Notitie Privacybeleid KRAMERKUIPER accountants|adviseurs

Inhoudsopgave notitie Privacybeleid KRAMERKUIPER accountants|adviseurs:

Bewustwording (A)

Tijdens de uitvoering van onze werkzaamheden communiceren wij elektronisch met onze cliënten en relaties. Hierin is tevens begrepen de onderlinge uitwisseling van persoonsgegevens, welke als data worden opgeslagen op onze computersystemen. Zoals mede benoemd in onze opdrachtbevestigingen zullen wij al hetgeen redelijkerwijs van ieder van ons verwacht mag worden, doen of nalaten ter voorkoming van het optreden van risico's voortvloeiende uit elektronische communicatie, het verwerken van persoonsgegevens en het voorkomen van datalekken.

Ons kantoor is niet verplicht om een privacybeleid op te stellen. Daar wij van mening zijn dat het verplicht opstellen van een privacybeleid (ook wel gegevensbeschermingsbeleid) niet in verhouding staat tot de door ons verrichte verwerkingsactiviteiten. Mede ingegeven door de beperkte omvang van onze verwerking van persoonsgegevens in relatie tot onze overige werkzaamheden zowel ten aanzien van onze tijdsbesteding als ook de omzet gemoeid met de verwerking van persoonsgegevens in relatie tot de omzet van het totale kantoor. Waarbij tevens opgemerkt wordt dat deze bewerking altijd plaats vindt onder eindverantwoordelijkheid van onze opdrachtgever. In veel gevallen is hiervan geen sprake, dan is ons kantoor de verwerkingsverantwoordelijke.

Wij zijn als kantoor wel van mening dat het nuttig is om een privacybeleid op te stellen. Hiermee trachten wij privacy risico's van verwerkingen van persoonsgegevens binnen ons kantoor inzichtelijk te maken, met vervolgens als doel het vermijden of verminderen van privacy risico's. Tevens laten wij hiermee, aan onze beroepsgroep en de Autoriteit Persoonsgegevens, zien dat wij invulling willen geven en willen voldoen aan de Algemene Verordening Gegevensbescherming (AVG).

In de notitie privacybeleid zal aandacht besteed worden aan 'the internet of things' binnen ons kantoor, de voor ons kantoor van toepassing zijnde soft- en hardware en onze leveranciers van cloud oplossingen.

Met deze notitie voldoen wij tevens aan onze verantwoordingsplicht (accountability) en trachten wij een belangrijke bijdrage te leveren aan de bescherming van het grondrecht van mensen op privacy. Hiermee laten wij zien dat wij de juiste technische en organisatorische maatregelen hebben genomen om persoonsgegevens te beschermen. En dat een verwerking voldoet aan rechtmatigheid, transparantie, doelbinding en juistheid.

De persoonsgegevens die door ons worden verkregen, opgeslagen en indien nodig worden bewerkt, vloeien voornamelijk voort uit onze accountancy- en fiscale werkzaamheden die wij beroepsmatig verrichten. Aan onze dienstverlening ligt een opdrachtbevestiging met onze cliënt ten grondslag. Wij zijn ons bewust van het feit dat cliënten waarvoor wij persoonsgegevens verwerken, het recht hebben op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens en het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

In deze notitie privacybeleid en het verwerkingsregister zal, waar van toepassing een omschrijving gegeven worden van de categorieën persoonsgegevens die wij verwerken. Hierbij is onze verplichting om niet meer persoonsgegevens te verwerken dan noodzakelijk wordt geacht om ons beroep te kunnen uitvoeren en onze diensten te kunnen verrichten. Persoonsgegevens worden daarnaast niet langer dan noodzakelijk voor onze beroepsgroep bewaard.

Door ons worden geen gegevens gedeeld met een land of internationale kantoor buiten de Europese Unie. Wij gebruiken de gegevens alleen voor de afgesproken doelen, zullen de gegevens niet zonder toestemming met anderen delen en zorgvuldig beveiligen.

