04 87 · 59 16 50
poort@poortvanhulst.nl

Postbus 90
6658 ZH Beneden Leeuwen

Beleid inzake gegevens- / privacybescherming

- Gegevensbescherming, Cybercriminaliteit, Meldplicht Datalekken -

INHOUDSOPGAVE

BEWUSTWORDING (A)

Tijdens de uitvoering van onze werkzaamheden communiceren wij mondeling, schriftelijk en elektronisch met onze cliënten en relaties. Persoonsgegevens, welke als data worden opgeslagen op onze computersystemen, kunnen onderling worden uitgewisseld. Zowel met cliënten als relaties waarmee wij werken. Discretie en het vertrouwelijk omgaan met deze gegevens vormen een basis voor onze samenwerking.

Wij zullen al hetgeen redelijkerwijs van ieder van ons verwacht mag worden, doen of nalaten ter voorkoming van het optreden van risico's voortvloeiende uit het verwerken van deze persoonsgegevens en het voorkomen van datalekken.

Wij vinden het nuttig om een beleid ter bescherming van de gegevens van cliënten op te stellen (hierna te noemen gegevensbeschermings-/privacybeleid). Hiermee willen wij privacy risico's van verwerkingen van persoonsgegevens binnen ons kantoor inzichtelijk maken. Het doel is het verminderen of vermijden van deze risico's en datalekken. Tevens willen wij hiermee invulling geven aan- en voldoen aan de Algemene Verordening Gegevensbescherming (AVG). In dit 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 dit beleid willen wij voldoen aan onze verantwoordingsplicht (accountability) en een bijdrage leveren aan de bescherming van het grondrecht van mensen op privacy. We laten zien welke technische en organisatorische maatregelen we hebben genomen om persoonsgegevens te beschermen. En dat de verwerking van persoonsgegevens voldoet aan rechtmatigheid, transparantie, doelbinding en juistheid.

De persoonsgegevens die door ons worden verkregen, opgeslagen en indien nodig worden bewerkt, vloeien voornamelijk voort uit opdrachten van cliënten die wij verkrijgen als:
- Werkzaamheden als financieel planner
- Werkzaamheden als levensexecuteur
- Werkzaamheden als assurantietussenpersoon

Cliënten hebben het recht 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 dit privacybeleid én in het verwerkingsregister zal, waar van toepassing, een omschrijving gegeven worden van de categorieën persoonsgegevens die wij verwerken. Wij willen niet meer persoonsgegevens verwerken dan noodzakelijk wordt geacht om ons werk te kunnen uitvoeren en onze diensten te kunnen verrichten. Persoonsgegevens worden niet langer dan noodzakelijk bewaard.

Wij gebruiken de gegevens alleen voor de afgesproken doelen; we zullen de gegevens niet zonder toestemming met anderen delen; we zullen de gegevens zorgvuldig beveiligen. Wij delen geen gegevens met een land of internationale kantoor buiten de Europese Unie.
Gezien de omvang van onze kantoor volstaan wij met het opstellen van dit privacybeleid (waarin begrepen een risico inventarisatie onder paragraaf F) alsook het opstellen van een verwerkingsregister.

Bij het opstellen van dit beleid is gebruik gemaakt van informatie van de Autoriteit Persoonsgegevens:
- Het 10 stappenplan van de Autoriteit persoonsgegevens
- Handleiding Algemene verordening gegevensbescherming

Geraadpleegde literatuur

1. Autoriteit persoonsgegevens, 10 stappenplan (datum onbekend)
2. Autoriteit persoonsgegevens, Handleiding Algemene verordening gegevensbescherming
3. Beleidsregels voor toepassing van artikel 34a van de Wbp (melding datalekken)
4. Ministerie van Veiligheid en Justitie, 10 vuistregels veilig internetten

DATA PROTECTION IMPACT ASSESSMENT, PIA (B)

Wij zullen geen Data Protection Impact Assessment uitvoeren.

