Notitie Privacybeleid
- Gegevensbescherming, Cybercriminaliteit, Meldplicht Datalekken -

Inhoudsopgave notitie Privacybeleid Kantoor Zon Accountants & Adviseurs B.V.:

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 vaak plaats vindt onder eindverantwoordelijkheid van onze opdrachtgever. In situaties waarbij ons kantoor een jaarrekening samenstelt, beoordeelt, controleert of een assurance-opdracht uitvoert is hiervan geen sprake. Dan is ons kantoor de eindverantwoordelijke.

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-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 internationaal 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 nieuwe 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, Privacy toolkit, maart 2018
2. NBA, model (sub-)bewerkersovereenkomsten
3. Autoriteit persoonsgegevens, website d.d. 24 mei 2018
4. Autoriteit persoonsgegevens, 10 stappenplan
5. Beleidsregels voor toepassing van artikel 34a van de Wbp (melding datalekken)
6. Ministerie van Veiligheid en Justitie, 10 vuistregels veilig internetten

Gevolgde trainingen

1. Auxilium Adviesgroep, update voorjaar d.d. 5 maart 2018
2. NBA, Spitsuursessie d.d. 25 april 2018

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 ons 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 het 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.

Leidende toezichthouder (D)

Er is geen sprake van een leidende toezichthouder. Daar ons 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 internationaal 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;
- computernetwerken en systemen hebben gescheiden, het netwerk blijft ten alle tijden op kantoor, laptops worden indien op locatie gebruikt enkel tijdelijk buiten de kantooromgeving gehouden;
- wij periodiek back-ups maken op externe, losgekoppelde, beveiligde gegevensdragers.

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;
B. Software updates worden uitgevoerd wanneer deze beschikbaar komen;
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 de salarisadministratie (alleen eigen personeel-DGA).

In het verwerkingsregister van ons kantoor is de volgende informatie opgenomen:

- de naam en contactgegevens van ons kantoor en de vertegenwoordiger;
- het doel waarvoor wij de persoonsgegevens verwerken (salaris of pensioen in eigen beheer);
- een beschrijving van de categorieën van verwerkingen die wij in opdracht van iedere verantwoordelijke uitvoeren (klanten, medewerkers van klanten);
- een beschrijving van de categorieën van persoonsgegevens (BSN, NAW-gegevens, geboortedatum, emailadressen, telefoonnummers).

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 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 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.

Kantoor aan huis

Ons kantoor is gevestigd op hetzelfde adres (woonadres) van de eindeverantwoordelijke accountant. De fysieke beveiliging wordt door ons als goed beschouwd. Het kantoor is een afzonderlijke ruimte en wordt afgesloten. De sleutels van de ruimte zijn enkel in het bezit van de eindverantwoordelijke accountant. Daarnaast zijn de dossiers opgeborgen in kasten met sloten.

Technische maatregelen

Binnen onze kantoor maken wij gebruik van de volgende hardware:

1. Laptops (2 ex.)
2. All-in-one printer HP Officejet (1 ex.)
3. Wester Digital (WD) Elements portable externe harde schijf (1 ex.)
4. Mobiele telefoons Apple Iphone 8 (1 ex.)

Binnen onze kantoor is de volgende software geïnstalleerd op onze laptops:

1. Microsoft Office Pakket

Hard- en software technische beveiliging

De laptops zijn beveiligd met een Bios wachtwoord én een Windows wachtwoord. Het Windows wachtwoord moet een uniek, sterk wachtwoord (minimaal een combinatie van cijfers en letters) zijn. 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.

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

Back-up en recovery

Tweewekelijks vindt een back up plaats van de laptop op een externe harde schijf. Dit geschiedt automatisch.

Periodiek wordt getest of de back up en recovery procedure werkt. Deze controle vindt visueel plaats door te beoordelen of recente bestanden in de back-up zijn opgenomen en bestanden in de back-up terug te zetten.

Mobiele telefoons

De mobiele telefoons zijn beveiligd met een pincode en touch id. De eindverantwoordelijke accountant is zich bewust van de telefoonnummers en namen van cliënten en relaties die zich op de mobiele telefoons bevinden, alsmede de zakelijke mail. Hij gaat 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

Data-uitwisseling vindt zoveel als mogelijk via de mail plaats. Bij hoge uitzondering en na onderlinge afstemming/instemming met cliënt wordt voor grote bestanden WeTransfer gebruikt.

Email

De outlook bestanden staan op de betreffende laptop en bij de serviceprovider.

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:

"*Disclaimer: De informatie verzonden in dit e-mailbericht en eventuele bijlage(n) is uitsluitend bestemd voor de geadresseerde(n) en kan informatie bevatten die persoonlijk of vertrouwelijk is. Openbaarmaking, vermenigvuldiging en/of verspreiding van deze informatie aan derden is, behoudens voorafgaande toestemming van Zon Accountants & Adviseurs B.V. strikt verboden. Indien bovenstaand e-mailbericht niet aan u is gericht of ten onrechte bij u is aangekomen, verzoeken wij u vriendelijk doch dringend het e-mailbericht terug te sturen aan de afzender en het origineel en eventuele kopieën te vernietigen. Zon Accountants & Adviseurs B.V. kan niet garanderen dat dit e-mailbericht juist, tijdig, volledig, virusvrij en zonder inbreuk of tussenkomst van onbevoegde(n) wordt overgebracht en kan hiervoor niet aansprakelijk worden gesteld. Het verzenden van e-mailberichten aan Zon Accountants & Adviseurs B.V. geschiedt geheel voor eigen risico.*".