Onze medewerkers:

- Zijn op de hoogte gebracht van de privacyregels;
- Zijn zich bewust van de huidige dreigingen op het terrein van informatiebeveiliging (cybercrime) en de belangrijkste oorzaken van datalekken; en
- Weten wat wij van hen in het kader van informatiebeveiliging en privacybescherming verwachten qua houding en gedrag.

Bij het opstellen van deze notitie is mede als leidraad gebruikt het 10 stappenplan van de Autoriteit persoonsgegevens. Literatuur is geraadpleegd en er zijn trainingen gevolgd:

Geraadpleegde literatuur

1. NBA Toolkit AVG;
2. SRA dossier AVG;
3. NBA, Datalekken in de MKB praktijk;
4. NBA, model (sub-)bewerkersovereenkomst;
5. SRA, model (sub-)bewerkersovereenkomst;
6. NBA NEMACC, brochure privacybescherming;
7. Autoriteit persoonsgegevens, website;
8. Autoriteit persoonsgegevens, 10 stappenplan;
9. Beleidsregels voor toepassing van artikel 34a van de Wbp (melding datalekken);
10. Ministerie van Veiligheid en Justitie, 10 vuistregels veilig internetten.

Data Protection Impact Assessment, PIA (B)

Wij zijn van mening dat wij niet verplicht zijn een zogenaamd Data Protection Impact Assessment uit te voeren, daar onze beoogde gegevensverwerking waarschijnlijk geen hoog privacyrisico met zich meebrengt. Daar wij als kantoor niet:

- systematisch en uitvoerig persoonlijke aspecten evalueren;
- op grote schaal bijzondere persoonsgegevens verwerken;
- op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied.

Gezien de omvang van onze kantoor volstaan wij met het opstellen van een notitie privacybeleid (waarin begrepen een risico inventarisatie onder paragraaf F) alsook het opstellen van een verwerkingsregister.

Functionaris voor de gegevensbescherming (C)

Wij zijn van mening dat wij geen functionaris voor de gegevensbescherming behoeven aan te stellen, daar wij niet kwalificeren als een kantoor zoals benoemd onder paragraaf B. Deze functionaris behoudt binnen de eigen kantoor toezicht op de toepassing en naleving van de AVG. Gezien onze geringe omvang behoeven wij deze functionaris niet te benoemen. Wij zijn ons als kantoor uiteraard bewust van een gedegen databescherming en wij realiseren ons dat data bescherming en het up to date houden hiervan, alsmede voldoen aan de AVG een continue proces is. De heer C. Kramer is binnen kantoor wel aangewezen als de personen waarbij medewerkers vragen kunnen stellen inzake gegevensbescherming en waarbij een datalek dient te worden gemeld.

Leidende toezichthouder (D)

Er is geen sprake van een leidende toezichthouder. Daar onze kantoor maar één vestiging kent en tevens niet is aangesloten bij een internationaal, opererend kantoor en/of netwerk. Onze gegevensverwerking heeft ook geen impact op meerdere lidstaten binnen de Europese Unie. Door ons worden geen gegevens gedeeld met een land of internationale kantoor buiten de Europese Unie.

Privacy by design & privacy by default (E)

Als kantoor voeren wij onze dienstverlening uit, in lijn met de uitgangspunten privacy by design en privacy by default.

De definities van privacy by design en privacy by default zijn ontleend aan de website Autoriteit Persoonsgegevens: Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat niet meer gegevens verzameld worden dan noodzakelijk voor het doel van de verwerking. En dat de gegevens niet langer bewaard worden dan nodig.

Privacy by default houdt in dat technische en organisatorische maatregelen genomen moeten worden om ervoor te zorgen dat wij alléén persoonsgegevens verwerken die noodzakelijk zijn voor het specifieke doel dat wij willen bereiken.