Wij zijn van mening dat onze gegevensverwerking geen hoog privacyrisico met zich meebrengt.

Als kantoor houden wij ons niet bezig met:
- Het systematisch en uitvoerig persoonlijke aspecten evalueren;
- Het op grote schaal bijzondere persoonsgegevens verwerken;
- Het op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied.

FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING (C)

Er is geen aparte functionaris voor de gegevensbescherming.

Wij kwalificeren niet als een kantoor zoals benoemd onder paragraaf B.
Wij zijn ons bewust van het beschermen van data. Wij realiseren ons dat data bescherming en het up to date houden hiervan, alsmede voldoen aan de AVG een continue proces is. Hierop zal worden toegezien door de eigenaar.

LEIDENDE TOEZICHTHOUDER (D)

Er is geen leidende toezichthouder.
Ons kantoor kent één vestiging en is niet 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)

In onze omgang met privacy gevoelige informatie, zoals het bewaren en verwerken van (persoons)gegevens en elektronische communicatie, nemen wij een professioneel kritische en alerte houding aan.

Dit doen wij door:
Het risico op een datalek voorkomen en het risico op schadelijke software verkleinen:
- tijdige software updates installeren, waar nodig met de expertise van onze automatiseerder/ software leverancier;
- computers, server en overige hardware blijft ten alle tijden op kantoor. De laptop wordt sporadisch gebruikt voor zakelijke e mails. Daarnaast kan deze gebruikt worden voor werken in de cloud. De toegang tot de laptop wordt beschermd met een sterk wachtwoord.
- periodiek back-ups maken op externe, losgekoppelde, beveiligde gegevensdragers.

De 10 vuistregels van veilig internetten, opgemaakt door het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie. 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

Als kantoor voeren wij onze dienstverlening uit in lijn met de uitgangspunten zoals opgesteld door de Autoriteit Persoonsgegevens: privacy by design en privacy by default.

"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."

VERWERKINGSREGISTER (F)

Data opslag (waar staan data, welke data, bij wie staan ze, wie kan erbij, contracten)

Wij verwerken regelmatig persoonsgegevens.
Als verwerkingsverantwoordelijke hebben wij een verwerkingsregister opgesteld.

In het verwerkingsregister van ons kantoor is de volgende informatie opgenomen:
- de naam en contactgegevens van onze kantoor en de vertegenwoordiger;
- de naam van de (mede)verwerkingsverantwoordelijke
- verwerkingsdoelen
- verwerkingsgrondslag
- van wie worden persoonsgegevens verwerkt
- welke persoonsgegevens worden verwerkt
- of sprake is van bijzondere persoonsgegevens
- met wie persoonsgegevens worden gedeeld;
- beoogde bewaartermijn
- getroffen technische en organisatorische maatregelen.

Een algemene beschrijving van de technische en organisatorische maatregelen die wij hebben genomen om persoonsgegevens te beveiligen is in dit beleid opgenomen (G).

RISICO INVENTARISATIE (G)

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

Organisatorische maatregelen

Ten aanzien van de organisatorische maatregelen is door ons kantoor:
- dit beleid opgesteld
- een privacy- en cookiebeleid opgemaakt welke beschikbaar gesteld is op onze website
- werken wij met (sub)verwerkersovereenkomsten.
- ten aanzien van het gebruik van cloudoplossingen, aanschaf van hard- en software producten hanteren wij de volgende vuistregels:

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 of collega's ervaringen hebben met betreffende partijen en diens producten.

Bedrijfsgebouw
Ons kantoor is verbonden aan een woonhuis waardoor vrijwel permanent toezicht is op het terrein om het kantoor heen. De fysieke beveiliging wordt door ons als goed beschouwd. Het terrein is afgescheiden door een hekwerk welke enkel voor huurders met een zogenoemde druppel en/of sleutel toegankelijk is. Het kantoor wordt iedere avond afgesloten en alle dossiers worden in een brandkast opgeborgen. Buiten kantoortijden heeft alleen de bewoonster van de woning toegang tot de ruimte. De sleutels van de brandkasten liggen op een voor de bewoonster onbekende plek.