De laptops zijn voorzien van Norton Virusscan. Genoemd abonnement wordt jaarlijks automatisch verlengd. De geplaatste router Linksys is beveiligd met een Firewall.

Wifi netwerk

Er is een Lokaal (eigen) Netwerk aanwezig. Het netwerk heeft een beheerdersaccount met een uniek wachtwoord. Het wifi netwerk wordt niet gedeeld met derden en is beveiligd met een zeer sterk wachtwoord.

Het kantoor maakt gebruik van een netwerk, bestaande uit 2 laptops en HP Officejet All-in-One. Deze zijn via kabels onderling verbonden en niet aangesloten op het wifi netwerk.

Website

De domeinnaam zonaccountants.nl is geregistreerd bij Yourhosting. De website is nog niet in gebruik. Door Yourhosting zijn de volgende beveiligingsmaatregelen getroffen:

Yourhosting: domeinnaam registratie en webmail (tekst ontleend aan Yourhosting)

De url www.zonaccountants.nl wordt gehost bij Yourhosting. Tevens maken wij gebruik van de webmail gefaciliteerd door yourhosting.

Bij Yourhosting ben je verzekerd van een veilige en betrouwbare omgeving. Onze informatiebeveiliging is gewaardeerd met de hoogst haalbare certificeringen. Daarnaast is Yourhosting 100% Nederlands en staat je data veilig op Nederlandse bodem. Met meer dan 15 jaar ervaring kunnen we alle soorten internetbedreigingen bovendien zo goed als mogelijk elimineren.

We monitoren ons netwerk en onze servers 24/7. Ook 's nachts en in het weekend lossen onze technische specialisten eventuele storingen direct op. De recovery-tijd hangt af van het type probleem, de responstijd is meestal enkele minuten.

Een DDoS-aanval komt van buitenaf en is helaas niet te voorkomen. Wél beperken we de gevolgen aanzienlijk door met de meest moderne en geavanceerde systemen het internetverkeer op ons netwerk continu te analyseren. Zo kunnen we snel ingrijpen als we onregelmatigheden signaleren.

Al het e-mailverkeer van onze managed hostingdiensten verloopt via ons Spamexperts-cluster. Daar wordt het continu gescand. Internetdreigingen als malware, phishing, virussen en spam beperken we zo tot een minimum.

Onze flexibele firewalls zijn voorzien van de modernste technieken en gedeeld in te zetten op maatwerkprojecten. Ze beveiligen in eerste instantie het gehele netwerk, maar kunnen ook integraal deel uitmaken van je maatwerkoplossing. Je kunt ook een virtuele firewall laten configureren.

Cloudoplossingen

Door ons kantoor wordt vooralsnog geen gebruik gemaakt van cloudoplossingen.

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 bewerker en de klant als verantwoordelijke dan leggen wij de afspraken vast in een bewerkersovereenkomst. Hiertoe maken wij gebruik van de model overeenkomsten zoals deze beschikbaar gesteld worden door de NBA.

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)

Amstelveen, 27 augustus 2018

drs. S. Born RA (eindverantwoordelijke accountant)

BIJLAGEN (K)

In de bijlagen bij deze notitie privacybeleid worden behandeld:

A. **Definities**
B. **Cloudoplossingen partijen (nvt)**

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 wordt echter met ingang van 25 mei 2018 gehandhaafd. Vanaf die datum geldt dezelfde privacywetgeving in de hele Europese Unie, waarmee de wet Wbp niet meer geldt. De AVG kent meer verplichtingen dan de wet Wbp.

Wat zijn persoonsgegevens?

De Wet bescherming persoonsgegevens (Wbp) geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.

Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens.

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;
- 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 Wet bescherming persoonsgegevens (Wbp) 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 Wbp is de verantwoordelijke degene die bepaalt wat met de persoonsgegevens moet of mag worden gedaan en hoe en is de bewerker degene die dienaangaande instructies van de verantwoordelijke dient op te volgen. Dit laatste brengt met zich mee dat indien u een bewerker bent, u niet vrijelijk kunt bepalen (dat wil zeggen niet zonder voorafgaande toestemming) hoe u bepaalde persoonsgegevens gebruikt.

Wie is bewerker?

Een bewerker is een persoon of kantoor aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed. Een bewerker 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 subbewerker?

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 subbewerkersschap. Indien de opdrachtgever daarvoor in zijn overeenkomst met de bewerker uitdrukkelijk ruimte heeft gegeven, kan de bewerker – met behoud van zijn volle aansprakelijkheid voor de naleving van zijn contract met de verantwoordelijke – delen van de verwerking uitbesteden aan sub-bewerkers.

De bewerker dient dan wel contractueel verzekerd te hebben dat de sub- bewerker 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 bewerker.

Dienstverlening door bewerker

Het bewerkersbegrip 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.

Ad B. Cloudoplossingen partijen (nvt)