Notitie Privacy-beleid LDE Accountants B.V.
- Gegevensbescherming, Cybercriminaliteit, Meldplicht Datalekken -

Inhoudsopgave:

Bewustwording (A)

Tijdens de uitvoering van onze werkzaamheden communiceren wij elektronisch met onze cliënten en relaties. Hierin is tevens begrepen de uitwisseling van persoonsgegevens met hen zowel als onderling, 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 privacy-beleid op te stellen. Daar wij van mening zijn dat het verplicht opstellen van een privacy-beleid (ook wel gegevensbeschermingsbeleid) niet in verhouding staat tot de door ons verrichte verwerkingsactiviteiten. Mede ingegeven door de beperkte omvang van onze verwerking van persoonsgegevens (enkel het voeren van salarisadministratie door Kees en Mark, het voeren van financiële administratie door Jolanda, Mirjam en Mitchell en tenslotte het opstellen van berekeningen van pensioen in eigen beheer door Eric) 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 bewerkingen altijd plaats vinden onder eindverantwoordelijkheid van onze opdrachtgever.

Wij zijn als kantoor wel van mening dat het nuttig is om richtlijnen voor privacy-beleid op te stellen. Hiermee trachten wij privacy-risico's van verwerkingen van persoonsgegevens binnen ons kantoor inzichtelijk te maken met het oog op 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 deze notitie privacy-beleid zal aandacht besteed worden aan 'the internet of things' binnen ons kantoor, de voor ons kantoor van toepassing zijnde soft- en hardware en de leveranciers van onze cloud-oplossingen.

Met deze notitie voldoen wij tevens aan onze verantwoordingsplicht (accountability) en trachten wij een 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 de verwerking voldoet aan de voorwaarden van 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/of 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 privacy-beleid 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 kantoor buiten de Europese Unie. Wij gebruiken de gegevens alleen voor de afgesproken doelen en zullen de gegevens niet zonder toestemming met anderen delen tenzij de Nederlandse wet of regelgeving ons daartoe verplicht en zullen de gegevens 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 bijeenkomsten bijgewoond:

Geraadpleegde literatuur

1. NBA, Datalekken in de MKB praktijk
2. NBA, model (sub-)bewerkersovereenkomst d.d. 16 april 2018
3. NBA NEMACC, brochure privacybescherming d.d. 15 mei 2018
4. Autoriteit persoonsgegevens, website d.d. 10 mei 2018
5. Autoriteit persoonsgegevens, 10 stappenplan d.d. 15 mei 2018
6. Beleidsregels voor toepassing van artikel 34a van de Wbp (melding datalekken)
7. Ministerie van Veiligheid en Justitie, 10 vuistregels veilig internetten

Bijeenkomsten / trainingen

1. Libra Service, infosessie AVG, 29 januari 2018
2. Auxilium, bijeenkomst

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. Dit 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 privacy-beleid (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.

Leidende toezichthouder (D)

Er is voor ons geen sprake van een leidende toezichthouder. Daar ons kantoor maar één vestiging kent en niet is aangesloten bij een internationaal opererend kantoor en/of netwerk. Onze gegevensverwerking heeft ook geen impact op meerdere lidstaten binnen de Europese Unie. Tenzij de Nederlandse wet of regelgeving anders verplicht, worden door ons geen gegevens gedeeld met een land of kantoor buiten de Europese Unie.

Privacy by design & privacy by default (E)

Als kantoor streven wij er naar onze dienstverlening uit te voeren 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 van de Autoriteit Persoonsgegevens:

- Privacy by design houdt in dat wij er al bij het ontwerpen van producten en diensten voor zorgen dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat niet meer gegevens verzameld worden dan noodzakelijk voor het doel van de verwerking en dat deze gegevens niet langer bewaard worden dan nodig.
- Privacy by default houdt in dat technische en organisatorische maatregelen genomen gaan 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 zullen wij een professioneel kritische

en alerte houding aannemen. 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:

- tijdig software updates te (laten) installeren en gebruik te maken van de expertise van onze cloud-leverancier / automatiseerders / software leverancier;
- geen verouderde protocollen te gebruiken;
- computernetwerken en systemen te scheiden, het netwerk blijft ten alle tijden op kantoor van onze cloud-leverancier, inlog is alleen mogelijk met een wachtwoord, laptops worden indien op locatie gebruikt enkel tijdelijk buiten de kantooromgeving gehouden;
- wij periodiek back-ups laten maken op fysiek gescheiden systemen.