Technische maatregelen
Binnen onze kantoor maken wij gebruik van de volgende hardware:

1. ProLiant MicroServer Gen8 (1 ex.) waarin begrepen Hewlett Packard Enterprise RAM geheugen en Microsoft Windows Server 2012 R2 Essentials
2. Werkstation en Laptop
3. Diverse All-in-one Brother printers
4. Wester Digital (WD) Elements portable externe harde schijf (5 ex.)

Binnen onze kantoor is de volgende software geïnstalleerd:
1. Microsoft Office Pakket
2. Op de laptop is geen verbinding met een werkstation mogelijk.

Externe partijen
Er wordt samengewerkt en gebruik gemaakt van het netwerk van Van Hulst Accountancy waarmee wij een samenwerking hebben. Zij hebben als externe automatiseerder Van Oyen Automatisering te Beneden-Leeuwen. Met dit bedrijf is door hen een geheimhoudingsovereenkomst afgesloten. Werkzaamheden door de automatiseerder vinden uitsluitend plaats op ons verzoek en bij voorkeur bij ons op kantoor onder toezicht van één van de eigenaren. In die situatie dat er korte (termijn) vragen zijn over het functioneren van het werkstation wordt het werkstation in de regel op kantoor hersteld.

Hard- en software technische beveiliging
De laptop is beveiligd met een sterk en uniek Windows wachtwoord (minimaal een combinatie van cijfers en letters). Er wordt zorgvuldig (als goed huisvader) omgegaan met de laptop. De laptop valt na twee minuten automatisch in de beveiligde modus.

Op het moment dat laptop vervangen wordt, wordt de 'oude' laptop (voor zover nodig) door de eigenaar of automatiseerder geschoond van zakelijke programmatuur en worden bestanden verwijderd.

Back-up en recovery
Dagelijks vind een roulerende back up plaats van de server op een externe harde schijf. Dit geschiedt automatisch in de loop van de nacht. Hiertoe zijn door de automatiseerder 5 schijven aangemaakt, een schijf per werkdag. Periodiek wordt getest door de eigenaar van Van Hulst Accountancy, dhr. B.A. Poort, dat de backup en recovery procedure werkt. De niet op de server aangesloten schijven worden bewaard in de brandkast op kantoor. De schijven zijn niet uit leesbaar via andere computers, de schijven zijn dan niet zichtbaar. De backup schijven werken enkel na rechtstreeks verbonden te zijn aan onze server.

Mobiele telefoons
Op de mobiele telefoon komt geen zakelijke email binnen. De mobiele telefoons zijn beveiligd met een pincode, touch id en/of gezichtsherkenning. We zijn ons bewust van de telefoonnummers en namen van cliënten en relaties die zich mogelijk op de mobiele telefoons bevinden. We 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 'Find my Phone'.

Data uitwisseling
Voor zover nog gewerkt wordt met (losse) usb sticks wordt de data op deze stick na uitlezing verwijderd van de stick. Er wordt niet gewerkt met een Drop Box. Alleen op verzoek van cliënt wordt gewerkt met Wetransfer om omvangrijke bestanden te kunnen ontvangen of te kunnen verzenden.

Email
Outlook bestanden worden uitsluitend op de server gearchiveerd.

Emailberichten worden 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:

Kantoor is ingeschreven in het handelsregister onder nummer 10038595.
Indien u niet de geadresseerde bent van dit bericht, verzoeken wij u ons dit onmiddellijk per e-mail of telefonisch (0487-591650) te melden en het bericht te vernietigen.

De laptop is voorzien van dezelfde antivirus scanner als op kantoor wordt gebruikt. Genoemd abonnement wordt jaarlijks verlengd geïnitieerd door onze automatiseerder of Kantoor. De geplaatste router is beveiligd met een Firewall.

