bedrijfsvoering verstoord of zelfs soms volledig stilgelegd.

- E-mail wordt nog steeds gezien als het meest gebruikte medium om ransomware te verspreiden, naast phishing-emails, gebruikers naar een valse (bank)website worden gelokt, om ze daar - nietsvermoedend - te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer.

Het Rathenau Instituut constateert in haar rapport: "Een nooit gelopen race, Over cyberdreigingen en versterking van weerbaarheid (2017), op pagina 23 het volgende over het MKB [**RATHENAU-1**]:

"Voor het midden- en kleinbedrijf (MKB) geldt een vergelijkbaar verhaal als voor de burger. Vooral kleinere bedrijven hebben over het algemeen maar een beperkt inzicht in de risico's die ze lopen. Ze hebben daarnaast onvoldoende middelen, kennis of toegang tot kennis om passende maatregelen te nemen (Verhagen 2016). Weliswaar worden door ICT-leveranciers allerlei beveiligingsproducten en -diensten aangeboden, maar mkb-bedrijven zijn vaak onvoldoende in staat geboden oplossingen op waarde te schatten en te beoordelen of die producten en –diensten voor hun situatie een goede oplossing bieden. Het CBP spreekt in dit verband van een kennisasymmetrie tussen ICT-leveranciers en -gebruikers. En omdat bedrijven niet weten wat ze aan beveiligingsmaatregelen moeten vragen, wordt de prijs vaak doorslaggevend (CPB 2016).

Binnen het MKB is de basisbeveiliging vaak niet op orde. Er worden geen sterke wachtwoorden gebruikt, beveiligingssoftware wordt onregelmatig geüpdatet, en er worden onvoldoende back-ups van belangrijke bestanden gemaakt. Het kan overigens ook voorkomen dat bedrijven zich laten verleiden tot de aanschaf van een in hun ogen innovatieve ICT-oplossing, zonder dat zij beschikken over de kennis om de software naar behoren te gebruiken of voldoende hebben nagedacht over de eigenlijke dreigingen waaraan ze blootstaan. Dat kan leiden tot schijnzekerheid.

Bovendien brengt technologie alleen vaak niet de oplossing. De werknemer achter de laptop, pc of tablet is vaak de zwakste schakel. Mensen laten zich door spear phishing e-mails gemakkelijk verleiden tot het aanklikken van geïnfecteerde weblinks. Een probleem dat hierbij meespeelt, is dat op ICT-gebied werk en privé vaak door elkaar lopen. Malware op de privé-computer of tablet kan ook de werkomgeving besmetten.

Binnen het MKB bestaat grote behoefte aan onafhankelijke advisering en ondersteuning ten aanzien van te nemen beveiligingsmaatregelen, die ook passend moeten zijn. Omdat het MKB bestaat uit een grote en zeer diverse groep bedrijven, variërend van zelfstandigen zonder personeel tot bedrijven met 250 werknemers, hangen de benodigde maatregelen af van het type bedrijf en de specifieke sector waarbinnen dat bedrijf werkzaam is. Ongeveer 97 procent van het bedrijfsleven maakt deel uit van het MKB. Daarmee vormt het gebrek aan weerbaarheid een serieus probleem."

ONDERZOEK NAAR PRIVACYBESCHERMING / DATALEKKEN

PWC heeft in het kader van het periodiek Privacy Governance onderzoek in mei 2017 een enquête uitgevoerd onder 327 organisaties. De belangrijkste conclusies zijn [**PWC-1**]:

- Verwerking persoonsgegevens: Driekwart (74%) heeft verwerkingen van persoonsgegevens nog niet inzichtelijk en gedocumenteerd, terwijl dit wel een verplichting is. Slechts 19% van de organisaties heeft dit inmiddels wel gedaan.
- **Right to be forgotten**: 69% heeft geen enkele procedure geïmplementeerd voor de afhandeling van inzage- en correctieverzoeken van betrokkenen.
- **Meldplicht datalekken**: slechts 49% heeft een draaiboek klaarliggen in geval van een datalek
- **Data Protection Officer (FG)**: 17% heeft de verantwoordelijkheid voor privacy neergelegd bij een privacy officer. 21% heeft daarentegen niemand aangewezen die de rol van Data Protection Officer gaat vervullen.
- **Bewerkersovereenkomst**: 13% sluit geen bewerkersovereenkomst af met derde partijen waarmee persoonsgegevens worden gedeeld. Belangrijkste reden is de onbekendheid hiervan.
- **Privacy Impact Assessment (PIA)**: De helft (50%) voert geen Privacy Impact Assessment uit bij organisatiewijzigingen die grote impact hebben op de verwerking van persoonsgegevens.

- **Bewaartermijnen**: Een derde heeft geen bewaartermijnen geïmplementeerd.
- **Menskracht**: het grootste struikelblok voor tijdige implementatie is gebrek aan mankracht (39 procent), gevolgd door onvoldoende kennis (34%).
- **Deadline**: Slechts 12% zegt nu klaar te zijn voor de nieuwe EU-vordering. De helft (52%) verwacht voor de deadline van 25 mei 2018 klaar te zijn met voorbereidingen.

MKB-Service desk heeft in juni 2017 een digitale poll gehouden op de site van MKB Servicedesk. Hieraan is meegewerkt door 3.192 ondernemers met tussen de 1 en 250 werknemers, actief in negen branches [**MKB-1**]. Uit het onderzoek blijkt dat slechts 25% van het MKB al maatregelen heeft genomen of dat van plan is. Bedrijven binnen de zakelijke dienstverlening en de handel blijken het slechtst op de hoogte van de nieuwe wet. Van het kleinbedrijf tot zes medewerkers wist zelfs driekwart van de respondenten van niets.

Uit een onderzoek van **Kaperskylab Pb7** [KAPERSKY-1] onder 310 bedrijven met 30 of meer medewerkers komt naar voren dat meer dan de helft van alle ondervraagde organisaties zegt in 2016 met één of meer lekken van gevoelige informatie te maken hebben gehad. De meest voorkomende gevallen van dataverlies hebben weinig met cybercriminaliteit te maken. Meer dan 30% van de organisaties heeft te maken gehad met het verlies van gevoelige data door het verdwijnen van computerapparatuur, zoals laptops of smartphones. Nog eens 23% geeft aan dat informatiedragers als USB-sticks met gevoelige informatie zijn kwijtgeraakt. En als medewerkers deze niet zelf verliezen, heeft 22% ook nog eens te maken gehad met diefstal van apparatuur en informatiedragers. Uiteindelijk heeft ook nog zo'n 13% data verloren door verschillende vormen van cybercrime.

De **Autoriteit Persoonsgegevens (AP**) registreert vanaf de start (1 januari 2016) van de meldplicht datalekken het aantal meldingen en geeft periodiek inzicht in het aantal en soort gemelde datalekken [**AP-4**].

Overzicht van ontvangen meldingen

Meldingen	1e kwartaal 2016	2e kwartaal 2016	3e kwartaal 2016	4e kwartaal 2016	1e kwartaal 2017	2e kwartaal 2017	3e kwartaal 2017
Nieuwe	**1.061**	**1.396**	**1.491**	**1.901**	**2.388**	**2.468**	**2.580**
Aanvullingen	150	220	267	333	382	396	368
Intrekkingen	36	43	76	77	71	71	72