In onze omgang met privacy gevoelige informatie, het bewaren en verwerken van (persoons)gegevens en elektronische communicatie betrachten wij een professioneel kritische en alerte houding aan te nemen. Dit uit zich onder meer in het feit dat wij het risico op een datalek trachten te voorkomen door het risico op onder meer malware te verkleinen door:

- tijdige software updates installeren waar nodig met de expertise van onze automatiseerder/ software leverancier;
- wij geen verouderde protocollen gebruiken;
- wij periodiek back-ups maken.

Binnen ons kantoor zijn de 10 vuistregels van veilig internetten opgemaakt door het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie bekend en wordt invulling gegeven hieraan. Dit impliceert dat:

A. Antivirus programma's zijn geïnstalleerd (in samenwerking met Woip);
B. Software updates worden uitgevoerd wanneer deze beschikbaar komen (in samenwerking met Woip);
C. Er worden 'sterke' wachtwoorden gehanteerd;
D. Er is alleen verbinding met vertrouwde wifi netwerken;
E. Er worden geen email berichten en onbekende bestanden geopend die wij niet vertrouwen en/of waarvan wij de afzender niet kennen;
F. Er worden alleen apps en programma's van bekende, officiële partijen gebruikt;
G. Webadressen (URL's) worden altijd gecontroleerd om vast te stellen of er sprake is van een nagemaakte of onveilige website;
H. Pop-ups worden in de browser niet geopend en waar nodig afgesloten met Alt+F4;
I. Wij denken goed na over te delen informatie op het internet (waaronder in ieder geval wordt verstaan onze website en sociale netwerksites);
J. Wij gebruiken ons gezond verstand, "iets wat te mooi lijkt om waar te zijn, is dat meestal ook."

Verwerkingsregister (F)

Data opslag (waar staan data, welke data, bij wie staan ze, wie kan erbij, contracten)
Binnen ons kantoor is een verwerkingsregister opgesteld daar ons kantoor minder dan 250 medewerkers heeft en wij beschikken over persoonsgegevens:

- die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of;
- waarvan de verwerking niet incidenteel is en/of;
- die vallen onder de categorie bijzondere persoonsgegevens.

Wij verwerken in opdracht van een verantwoordelijke persoonsgegevens. De verwerking ziet op het verwerken van financiële administraties en salarisadministraties. In het verwerkingsregister van ons kantoor is de volgende informatie opgenomen:

- de naam en contactgegevens van onze kantoor en de vertegenwoordiger;
- het doel waarvoor wij de persoonsgegevens verwerken;
- een beschrijving van de categorieën van verwerkingen die wij in opdracht van iedere verantwoordelijke uitvoeren;
- een beschrijving van de categorieën van persoonsgegevens.

Een algemene beschrijving van de technische en organisatorische maatregelen die wij hebben genomen om persoonsgegevens te beveiligen is in deze notitie opgenomen.

Risico inventarisatie (G)

Bij onze risico inventarisatie hebben wij een onderscheid gemaakt naar: organisatorische maatregelen en technische maatregelen.

Organisatorische maatregelen

Ten aanzien van de organisatorische maatregelen is door ons kantoor deze notitie opgesteld, is een privacy- en cookiebeleid opgemaakt welke beschikbaar gesteld is op onze website en werken wij met (sub)bewerkersovereenkomsten. Ten aanzien van het gebruik van cloudoplossingen, aanschaf van hard- en software producten het volgende: als kantoor streven wij naar kwaliteit en het samen willen werken met in de praktijk bekende en bewezen producten van betrouwbare partijen. Voorafgaand aan deze keuze verdiepen wij ons in de aangeboden producten van de betreffende leverancier en waar mogelijk diens concurrenten, testen en analyseren wij de producten bij voorkeur in een demo (test)omgeving indien die mogelijk en van toepassing is. Tevens informeren wij binnen ons netwerk (collega accountants) of collega's ervaringen hebben met betreffende partijen en diens producten. Deze testwerkzaamheden worden vroegtijdig en normaliter buiten ons 'business season' uitgevoerd, waarmee wij de prioriteit hiermee willen aangeven die gemoeid is met de keuzes die wij hierin als kantoor maken.