Wifi netwerk
Er is een Lokaal (eigen) Netwerk aanwezig. De server heeft een beheerdersaccount met een uniek wachtwoord. Er wordt gebruik gemaakt van een ingaande (inbel)verbinding met de server, uitsluitend te gebruiken door de extern automatiseerder.

Er zijn twee eigen wifi netwerken VaHe20C en VaHe20C_NEW. Op verzoek kan een tijdelijk netwerk voor gasten geactiveerd worden. Beide wifi netwerken worden niet gedeeld met derden en zijn beveiligd met een zeer sterk wachtwoord. Het gasten wifi netwerk is bestemd voor derden (lees: cliënten) en wordt enkel op verzoek aan bekende cliënten en/of relaties op kantoor gedeeld. Het gasten netwerk is beveiligd met een wachtwoord.

Het kantoor maakt gebruik van een netwerk waar binnen zich de server, de werkstations en de printers zich bevinden. Deze apparatuur is via kabels onderling verbonden en niet aangesloten op het wifi netwerk.

Website
Er is momenteel geen website en nergens onder beheer.

De domeinnaam www.poortvanhulst.nl is geregistreerd bij Mijndomein.nl

(Cookies, of vergelijkbare technieken, zijn kleine stukjes (tekst)informatie die bij het bezoek van een website worden meegestuurd aan onze browser en vervolgens op uw harde schijf of in het geheugen van uw computer, tablet of mobiele telefoon worden opgeslagen. Voor het verzamelen van gegevens, wordt door Kantoor behoudens voor eigen gebruik Google Analytics, verder geen gebruik gemaakt van tracking cookies. Op de website wordt in ons privacy en cookiebeleid hiervan melding gemaakt.)

Cloudoplossingen
Door ons kantoor wordt gebruik gemaakt van de volgende cloudoplossingen:

1. Innovixion (pakket voor het beheren van de assurantieportefeuille)
2. Findash (pakket voor berekeningen voor financiële planning)

De genoemde cloudoplossingen hebben veiligheidstoepassingen. Uitleg en omschrijvingen hiervan worden gegeven op de website, overeenkomst of naar aanleiding van telefonisch contact. Wij zijn van mening dat alle genoemde partijen afdoende maatregelen hebben genomen om de data van onze cliënten te waarborgen.

Wij hebben regelmatig overleg met genoemde partijen. Inlog maatregelen genomen door genoemde partijen zijn:
- Innovixion: gebruikersnaam en wachtwoord.
- Findash: gebruikersnaam en wachtwoord.

In de bijlagen van dit beleid wordt per aanbieder ingegaan op de beveiligingsmaatregelen die genoemde aanbieder heeft getroffen.

Toestemming en (sub)verwerkersovereenkomsten (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: cliënt is geïnformeerd dat wij zijn persoonsgegevens verwerken (1) ten behoeve van specifiek deze opdracht (2). Wij zijn van mening dat wij deze toestemming van cliënt ontvangen op het moment dat cliënt ons vraagt een opdracht voor hem uit te voeren.

MELDPLICHT DATALEKKEN (I)
Wij maken afwegingen en beslissingen of een gebeurtenis die zich heeft voorgedaan gemeld moet worden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene. 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 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 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 sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident denken wij bij voorbeeld aan het kwijtraken van een USB-stick, diefstal van een laptop of een inbraak door een hacker. Niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uitgesloten kan worden. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. We hoeven 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)
Boven-Leeuwen, 29 oktober 2019

Mw. F.M. van Hulst FFP RPLP

BIJLAGEN (K)
In de bijlagen bij dit 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 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;

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. “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 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 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

Wij zijn van mening dat alle, hieronder genoemde partijen afdoende maatregelen hebben genomen om de data van onze cliënten te waarborgen:

1. Innovixion
2. Solverium / Findash