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%

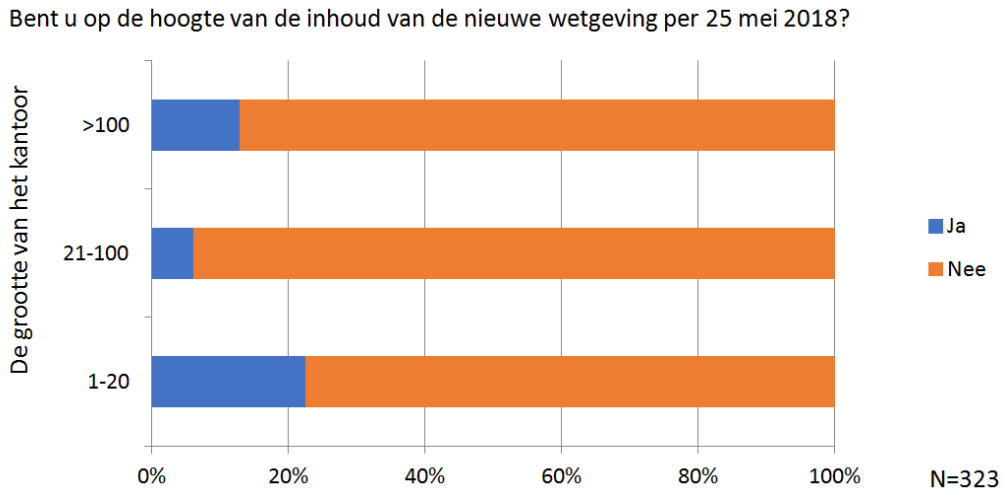
Belangrijkste gegevens

Naam- en adresgegevens, geboortedatum, telefoon, BSN, financiële en gezondheidsgegevens.

De AP startte in het 2e kwartaal 2017 123 onderzoeken naar beveiliging en datalekken. Onder meer naar aanleiding van meldingen van datalekken. De AP startte ook onderzoeken naar mogelijke datalekken bij organisaties die dit níet hebben gemeld bij de AP. De AP gaf het merendeel van de onderzochte organisaties een waarschuwing. Over het algemeen leidde dat tot beëindiging van de overtreding. Bijvoorbeeld doordat organisaties een beveiligingslek zelf hebben gemeld aan de betrokkenen. Of hun beveiligingsmaatregelen hebben aangescherpt.

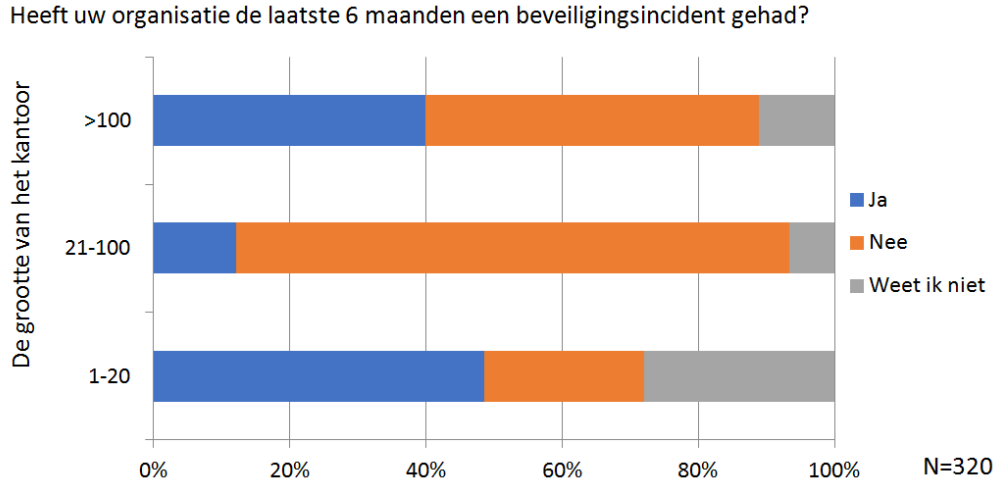
NEMACC heeft zelf tijdens het symposium op 8 juni 2017 een korte enquête gehouden onder de deelnemers (ruim 550 deelnemers, waarvan er ruim 300 deelnamen aan de enquête.