In onze opdrachtbevestiging benoemen wij onder hoofdstuk elektronische communicatie de risico's die hiermee mogelijk gepaard kunnen gaan. Indien cliënt elektronisch communicatie niet op prijs stelt dan dient opdrachtgever dit te melden, waarna wij gepaste maatregelen zullen nemen. In die situatie worden privacy gevoelige gegevens per post verzonden aan opdrachtgever.

Er is een verzekering afgesloten, waarbij onder meer de inzet van technische experts bij calamiteiten wordt gewaarborgd.

Ons kantoor is gevestigd in een bedrijfsverzamelgebouw aan de Ampèrestraat 43 te Purmerend. De fysieke beveiliging wordt door ons als goed beschouwd. Het pand is uitsluitend toegankelijk met een zogenoemde druppel. Met deze druppel kan de voordeur van het pand geopend worden. Tevens wordt de druppel gebruikt om het alarm van ons deel van het

bedrijfsverzamelgebouw aan of uit te zetten. Hiernaast zijn er fysieke sleutels nodig om in ons kantoor binnen het bedrijfsverzamelgebouw te komen.

Technische maatregelen

Binnen onze kantoor maken wij gebruik van de Data-, applicatie- terminal en back-up servers van Woip (zie bijlage "Netwerkdiagram"). Dit geldt alleen nog voor de "legacy software". Vrijwel alle applicaties worden direct via de leverancier gehost, dit betreffen:

- Fiscaal Gemak;
- Personeels en Salaris Online;
- Exact Online;
- Simplicate;
- Grub;
- Sharepoint;
- Audit+;
- Validsign;
- Visma Compilation.

Op de laptops is geen bedrijfssoftware geïnstalleerd. Bedrijfslaptops worden alleen gebruikt om via internet in te loggen op de kantooromgeving. De laptops zijn gekoppeld aan onze Microsoft Tenant. Een overzicht van de bedrijfslaptops en IT randapparatuur wordt separaat bijgehouden op de interne Sharepoint.

De beveiliging, installatie en back-up van de systemen zijn volledig uitbesteed aan Woip en de leveranciers van de applicaties.

Hard- en software technische beveiliging

Toegangsbeveiliging netwerk

Medewerkers loggen in middels een gebruikersnaam en wachtwoord. Het wachtwoord dient minimaal een cijfer, hoofdletter en bijzonder teken te bevatten en wordt elk jaar (afgedwongen) gewijzigd. Voor de applicaties die worden gehost door de leveranicers (Cloud oplossingen) is eveneens sprake van toegangsbeveiliging via een gebruikersnaam en wachtwoord. Met ingang van 2021 is daarnaast sprake van 2 factor authentication, waarbij medewerkers voor vrijwel elke applicatie ook een code op de telefoon dienen in te voeren.

Laptops

De laptops zijn beveiligd met een Windows wachtwoord. Het Windows wachtwoord moet een uniek, sterk wachtwoord (minimaal een combinatie van cijfers en letters) zijn. Het beleid is dat op de laptops geen data van cliënten lokaal opgeslagen wordt. Periodiek moet de map 'downloads' alsook de 'prullenbak' leeggemaakt worden. Er wordt zorgvuldig (als goed huisvader) omgegaan met de laptops, deze mogen niet 'alleen' gelaten worden. De laptop valt na twee minuten automatisch in de beveiligde modus. Er mag géén privé software/ programmatuur geplaatst worden op de zakelijk gehouden laptop.

Op het moment dat laptops vervangen worden, dan worden de 'oude' laptops door de automatiseerder geschoond van zakelijke programmatuur en worden de bestanden verwijderd.

Clientdossiers

De clientdossiers zijn ingericht in de betreffende applicaties. Voor elke cliënt is er daarnaast een aparte Sharepoint site. Medewerkers hebben standaard *geen* toegang tot de Sharepointsite van een cliënt. Via de Admin account kunnen de rechten van de medewerkers worden aangepast. De heer C. Kramer en mevrouw L. Quist hebben toegang tot het Admin account via een apart gebruikersprofiel, dat is beveiligd middels een wachtwoord.

