Notitie privacybeleid

HD Accountants B.V.

A. Bewustwording

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

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

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).

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

De persoonsgegevens die door ons worden verkregen, opgeslagen en indien nodig worden bewerkt, vloeien voornamelijk voort uit onze accountancy- en/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 privacybeleid en het verwerkingsregister zal, waar van toepassing een omschrijving gegeven worden van de categorieën persoonsgegevens die wij verwerken. Hierbij is onze verplichting om niet meer persoonsgegevens te verwerken dan noodzakelijk wordt geacht om ons beroep te kunnen uitvoeren en onze diensten te kunnen verrichten. Persoonsgegevens worden daarnaast niet langer dan noodzakelijk voor onze beroepsgroep bewaard.

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

B. Data Protection Impact Assessment

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

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

Gezien de omvang van onze kantoor volstaan wij met het opstellen van een notitie privacybeleid alsook het opstellen van een verwerkingsregister.

C. Functionaris voor de gegevensbescherming

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.

D. Leidende toezichthouder

Er is geen sprake van een leidende toezichthouder. Daar onze kantoor maar één vestiging kent en tevens niet is aangesloten bij een internationaal, opererend kantoor en/of netwerk. Onze gegevensverwerking heeft ook geen impact op meerdere lidstaten binnen

de Europese Unie. Door ons worden geen gegevens gedeeld met een land of internationale kantoor buiten de Europese Unie.

E. 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 alleen 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.

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:

1. Antivirus programma’s zijn geïnstalleerd.
2. Software updates worden uitgevoerd wanneer deze beschikbaar komen.
3. Er worden ‘sterke’ wachtwoorden gehanteerd.
4. Er is alleen verbinding met vertrouwde wifi netwerken.
5. Er worden geen e-mailberichten en onbekende bestanden geopend die wij niet vertrouwen en/of waarvan wij de afzender niet kennen.
6. Er worden alleen apps en programma’s van bekende, officiële partijen gebruikt.
7. Webadressen worden altijd gecontroleerd om vast te stellen of er sprake is van een nagemaakte of onveilige website.
8. Pop-ups worden in de browser niet geopend en waar nodig afgesloten.
9. Wij denken goed na over te delen informatie op het internet (waaronder in ieder geval wordt verstaan onze website en sociale netwerksites).
10. Wij gebruiken ons gezond verstand, iets wat te mooi lijkt om waar te zijn, is dat meestal ook.

F. Verwerkingsregister

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.

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 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.

G. Risico inventarisatie

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

Organisatorische maatregelen

a. Het kantoor is voorzien van deugdelijke sloten en te allen tijde afgesloten.

b. Kantoorbezoek is alleen mogelijk op afspraak. Het kantoor is niet vrij toegankelijk.

c. Het archief is alleen toegankelijk voor werknemers binnen het kantoor.

d. De serverruimte is alleen toegankelijk na binnentreding kantoor.

e. Binnen het kantoor zijn werknemers bewust van beveiliging en privacy. Er worden geen e-mailberichten en onbekende bestanden geopend die wij niet vertrouwen en/of waarvan wij de afzender niet kennen. Wij denken goed na over te delen informatie op het internet (waaronder in ieder geval wordt verstaan onze website en sociale netwerksites). Wij gebruiken ons gezond verstand, iets wat te mooi lijkt om waar te zijn, is dat meestal ook.

Technische maatregelen

Toegangsbeveiliging

a. De harde schijven in de serverruimte en draagbare apparaten zijn gecodeerd door middel van Bitlocker, waardoor bij vervreemding van de harde schijven de data onleesbaar zijn.

b. De toegang tot de beheerdersfunctie van de server is door de externe systeembeheerder beveiligd door middel van twee-staps-verificatie.

c. De toegang tot gebruikers zijn beveiligd met een combinatie van gebruikersnaam en wachtwoord. Deze wachtwoord is persoonsgebonden en moet voldoen aan bepaalde eisen, zoals lengte, hoofdletters en speciale tekens. Tevens moet het wachtwoord per kwartaal worden gewijzigd.