Op de vraag: **Bent u op de hoogte van de inhoud van de wetgeving per 25 mei 2018**? antwoordde slechts **41 (12,7%)** van de **323** deelnemers aan de enquête met **JA**.



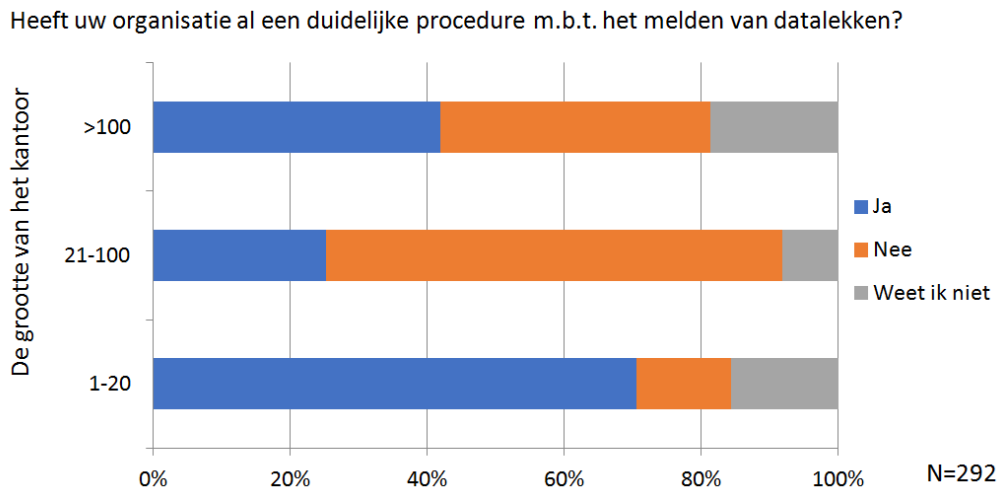
Afbeelding 22: Bron NEMACC

Op de vraag: **Heeft uw organisatie de laatste 6 maanden een beveiligingsincident gehad**? antwoordde **92 (28,8%)** van de **320** deelnemers aan de enquête met **JA**.



Afbeelding 23: Bron NEMACC

Op de vraag: **Heeft uw organisatie al een duidelijke procedure m.b.t. het melden van datalekken**? antwoordde **127 (43,5%**) van de **292** deelnemers aan de enquête met **JA**.



Afbeelding 24: Bron NEMACC

H-18:GERAADPLEEGDE / BESCHIKBARE KENNISBRONNEN

[**AICPA-1**] AICPA, SOC for Cybersecurity, 2017
https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

[**AP-1**] De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) Beleidsregels voor toepassing van artikel 34a van de Wbp, 8 december 2015.
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

[**AP-2**] In 10 stappen voorbereid op de AVG, publicatie van de AP.
https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

[**AP-3**] Algemeen.
https://autoriteitpersoonsgegevens.nl/nl

[**AP-4**] Datalekken.
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-meldingen-datalekken

[**AP-5**] Actualiteit.
https://autoriteitpersoonsgegevens.nl/nl/actueel?f[0]=cbp_sections%3A3269

[**BFT-1**] Specifieke leidraad naleving WWFT voor accountants, belastingadviseurs, administratiekantoren en alle overige instellingen genoemd in artikel 1 lid 1 letter a sub 11, 12 en 13 en 23 WWFT, BFT.
https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/specifieke_leidraad_naleving_wwft_voor_accountants_en_belastingadviseurs__0.pdf

[**CBP-1**] CBP Richtsnoeren: IDENTIFICATIE EN VERIFICATIE VAN PERSOONSGEGEVENS Gebruik van 'kopietje' paspoort in de private sector, CBP, juli 2012.
https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_kopie-identiteitsbewijs.pdf

[**CBP-2**] CBP Richtsnoeren: BEVEILIGINGVAN PERSOONSGEGEVENS, CPB, februari 2013.
https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

[**CBP-3**] Raamwerk Privacy Audit, CBP, 19 december 2000.
https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/raamwerk_privacyaudit.pdf