Fileshare

Voor de opslag van data wordt gebruikt gemaakt van de SharePoint. De toegang tot de bestanden in de Sharepoint zijn beveiligd door midden van rechten die aan de profielen van de medewerker zijn gekoppeld. Tevens wordt de toegang tot de bestanden wordt gelogd.

Back-up en recovery

De back-up procedure is uitbesteed aan Woip en onderdeel van de SLA/verwerkersovereenkomst. Er vindt separate back-up van de Sharepoint omgeving plaats.

Mobiele telefoons

De mobiele telefoons zijn beveiligd met een pincode en touch id/face id. De vennoten zijn zich bewust van de telefoonnummers en namen van cliënten en relaties die zich op de mobiele telefoons bevinden. Zij gaan als een goed huisvader overweg met de mobiele telefoons.

In geval van diefstal of verlies dan kunnen de mobiele telefoons op afstand gevolgd, leeggemaakt worden en/of versleuteld worden via 'vind mijn iPhone'.

Data uitwisseling

Bij gebruik van USB sticks worden deze direct geschoond nadat bestanden zijn overgezet. Bestanden worden bij voorkeur via de e-mail verzonden of gedeeld via SharePoint.

Email

Emailberichten worden enkel vanuit het zakelijke emailaccount in Outlook verzonden. Er wordt voorafgaand aan de verzending scherp gelet op het selecteren van de juiste ontvanger. Mocht er onverhoopt een email verzonden zijn aan een verkeerde ontvanger dan is het verzoek om ons dit onmiddellijk te melden en het bericht te vernietigen. Onderstaande tekst moet onder elk uitgaande kantooremail opgenomen zijn:

"Indien u dit bericht per vergissing heeft ontvangen, verzoeken wij u ons onmiddellijk op de hoogte te stellen en dit bericht te vernietigen"

Wifi netwerk

Binnen het bedrijfsverzamelgebouw komen diverse glasvezel netwerken binnen die van elkaar gescheiden zijn. Er is een eigen wifi netwerk en een apart wifi netwerk voor gasten beschikbaar. Het wifinetwerk is beveiligd met een zeer sterk wachtwoord. Het gasten wifi netwerk is bestemd voor derden (lees cliënten) en wordt alleen met relaties op kantoor gedeeld. Het gasten netwerk is beveiligd met een wachtwoord. Hiernaast heeft elke kamer een eigen wifi punt wat afzonderlijk beveiligd is. Het wifi netwerk staat los van het bedrijfsnetwerk (aparte modem én internprovider).

Cloudoplossingen

Alle cloudoplossingen hebben veiligheidstoepassingen, waaronder toegangsbeveiliging. Wij zijn van mening dat alle genoemde partijen afdoende maatregelen hebben genomen om de data van onze cliënten te waarborgen. Met de leveranciers van bovenstaande applicaties hebben wij een verwerkersovereenkomst gesloten of overeenkomst afgesloten waarin de beveiliging van de data is geregeld.

Toestemming en (sub)bewerkersovereenkomsten (H)

De AVG eist dat wij moeten kunnen aantonen dat wij geldige toestemming van betrokkenen hebben gekregen om persoonsgegevens te verwerken. De twee eisen die gesteld worden aan een geldige toestemming zijn dat deze geïnformeerd en specifiek gegeven is. Zo moeten organisaties kunnen bewijzen dat zij geldige toestemming hebben gekregen.

Indien sprake is van de verwerking van persoonsgegevens waarbij wij optreden als verwerker en de klant als verantwoordelijke dan leggen wij de afspraken vast in een verwerkersovereenkomst. Hiertoe maken wij gebruik van de model overeenkomsten zoals deze beschikbaar gesteld worden door de NBA/SRA.

Meldplicht datalekken (I)

Bij de beslissing of wij een gebeurtenis die zich heeft voorgedaan moeten melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moeten wij een aantal afwegingen maken. Het onderstaande schema, ontleend aan de beleidsregels voor toepassing van artikel 34a van de wet Wbp geeft onze afwegingen weer:

Beveiligingslek -> Heeft zich een beveiligingsincident voorgedaan?