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 hieraan invulling gegeven. Daartoe:

A. zijn antivirus programma's geïnstalleerd
B. worden software updates uitgevoerd wanneer deze beschikbaar komen
C. worden er 'sterke' wachtwoorden gehanteerd
D. wordt er op kantoor een eigen wifi netwerk gebruikt voor de laptops en wordt er buiten kantoor gebruik gemaakt van wifi-netwerken van de cliënt of van de bedrijfstelefoon als Wifi toegangspunt;
E. worden geen email berichten en onbekende bestanden geopend die wij niet vertrouwen
F. worden alleen programma's van bekende, officiële partijen gebruikt
G. webadressen (URL's) worden gecontroleerd om vast te stellen of er sprake is van een nagemaakte of onveilige website
H. niet vertrouwde pop-ups worden in de browser niet geopend en waar nodig afgesloten met Alt+F4
I. denken wij na over te delen informatie op het internet (waaronder in ieder geval wordt verstaan onze website en sociale netwerksites)
J. gebruiken wij 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 degenen van wie wij de persoonsgegevens verwerken;
- waarvan de verwerking niet incidenteel is;
- die vallen onder de categorie bijzondere persoonsgegevens.

Wij verwerken in opdracht van een verantwoordelijke persoonsgegevens. De verwerking ziet op het verwerken van de salarisadministratie, de financiële administratie en het opmaken van pensioenberekeningen in eigen beheer.

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 (salaris-, financiële-administratie 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 (kopie identiteitsbewijzen, BSN, NAW-gegevens, geboortedatum, emailadressen, telefoonnummers);
- met wie wij deze gegevens delen.

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 opdracht gegeven tot het op onze website opnemen van privacy- en cookiebeleid 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 als dat mogelijk is in een demo (test)omgeving.
Tevens informeren wij binnen ons netwerk (collega accountants en/of cliënten en relaties) of zij ervaringen hebben met de betreffende partijen en hun producten. Deze testwerkzaamheden worden als dat haalbaar is vroegtijdig en buiten de drukste periodes in voor en najaar 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.

Ons kantoor is gevestigd in een eigen pand. Slechts de kantine wordt gedeeld met een onderhuurder. De fysieke beveiliging van onze kantoorruimte wordt door ons als goed beschouwd door het gekozen sleutelsysteem dat het mogelijk maakt (en ook zo is uitgevoerd) dat sleutels van de compagnons meer mogelijkheden hebben dan de sleutels van de medewerkers). Daarnaast is de eigen dossierruimte beveiligd met een toegangscode zodat slechts de compagnons daar toegang toe hebben.

Technische maatregelen

Binnen ons kantoor maken wij gebruik van desktop-computers zowel als laptops die dienen ter inlog op ons cloud-omgeving. Deze PC's zijn voorzien van Windows-10 software en maken gebruik van de daarin ingebouwde beveiligingsmaatregelen en -software (Defender).
Deze computers worden niet gebruikt voor locale bestandsopslag.

Er is een uitzondering: de PC van Timo. Dit omdat er een aantal klanten oude (boekhoud-) software gebruikt die niet compatibel is met onze server-software in de cloud-omgeving. Deze klanten weigeren om over te stappen naar een nieuwe(re) versies van hun programmatuur. Timo's PC is daarom beveiligd met een wachtwoord.
Voor de overige computers is daarvoor niet gekozen, omdat dit het door ons voorgestane flexwerken onmogelijk zou maken.

Externe partijen

Als cloud-leverancier en externe automatiseerder treedt op Global-E te Gilze, met hen is een (sub-)verwerkersovereenkomst met geheimhoudingsclausule afgesloten. Werkzaamheden door de automatiseerder vinden doorlopend plaats om een goede werking van ons systeem te garanderen.

Hard- en software technische beveiliging

Aangewezen computers zijn beveiligd met een wachtwoord. Ook de inlog via een remote desktop op ons systeem in de cloud, is met een wachtwoord beveiligd. Deze wachtwoorden moeten unieke en sterke wachtwoorden zijn (minimaal een combinatie van cijfers en letters).
Het beleid is dat er lokaal geen data van cliënten opgeslagen wordt. Periodiek moeten de map 'downloads' alsook de 'prullenbak' leeggemaakt worden. Er wordt zorgvuldig (als goed huisvader) omgegaan met de computers, deze mogen niet 'alleen' gelaten worden. Als er op gedurende een periode van 15 minuten geen activiteit wordt waargenomen van ingelogde medewerkers, wordt de sessie automatisch afgesloten.

Er mag géén privé software/ programmatuur geplaatst worden op onze zakelijke computers.

Indien op locatie wordt gewerkt waarin inloggen in de cloud niet mogelijk is, worden enkel de benodigde documenten lokaal op een laptop gezet welke direct na uitvoering van de werkzaamheden op kantoor weer teruggeplaatst worden op ons beveiligde systeem.

Op het moment dat computers vervangen worden, dan worden de 'oude' computers geschoond van zakelijke programmatuur en worden de bestanden verwijderd (c.q. wordt de harde schijf vernietigd).

Back-up en recovery

Continue en automatisch vindt er back up op plaats op en van het systeem. Hierover zijn afspraken gemaakt met de cloud-leverancier. Voor zover daarop een beroep moest worden gedaan, waren de back-ups ook steeds beschikbaar.

Mobiele telefoons

Op de door ons verstrekte mobiele telefoons komt zakelijke email binnen en ook collega's die gebruik maken van een eigen mobiele telefoon, ontvangen veelal hun zakelijke mail op die telefoon.

De door kantoor verstrekte mobiele telefoons zijn beveiligd met een pincode en touch id. De gebruikers daarvan zijn zich bewust van de e-mails, de telefoonnummers en namen van cliënten en relaties die zich op de mobiele telefoons bevinden. Zij gaan als een goed huisvader om met de mobiele telefoons.

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

Data uitwisseling

Er zijn geen onbeveiligde usb sticks, er wordt niet gewerkt met DropBox, WeTransfer of vergelijkbare diensten om data naar onze cliënten te verzenden.

Indien grote bestanden uitgewisseld dienen te worden dan zal dit bij voorkeur plaatsvinden via ons beveiligde Portaal. Dit portaal is door middel van een login en wachtwoord beveiligd.

Email

De outlook bestanden worden meegenomen in de beveiliging via onze cloud-leveracier en staan niet "los" op onze computers.
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 elke uitgaande kantoor-email opgenomen zijn:

"Indien u niet de geadresseerde bent van dit bericht, verzoeken wij u ons dit onmiddellijk per e-mail of telefonisch te melden en dit bericht te vernietigen".
Ons cloud-systeem is voorzien van de nodige beveiliging.

Wifi netwerk
Er is een wifi netwerk aanwezig, dit netwerk is beveiligd met een wachtwoord en kan door personeelsleden en gasten gebruikt worden om in te loggen op het internet. Het wachtwoord wordt -enkel op verzoek- aan bekende cliënten en/of relaties op kantoor gedeeld.
Het wifi netwerk maakt gebruik van een Ziggo internetverbinding en opereert daarmee volstrekt gescheiden van de verbinding met onze cloud bij Global-E.

Website
De domeinnaam www.LDEaccountants.nl is geregistreerd bij Global-e ICT solutions B.V. te Gilze. De website is onder beheer van Ibou B.V. te Oisterwijk en de zoekmachine-optimalisatie wordt verzorgd door Grizzly New Marketing B.V.