d. De externe toegang tot het netwerk en server is beveiligd met twee-staps-verificatie.

e. De verbinding naar de server wordt versleuteld met Secure Sockets Layer (SSL).

f. De Thin Clients worden gebruikt om verbinding te maken met extern bureaublad. De Thin Clients zijn geconfigureerd als stand alone, dat betekent dat de Thin Clients alleen toegang hebben tot het lokale netwerk.

g. De afdeling personeelszaken meldt vroegtijdig uitdiensttreding van werknemers aan de externe systeembeheerder om de toegang op de dag na vertrek te blokkeren.

h. Het scherm wordt bij extern gebruik na een halfuur vergrendeld.

Virusbeveiliging

a. De server is voorzien van antivirussoftware die real-time wordt bijgewerkt naar de nieuwste virusdefinities.

b. De besturingssysteem van de server wordt door de externe systeembeheerder periodiek bijgewerkt. De gebruikte besturingssysteem Windows Server 2008 R2 wordt tot 2020 voorzien van beveiligupdates.

c. De programma's op de server wordt periodiek door de externe serverbeheerder bijgewerkt naar de laatste versie. Niet gebruikte programma's worden na overleg verwijderd door de externe systeembeheerder.

d. Het gebruikt van randapparatuur als usb-sticks zijn geblokkeerd.

e. Binnengekomen e-mailberichten worden gescand op ongewenste berichten en virussen.

Data-uitwisseling

a. Het e-mailverkeer tussen mailservers is versleuteld met behulp van STARTTLS.

Externe diensten

a. E-mailaccountants zijn alleen op het interne netwerk ingesteld. De enige uitzondering op de regel is de directeur. Deze ontvangt op zijn smartphone ook de e-mailberichten. Bij vervreemding kan op afstand de smartphone worden gewist.

b. Externe diensten voor verwerking van salarisadministratie, belastingaangiftes en online administraties zijn beveiligd met een combinatie van gebruikersnaam en wachtwoord. Daarnaast wordt er gebruik gemaakt van twee-staps-verificatie waar nodig.

Dataverzameling door derden

a. De dataverzamelingsfuncties van derden zijn waar nodig uitgeschakeld. In het besturingssysteem zijn telemetrie services uitgeschakeld. In Microsoft Office hebben is de optie om te helpen met het verbeteren van de producten uitgeschakeld.

b. Binnen het kantoor wordt hoofdzakelijk gebruik gemaakt van de privacyvriendelijke webbrowser Firefox. Bij compatibiliteitsproblemen wordt er uitgeweken naar Internet Explorer.

c. In de webbrowser worden cookies van derden geweigerd en de browsergeschiedenis na een week verwijderd om tracking te voorkomen. Daarnaast is de functie ‘bescherming tegen volgen’ binnen Firefox ingeschakeld, waarbij trackingcookies worden geblokkeerd en een ‘Niet volgen’-signaal wordt verstuurd.

Back-up en recovery

a. Dagelijks wordt er een back-up gemaakt. Deze zijn opgeslagen op het NAS-systeem in de serverruimte en deels in de Cloud.

- Terminal servers: alleen NAS
- APP’s: NAS en Cloud
- Data schijf: NAS en Cloud
- E-mail: NAS
  SQL (Allure) NAS

NAS: dagelijks en 26 weken terug te zetten
Cloud: een maand

Cloudoplossingen

Door ons kantoor wordt gebruik gemaakt van de volgende cloudoplossingen:

1. SnelStart, online boekhouden
2. Nextens, fiscale aangiften (inkomsten- en vennootschapsbelasting)

De genoemde cloudoplossingen hebben veiligheidstoepassingen, uitleg en omschrijvingen ontleend aan de website of naar aanleiding van telefonisch contact met 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.

H. Toestemming en (sub)bewerkersovereenkomsten

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

I. Meldplicht datalekken

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.