Datalek -> Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan, of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?

Melden aan de Autoriteit Persoonsgegevens -> Gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?

Melden aan de betrokkene -> Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker. Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

Indien een melding gedaan moet worden, dan wordt het meldformulier van het meldloket datalekken gehanteerd.

Ondertekening (J)

C.J.G.P. Kramer RA	M. Kuiper AA
Beleidsbepaler	Beleidsbepaler

BIJLAGEN (K)

In de bijlagen bij deze notitie privacybeleid worden behandeld:

A. Definities
B. Cloudoplossingen partijen

Ad A. Definities

Wet bescherming persoonsgegevens (Wbp)
De wet bescherming persoonsgegevens is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens. De Wbp is sinds 1 september 2001 van kracht.

Algemene Verordening Gegevensbescherming (AVG)
Op 4 mei 2016 is de AVG gepubliceerd door de Europese Unie. De verordening is van kracht met ingang van 25 mei 2018. Vanaf die datum geldt dezelfde privacywetgeving in de hele Europese Unie.

Wat zijn persoonsgegevens?
In de Algemene verordening gegevensbescherming(AVG) staat als definitie voor persoonsgegevens: 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'. Dit betekend dat informatie ofwel direct over iemand gaat of ofwel naar deze persoon te herleiden is.

Voor de hand liggende gegevens zijn iemands naam, adres, woonplaats telefoonnummer en pasfoto. Maar persoonsgegevens zijn bijvoorbeeld ook: informatie over wat iemand op internet doet of koopt, of iemand allergieën heeft, klant- of personeelsnummers, maar ook kan een IP-adres een persoonsgegeven zijn.

Persoonsgegevens van gevoelige aard
Persoonsgegevens waarbij verlies of onrechtmatige verwerking kunnen leiden tot (onder meer) stigmatisering of uitsluiting van Betrokkene , schade aan de gezondheid, financiële schade of tot (identiteits)fraude. Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend:

- Bijzondere persoonsgegevens;
- Gegevens over de financiële of economische situatie van de Betrokkene;
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de Betrokkene;
- Gebruikersnamen, wachtwoorden en andere inloggegevens;
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude.

Wat zijn bijzondere persoonsgegevens?
Een kantoor mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is. Bijzondere persoonsgegevens zijn gegevens vanuit:

- godsdienst of levensovertuiging;
- ras;
- politieke voorkeur;
- gezondheid;
- seksuele leven;
- lidmaatschap van een vakbond;

Naast de bijzondere persoonsgegevens zijn er ook andere gevoelige persoonsgegevens die niet vallen onder het begrip bijzondere persoonsgegevens, maar waarvoor wel speciale regels gelden zoals:

- strafrechtelijk verleden;
- burgerservicenummer (BSN).

Wat houdt verwerken van persoonsgegevens in?
Verwerken is alle handelingen die een kantoor kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen. Dit is dus een zeer ruim begrip. Handelingen die er volgens de Algemene verordening gegevensbescherming (AVG) in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Vanuit de website van de NBA geciteerd: “Verwerking van persoonsgegevens” omvat alle denkbare handelingen met persoonsgegevens. Maar let op: ook meer passieve handelingen zoals de enkele aanwezigheid van de gegevens op uw servers valt onder het begrip “verwerken”. Bij “persoonsgegevens” denkt u ongetwijfeld aan gegevens als NAW, BSN en herkenbare afbeeldingen zoals pasfoto’s. Maar ook gegevens die in eerste instantie misschien geen persoonsgegevens lijken, kunnen dat zijn: bijvoorbeeld IP-adressen en binnen een bepaalde context ook (mobiele) telefoonnummers en nummerborden. Volgens de AVG is de verantwoordelijke degene die bepaalt wat met de persoonsgegevens moet of mag worden gedaan en hoe en is de verwerker degene die dienaangaande instructies van de verantwoordelijke dient op te volgen. Dit laatste brengt met zich mee dat indien u een verwerker bent, u niet vrijelijk kunt bepalen (dat wil zeggen niet zonder voorafgaande toestemming) hoe u bepaalde persoonsgegevens gebruikt.