[**CBP-4**] CONTOUREN voor COMPLIANCE, Handreiking bij het Raamwerk Privacy Audit, CBP, 24 mei 2005.
https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/handreiking_rpa.pdf

[**CBP-5**] WBP.
https://www.eerstekamer.nl/behandeling/20000706/publicatie_wet_2/document3/f=/w25892st.pdf

[**CBP-6**] Instemming met richtlijn door Cbp.
https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/brf_cbp.pdf

[**CBP-7**] Handreiking bij het Raamwerk Privacy Audit.
https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/handreiking_rpa.pdf

[**CBS-1**] Cybersecuritymonitor 2017, Een eerste verkenning van dreigingen, incidenten en maatregelen
https://www.cbs.nl/-/media/_pdf/2017/06/csm2017_web.pdf

[**CE-1**] Cyber Edge, 2016 Cyberthreat Defense Report
https://cyber-edge.com/wp-content/uploads/2016/08/CyberEdge-2015-CDR-Report1-1.

[**CMS-1**] Introductie tot de Algemene verordening gegevensbescherming (Verordening (EU) 2016/679), CMS, 2016
https://cms.law/nl/content/download/196061/5510277/version/1/file/2016_07_Introductie_tot_de_Algemene_verordening_gegevensbescherming.pdf

[**Del-1**] Deloitte, Cyber Value at Risk in the Netherland, 2016
https://www.accountant.nl/nieuws/2016/4/deloitte-cybercrime-kost-nederlandse-organisaties-10-miljard-euro-per-jaar/

[**DNB-1**] Toetsingskader Informatiebeveiliging.
http://www.toezicht.dnb.nl/3/50-203304.jsp

[**ENISA-1**] https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

(**EU-1**] VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), Publicatieblad van de Europese Unie, 4.5.2016.
http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL

[**EU-2**] Opinion 1/2010 on the concept of "controller" and "processor" (00264/10EN WP 169). Article 29 Data Protection Working Party.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[**KAPERSKY-1**] Kaperskylab Pb7.
http://newsroom.kaspersky.eu/fileadmin/user_upload/nl/Downloads/meldplichtdatalekken.pdf

[**KPMG-1**] "Informatiebeveiliging onder controle", Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit. 2000, ISBN 90-430-0289-5

[**KZ-1**] Keurmerk Zeker-Online.
https://www.zeker-online.nl/

[**MINFIN-1**] Handleiding voor advocaten, notarissen, accountants, belastingadviseurs en administratiekantoren, Wet ter voorkoming van witwassen en financiering van terrorisme (WWFT), Ministerie van Financiën.
https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/brochures/2009/02/17/handleiding-advocaten-notarissen-accountants-belastingadviseurs-en-administratie/handleiding-advocaten-notarissen-accountants-belastingadviseurs-en-administratiekantoren.pdf

[**MKB-1**] MKB-Service desk.
http://www.mkbservicedesk.nl/10941/mkb-slecht-voorgelicht-over-europese.htm

[**NBA-1**] Verordening gedrags- en beroepsregels accountants (VGBA), Geldend per 1 januari 2014, NBA.
https://www.nba.nl/tools/hra-2017/?folder=5791

[**NBA-2**] Nadere voorschriften controle- en overige standaarden, Standaard 230: Controledocumentatie, Ingangsdatum 1 januari 2017.
https://www.nba.nl/tools/hra-2017/?folder=899

[**NBA-3**] Datalekken in de praktijk, NBA, Oktober 2016.
https://www.nba.nl/globalassets/themas/thema-mkb/overige-publicaties/datalekken.pdf

[**NBA-4**] Presentatie datalekken en de accountant, NBA, 17 mei 2016.
https://www.nba.nl/globalassets/projecten/kennis-delen-pmls/cybersecurity/presentatie-datalekken-en-de-accountant.pdf

[**NBA-5**] NBA-handreiking 1124: Richtsnoeren voor de interpretatie van de Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT) voor belastingadviseurs en accountants, juni 2014.
https://www.nba.nl/globalassets/wet--en-regelgeving/nba-handreikingen/nba-handreiking_1124_richtsnoeren_wwft.pdf

[**NBA-6**] Website NBA inzake privacywetgeving en Meldplicht datalek.
https://www.nba.nl/tools-en-voorbeelden/model-bewerkersovereenkomst/

[**NBA-7**] Model bewerkersovereenkomst: Klant (Verantwoordelijke) – Accountant (Bewerker) EER, NBA.
https://www.nba.nl/contentassets/c7e72b5e2f22475d981f653649b90356/model_bewerkersovereenkomst_nba_bewerker_eer.docx

[**NBA-8**] Model bewerkersovereenkomst: Accountant (verwerker) – derde (sub-verwerker) EER, NBA.
https://www.nba.nl/contentassets/c7e72b5e2f22475d981f653649b90356/model_bewerkersovereenkomst_subbewerker_eer_24032017.docx

[**NBA-9**] Datalek wordt boardroom topic, Accountant.nl, 9 februari 2016.
https://www.accountant.nl/artikelen/2016/2/datalek-wordt-board-room-topic/#_ga=1.125169352.356022594.1480592963

[**NBA-10**] Let op privacy in de cloud, Accountant.nl, 16 februari 2016.
https://www.accountant.nl/artikelen/2016/2/let-op-privacy-in-de-cloud/#_ga=1.166601212.356022594.1480592963

[**NBA-11**] Van hype naar aanpak, Publieke managementletter over cybersecurity, NBA, mei 2016.
https://www.nba.nl/globalassets/projecten/kennis-delen-pmls/cybersecurity/pml-cyber-security.pdf

[**NBA-12**] De mkb-accountant en Cloud Computing (november 2014).
https://www.nba.nl/globalassets/themas/thema-mkb/nemacc/publicaties/nba-brochure-de-mkb-accountant-en-cloud-computing.pdf

[**NBA-13**] Handreiking bij Volwassenheidsmodel Informatiebeveiliging.
https://www.nba.nl/nieuws-en-agenda/nieuwsarchief/2016/mei/lio-presenteert-volwassenheidsmodel-informatiebeveiliging/

[**NBA-14**] Accountantsdag 2017, 7 Crazy facts.
https://www.nba.nl/accountantsdag-2017/crazy-facts/

[**NBA-15**] FRAUDE IN PRAKTIJK 100: Het Paard van Troje in de 21ste eeuw.
https://www.accountant.nl/artikelen/het-paard-van-troje-in-de-21ste-eeuw/

[**NCSC-1**] ICT-beveiligingsrichtlijnen voor webapplicaties.
https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

[**NCSC-2**] Beveiligingsrichtlijnen voor mobiele apparaten.
https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/beveiligingsrichtlijnen-voor-mobiele-apparaten.html

[**NCSC-3**] Cybersecuritybeeld Nederland (CSBN) 2017.
https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2017/1/CSBN2017.pdf

[**NCSC-4**] Beveilig apparaten gekoppeld aan internet, Factsheet FS-2012-07, versie 1.1 | 17 december 2012.
https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/factsheets/factsheet-beveilig-apparaten-gekoppeld-aan-internet/1/Factsheet%2BBeveilig%2Bapparaten%2Bgekoppeld%2Baan%2Binternet.pdf

[**NCSC-5**] Uw ICS/SCADA- en gebouwbeheersystemen online, Factsheet FS-2012-01, versie 2.2 | 6 juni 2016.
https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/factsheets/beveiligingsrisicos/1/Uw%2BICS%2BSCADA%2B%2Ben%2Bgebouwbeheersystemen%2Bonline.pdf

[**NEN-1**] Code voor Informatiebeveiliging NEN-ISO/IEC 27001+C11+C1+C2:2015 (nl), Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging – Eisen.
http://www.nen.nl/

[**NEN-2**] Code voor Informatiebeveiliging NEN-ISO/IEC 27002+C1+C2:2015 (nl), Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (ISO/IEC 27002:2013 en IDT).
http://www.nen.nl/

[**NEN-3**] NEN 7510.
http://www.nen7510.org

[**NEN-4**] NEN-ISO 31000 (2009) Risicomanagement - Principes en richtlijnen, geeft een kader voor integraal risicomanagement.
https://www.nen.nl/NEN-Shop/Norm/NENISO-310002009-nl.htm

[**NEMACC-1**] De gevolgen van cloud computing voor de werkzaamheden van de mkb-accountant.
https://www.nba.nl/globalassets/themas/thema-mkb/nemacc/publicaties/nemacc-gevolgen-cloud-computing-voor-mkb-accountant-jan-2014.pdf

[**NIST-1**] http://www.nist.gov/itl/cloud/index.cfm

[**NIST-2**] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[**NOREA-1**] Privacy-Audit-Proof.
https://www.privacy-audit-proof.nl/

[**NOREA-2**] Richtlijn 3600.
https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/richtlijn_3600_privacy-audit.pdf

[**NOREA-3**] Addendum bij Richtlijn 3600n.
https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/addendum-norea-privacy-audit-2016.pdf

[**NOREA-4**] Privacy Impact Assessment.
https://www.norea.nl/download/?id=522

[**NOREA-5**] Handreiking “Werkprogramma ‘Meldplicht Datalekken’, Versie 1.0 – Mei 2017”.
https://www.norea.nl/download/?id=2975

[**NOREA-6**] Cyber Security Assessment (NOREA-CSA), Introductie, handreiking en vragenlijst, Augustus 2015.
https://www.norea.nl/download/?id=2291

[**PCI-1**] PCI Security Standards Council, Data security standards overview.
https://www.pcisecuritystandards.org/security_standards/index.php

[**Pear-1**] Pearson. S. and Mont, M.C., Sticky Policies: An Approach for Managing Privacy across Multiple Parties, Computer, sept 2011
https://www.computer.org/csdl/mags/co/2011/09/mco2011090060.html

[**PMP-1**] “Grip op de AVG”, dr. Koen Vermissen, mr. Drs. Jeroen Terstegge, Natalja Krijgsman. Uitgave van Wolters Kluwer (2017) ISBN 978 90 13 13920 4

[**PMP-2**] “Grip op de AVG, werkboek”, dr. Koen Vermissen, mr. Drs. Jeroen Terstegge, Natalja Krijgsman. Uitgave van Wolters Kluwer (2017) ISBN 978 90 13 14439 0

[**PWC-1**] Privacy Governance-onderzoek mei 2017.
http://www.pwc.nl/nl/themas/digital/cybersecurity-privacy/privacy-en-de-avg/privacy-governance-onderzoek.html

[**RATHENAU -1**] Een nooit gelopen race, Over cyberdreigingen en versterking van weerbaarheid (2017).
https://www.aivd.nl/binaries/aivd_nl/documenten/rapporten/2017/03/02/rapport-rathenau-overheid-en-bedrijven-onvoldoende-beschermd-tegen-cyberdreigingen/20170302+Rathenau+Instituut++Een+nooit+gelopen+race.pdf

[**V&J-1**] Regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming).
https://www.internetconsultatie.nl/uitvoeringswetavg/document/2637

[**VNG-1**] Strategische baseline informatiebeveiliging.
https://www.ibdgemeenten.nl/wp-content/uploads/2016/07/Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.02.pdf.pagespeed.ce.8hl4iGUUOx.pdf

[**VNG-2**] Tactische-Baseline-Informatiebeveiliging.
https://www.ibdgemeenten.nl/wp-content/uploads/2016/07/Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.02.pdf.pagespeed.ce.qV9L-8-xni.pdf

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