J. Ondertekening

1 juni 2018 Harold Keuter directeur

Bijlage: Cloudoplossingen

Ad 1 SnelStart bij online boekhouding

Het is SnelStart er alles aangelegen om er zeker van te zijn dat de klantdata veilig is. Zij voldoen aan de strenge eisen, zoals vastgelegd in de internationale norm van de ISO 27000 serie. Het voldoen aan deze norm wordt internationaal gezien als garantie voor veiligheid. Daarnaast maken zij gebruik van de laatste stand van de techniek en worden er 24/7 actieve detectie controles op alle vormen van bedreiging uitgevoerd.

SnelStart maakt gebruik van "industrie standard protocollen" om verbinding te maken met haar dienstenplatform. Naast integriteit en snelheid biedt dit tevens de gelegenheid om in te haken met adequate transportbeveiliging om privacy van het netwerkverkeer te borgen.

De applicaties van SnelStart worden vanuit Nederland gehost. De wet bescherming persoonsgegevens wordt onverkort nageleefd.

SnelStart garandeert voor klantdata een beschikbaarheid van 99,9%. Randvoorwaarde is wel dat verplichtingen van de klant jegens SnelStart worden nagekomen, zoals het tijdig voldoen van de financiële verplichtingen.

De beschikbaarheid wordt 24/7 gemonitord. Bij iedere afwijking die geconstateerd wordt gaat er automatisch een bericht naar een van onze DEVOPS-teams. Deze teams hebben 24/7 specialisten beschikbaar om aan eventuele problemen het hoofd te bieden.

De specialisten kunnen besluiten om een uitwijklocatie in gebruik te nemen mocht dat noodzakelijk zijn. Hierbij wordt primair de impact voor klanten in het oog gehouden ten einde deze zo beperkt mogelijk te houden.

Microsoft is verantwoordelijk voor de veilige opslag van de aangeleverde klantdata binnen de Microsoft architectuur. Deze zelfde verantwoordelijkheid geldt voor de desktop applicaties en services binnen de SnelStart IT-infrastructuur. Daarnaast zorgt SnelStart voor een veilige (TLS) verbinding tussen SnelStart en Microsoft.

Ad 2 Nextens, onderdeel van Reed Business Information

De data van Elsevier Nextens wordt versleuteld opgeslagen op de servers van het Microsoft Azure Platform. De cloud-omgeving is ISO/IEC 27001:2005-gecertificeerd. Deze certificering is een informatie veiligheidsstandaard gepubliceerd door International Organization for Standardization (ISO) en International Electrotechnical Commission (IEC). IEC is met 110 jaar de oudste kantoor van de twee. IEC richt zich voornamelijk op alle internationale normen voor alle elektrische, elektronische en aanverwante technologieën.

De programma's en gegevens van Nextens draaien op het Azure-platform van Microsoft. Deze voldoen aan de veiligheidskeurmerken. Voor Microsoft is de beveiliging de hoogste prioriteit. Uw programma's staan dus niet op uw computer, maar op een server, in Nederland, met back-up in Europa (Ierland). De cloudserver is een digitale opslagplaats. U en andere gebruikers loggen in via internet. Zowel Microsoft als Nextens kunnen uw data niet lezen doordat deze geanonimiseerd zijn volgens de Wet bescherming Persoonsgegevens. Alleen met uw persoonlijke inlog heeft u de sleutel om uw data te lezen.

Reed Business Information zal de data die door of namens u in de Applicatie worden verwerkt en opgeslagen strikt vertrouwelijk behandelen (overeenkomstig artikel 12 Wet bescherming persoonsgegevens), deze uitsluitend gebruiken voor zover noodzakelijk voor het uitvoeren van de overeenkomst, deze uitsluitend verwerken ten behoeve van u en deze niet aan derden verstrekken behalve in het geval van een gerechtelijk bevel of op uitdrukkelijk schriftelijk verzoek van een toezichthouder. De persoonsgegevens die door of namens u in de Applicatie worden verwerkt en opgeslagen zullen door Reed Business Information in overeenstemming met de Wet bescherming persoonsgegevens worden behandeld. De persoonsgegevens worden binnen de EU opgeslagen. In geval van een inbreuk op de beveiligingsmaatregelen, geïmplementeerd in de Applicatie, zal Reed Business Information u hierover informeren.