De domeinnaam is beveiligd met een SSL certificaat welke jaarlijks zal wordt verlengd na authenticatie door Global-E.

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 anders dan door door Grizzly New Marketing B.V. voor analytisch gebruik op enkele speciaal daarvoor opgemaakte paginas, geen gebruik gemaakt van tracking cookies.

Global-E
Global-E te Gilze verzorgt onze cloud (remote desktop en virtuele servers), het applicatiebeheer en zal binnenkort en (binnenkort) een deel van onze internetverbingen als ze ook een van onze ISP's zullen worden. Door Global-E zijn de volgende beveiligingsmaatregelen getroffen:

Ibou B.V.
Het beheer van de website vindt plaats door Ibou te Oisterwijk.

Grizzly New Marketing B.V.

Website-optimalisatie door Grizzly New Marketing B.V.
Zij passen op door hen geoptimaliseerde web-paginas cookies toe voor analytische doeleinden.

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

1. Nmbrs, online loonadministratie
2. Elvy, scan en herkenfaciliteit
3. KBP aangiftesoftware, fiscale aangiften (inkomsten- en vennootschapsbelasting)
4. Nextens, aangiften omzetbelasting
5. Afas (Pocket), database en urenregistratie

De genoemde cloudoplossingen hebben veiligheidstoepassingen, uitleg en omschrijvingen ontleend aan de website van de betreffende partij, zie hiertoe de bijlage. Wij zijn van mening dat alle genoemde partijen afdoende maatregelen hebben genomen om de data van onze cliënten te waarborgen. Wij hebben waar nodig ook overleg met genoemde partijen.

Inlogmaatregelen reeds genomen door genoemde partijen zijn:

- Nmbrs, gebruikersnaam en wachtwoord.
- Elvy, gebruikersnaam en wachtwoord.
- KBP aangiftesoftware, gebruikersnaam en wachtwoord.
  Two factor authentication (sms) wordt aan gewerkt.
- Nextens aangiftesoftware, gebruikersnaam en wachtwoord.
  De functionaliteit inlog bij sms wordt nog niet ondersteund doch is voorgelegd aan de uitgever en het ontwikkelteam
- Afas (Pocket), gebruikersnaam en wachtwoord (vingerafdruk via telefoon).

In de bijlagen van deze notitie wordt per bovenstaande, genoemde aanbieder ingegaan op de beveiligingsmaatregelen die genoemde aanbieder heeft getroffen.

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 wij kunnen bewijzen dat we 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 en die zijn aangepast aan onze situatie.

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.

BIJLAGEN (K)

In de bijlagen bij deze notitie privacy-beleid 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;
- 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

Onderstaande cloudoplossingen hebben de navolgende veiligheidstoepassingen, uitleg en omschrijvingen ontleend aan de website van de betreffende partij en/of als schriftelijke toelichting ontvangen naar aanleiding van gevoerd overleg. Wij zijn van mening dat alle, genoemde partijen afdoende maatregelen hebben genomen om de data van onze cliënten te waarborgen.

1. NMBRS, online loonadministratie
2. Elvy, scan en herkenfaciliteit
3. KBP, fiscale aangiften (inkomsten- en vennootschapsbelasting)
4. Nextens, fiscale aangiften (omzetbelasting)
5. Afas (Pocket App), database en urenregistratie

Ad 1. NMBRS

Wij waarborgen privacy

Nmbrs® zal persoonsgegevens nooit voor andere doeleinden dan HR- en payroll-gerelateerde toepassingen gebruiken. Bovendien doen wij er alles aan om te zorgen dat niemand anders dat met onze data zou kunnen doen. Alle klantgegevens die opslag behoeven, bevinden zich in het Equinix datacenter met de hoogste niveaus van beveiliging en operationele betrouwbaarheid. Het delen van gegevens met toepassingen of tools die ons product verbeteren, gebeurt in overeenstemming met de EU Data Protection Act. Dit houdt in dat de gedeelde informatie zeer beperkt is en geen gevoelige data overdraagt.

Hoe beschermen wij klantgegevens?

Ons beleid streeft zowel veiligheid als gebruiksgemak voor onze klanten na. We gebruiken verschillende tools voor die ons team waarschuwen tijdens kritieke situaties binnen de infrastructuur van onze applicatie. Daarnaast bieden wij onze klanten opties om de veiligheid van hun account te verhogen. De Nmbrs® IT-whitepaper biedt een volledig overzicht van deze inspanningen en beleidsmaatregelen die ons helpen bij het beveiligen van klantgegevens.

Infrastructuur

Het dataverkeer naar onze servers wordt 24 uur per dag gecontroleerd vanuit een centrale controlekamer. Binnen 30 minuten zal Nmbrs® reageren op pogingen tot inbreuk, ander onregelmatig verkeer of pogingen om Nmbrs® te onderbreken. De infrastructuur van

Nmbrs® wordt beveiligd door een Firewall in beheer van hosting partners die het verkeer scannen om mogelijke bedreigingen te identificeren. Bovendien wordt elke server die via internet toegankelijk is (webservers) beschermd door een extra Firewall voor het besturingssysteem.

SSL Encryptie

De client / Server communicatie is uitgevoerd met HTTPS, wat de integriteit van gegevens garandeert en datamanipulatie voorkomt. Het Nmbrs® certificaat maakt gebruik van een 2048 bit encryptie. De HTTPS transportlagen gebruiken een standaard TLS zonder terugval naar SSLv2 / SSlv3, die door veiligheidsredenen zijn uitgeschakeld. Internetgebruikers herkennen de beveiligde SSL-status aan het vergrendelingspictogram voor de adresbalk en beveiligde websites met uitgebreide validatie aan de groene adresbalk.

Gebruikersverificatie

Nmbrs® slaat geen originele gebruikerswachtwoorden op in de database. In plaats daarvan slaan wij een *salted hash* van het wachtwoord op, wat betekent dat zelfs toegang tot de database nog geen inzicht in de wachtwoorden verleent. Qua wachtwoordbeleid kunnen klanten zowel periodieke wachtwoord resets als het gebruik van pincodes aansturen, en biedt two-factor verificatie mogelijkheid tot een tweede verificatieniveau voor het Nmbrs®-account.

IP Validatie

Elke gebruiker heeft een whitelist met goedgekeurde IP-adressen om toegang te krijgen tot het systeem. Wanneer gebruikers toegang krijgen tot het systeem vanuit een nieuw IP-adres, wordt een e-mail verzonden om deze te verifiëren. Het is ook mogelijk om de toegang tot Nmbrs® accounts te beperken tot een voorgedefinieerde lijst met IP-adressen of IP-bereik. Dit beleid voorkomt inbreuk op Nmbrs® accounts vanuit onbekende locaties of apparaten.

Wie verifieert onze kwaliteit?

Wij vertrouwen op externe partijen om onze operationele kwaliteit, procedures en methodieken te verifiëren. Nmbrs® handhaaft een reeks certificaties die een onafhankelijk deze controle op onze kwaliteit vormen.

ISAE 3402 Type II

Het doel van dit ISAE 3402 Type II rapport is onder andere om de klanten te voorzien van antwoord op de vraag hoe Nmbrs® als service organisatie processen beheerst; hoe wij omgaan met risicomanagement, informatiebeveiliging en anti-fraude. Processen die uitgevoerd worden door een serviceorganisatie hebben namelijk vaak invloed op

financiële en operationele processen die effect hebben op de jaarrekening van de gebruikersorganisatie.

Ad 2. Elvy

Elvy neemt passende technische en organisatorische maatregelen om de persoonsgegevens van de klant te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen worden aangemerkt als een passend beveiligingsniveau in de zin van de AVG.
De klant is gerechtigd om in overleg met Elvy tijdens de looptijd van de overeenkomst door een onafhankelijke deskundige de naleving hiervan te controleren, bijvoorbeeld door middel van het uitvoeren van een audit.
Elvy zal, indien een verzoek gedaan wordt door de Stichting Autoriteit Financiële Markten, De Europese Centrale Bank of De Nederlandsche Bank N.V., op grond van de uitvoering van hun taak uit hoofde van de Wft, of op grond van andere wet- en regelgeving, alle informatie beschikbaar stellen aan de betreffende organisatie.
De datacenters waar de servers van Elvy Online gehuisvest zijn, bevinden zich uitsluitend in Nederland (Rotterdam). De datacenters vallen onder Nederlandse wet- en regelgeving en voldoen aan de strenge Nederlandse en Europese wetgeving met betrekking tot logische en fysieke toegangsbeveiliging en continuïteit. De datacenters zijn ISO 27001 gecertificeerd.
Elvy heeft gekozen voor datacenters van I3D.net en deze is hiermee subverwerker van de klantdata. Persoonsgegevens worden door Elvy en subverwerker uitsluitend verwerkt binnen de Europese Economische ruimte.

Ad 3. KBP aangiftesoftware, (inkomsten- en vennootschaps-belasting)

KBP aangiftesoftware is onderdeel van Kluwer.

Wolters Kluwer garandeert dat uw KBP-inloggegevens en -data optimaal beveiligd zijn. Alle gegevens worden opgeslagen op de Wolters Kluwer-server in de Europese datacenters en er worden automatisch backups gemaakt in onze zeer veilige private cloud.

Ad 4. Nextens

Nextens is onderdeel van Reed Business Information.

Nextens draait op het Microsoft Azure-platform in Nederland. De servers van dit platform maken altijd een kopie op servers op een andere locatie binnen Europa. Het platform voldoet aan alle veiligheidskeurmerken en verzekert u van een veilige opslag van uw klantgegevens

Windows Azure wordt uitgevoerd in datacenters die door Microsoft Global Foundation Services (GFS) worden beheerd en geëxploiteerd. Deze geografisch verspreide datacenters voldoen aan de belangrijkste industrienormen voor beveiliging en betrouwbaarheid, zoals ISO/IEC 27001:2005. Ze worden beheerd en bewaakt door Microsoft-personeel dat een jarenlange ervaring heeft met het 24 uur per dag, zeven dagen per week leveren van de grootste online services ter wereld.

Het datacenter van Microsoft wat wij gebruiken staat in Amsterdam en heeft:
- Fysieke beveiliging
- Bescherming tegen DDOS aanvallen
- Uitwijkmogelijkheden

Naast het beveiligingsbeleid voor datacenters, netwerken en personeel gelden er voor Windows Azure diverse beveiligingsregels op de toepassings- en platformniveaus voor een nog uitgebreidere beveiliging voor ontwikkelaars van toepassingen en servicebeheerders.
Een totaaloverzicht van de beveiligingen op het Azure platform vind je op http://www.windowsazure.com/nl-nl/support/trust-center/

Ad 5. Afas (Pocket App)

Altijd werken met de meest recente versie

Je gebruikt de software van AFAS via de cloud. Wij verzorgen het systeembeheer, een optimale beveiliging en een dagelijkse back-up. Je bent en blijft zelf eigenaar van de data. De beveiliging van jouw gegevens is voor ons absolute prioriteit. Beveiliging is van toepassing op zowel het fysieke datacentrum, de dataverbinding als gegevensbeheer.

Doordat je werkt met AFAS Online worden cao-updates, nieuwe versies, patches en wettelijke wijzigingen automatisch voor je geïnstalleerd.

Twee-factor-authenticatie

Vanaf medio mei 2018 zal AFAS gefaseerd verplichte twee-factor-authenticatie uitleveren. Dit betekent dat je bij het inloggen, naast je gebruikersnaam en wachtwoord, een extra stuk informatie moet toevoegen die alleen voor jou als gebruiker beschikbaar is. Je bevestigt je aanmelding via de AFAS Pocket App of een SMS. Eventueel misbruik van je gegevens wordt hierdoor vele malen moeilijker gemaakt.