Wie is verwerker?
Een verwerker is een persoon of kantoor aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed. Een verwerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens. Maar de bewerker heeft wel een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens.

Wie is subverwerker?
Uit de verantwoordelijkheid van de opdrachtgever – die in de zin van de wet geldt als verantwoordelijke voor de gegevensverwerking – vloeit voort dat hij uitdrukkelijk heeft ingestemd met het subverwerkersschap. Indien de opdrachtgever daarvoor in zijn overeenkomst met de verwerker uitdrukkelijk ruimte heeft gegeven, kan de verwerker – met behoud van zijn volle

aansprakelijkheid voor de naleving van zijn contract met de verantwoordelijke – delen van de verwerking uitbesteden aan sub-bewerkers.

De verwerker dient dan wel contractueel verzekerd te hebben dat de sub- verwerker zich eveneens richt naar de instructies van de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt. De verantwoordelijke dient hiervan wel op de hoogte te worden gesteld opdat deze in staat is toe te zien op de naleving van zijn afspraken met de verwerker.

Dienstverlening door verwerker
Het verwerkersbegrip is in principe van toepassing op verschillende vormen van dienstverlening. Uitgangspunt is daarbij dat de dienstverlening betrekking heeft op het verwerken van persoonsgegevens. Zodra de gegevensverwerking een uitvloeisel is van een andere vorm van dienstverlening, is de dienstverlener daarvoor zelf verantwoordelijk.

Datalek
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot - of waarbij redelijkerwijs niet uit te sluiten valt dat die kan leiden tot - de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Meldplicht datalekken
De verplichting tot het melden van Datalekken aan de Autoriteit Persoonsgegevens en (in sommige gevallen) aan Betrokkene(n).

Rechten van betrokkenen
Betrokkenen hebben **recht op inzage**. Dat houdt in dat zij een kantoor mogen vragen of deze persoonsgegevens van hen heeft vastgelegd en zo ja, welke. Zij hoeven geen reden te geven voor een inzageverzoek. Het recht op inzage betreft alleen inzage in iemands eigen gegevens. Mensen hebben dus geen recht op informatie over anderen.

Vraagt iemand om inzage, dan moet de kantoor diegene op een duidelijke en begrijpelijke manier laten weten óf de kantoor zijn persoonsgegevens gebruikt, en zo ja:

- om welke gegevens het gaat;
- wat het doel is van het gebruik;
- aan wie de kantoor de gegevens eventueel heeft verstrekt;
- wat de herkomst is van de gegevens, als deze bekend is.

Mensen hebben het **recht om correctie** van hun persoonsgegevens te vragen. Dat houdt in dat zij een kantoor mogen vragen hun persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Iemand kan om correctie vragen als zijn persoonsgegevens:

- feitelijk onjuist zijn;
- onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
- op een andere manier in strijd met een wet worden gebruikt.

Onder de AVG krijgen betrokkenen het **recht op dataportabiliteit**, oftewel overdraagbaarheid van persoonsgegevens. Dit houdt in dat zij het recht hebben om de persoonsgegevens te ontvangen die een kantoor van hen heeft.

Het **recht op vergetelheid** houdt in dat organisaties in een aantal gevallen persoonsgegevens moeten wissen als een betrokkene hierom vraagt. Dit nieuwe recht lijkt op het huidige recht op correctie en verwijdering, maar is breder.

In de AVG staan tevens de voorwaarden voor organisaties om **geldige toestemming** te krijgen van mensen om hun persoonsgegevens te verwerken. De twee eisen die gesteld worden aan een geldige toestemming zijn dat deze geïnformeerd en specifiek gegeven is. Zo moeten organisaties kunnen bewijzen dat zij geldige toestemming hebben gekregen. En moet het voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven.