PRIVACYBELEID ROOTH

1. Inleiding

Rooth hecht grote waarde aan de bescherming van de persoonsgegevens van haar klanten, personeel en andere relaties. Persoonlijke gegevens worden door Rooth dan ook met de grootst mogelijke zorgvuldigheid behandeld en beveiligd. Rooth houdt zich dan ook in alle gevallen aan de eisen die de Algemene Verordening Gegevensbescherming (afgekort: 'AVG') stelt.

In dit privacy beleid staat beschreven hoe Rooth persoonsgegevens en gegevensbestanden registreert, verwerkt, beschermd en bewaart. Ook de gerelateerde onderwerpen, zoals het raadplegen, muteren, uitwisselen en verstrekken van gegevens staat in dit beleid beschreven. Het privacy beleid omvat alle on-en offline systemen waarin persoonsgegevens voorkomen en is van toepassing op alle organisatieonderdelen.

1.1 Vereisten verwerking persoonsgegevens

De AGV stelt eisen aan organisaties die gegevensbestanden beheren, zoals een personeelsadministratie. Deze eisen zijn:

- Toestemming van de medewerker voor het verwerken van de gegevens;
- Juist en nauwkeurig bijhouden van deze gegevens;
- Beveiligen van deze gegevens;
- Op verzoek inzage verlenen in de eigen opgeslagen persoonsgegevens;
- Uitsluitend gebruik van de persoonsgegevens voor het doel waarvoor ze verzameld zijn.

Conform de AGV is het Rooth toegestaan persoonsgegevens te verwerken; categorie Bijzondere persoonsgegevens 'Burgerservicenummer'.

1.2 Aanvullende vereisten

Rooth stelt met dit privacy beleid, naast de wettelijke vereisten, ook een aantal aanvullende richtlijnen vast voor het verwerken van persoonsgegevens. Het beleid bevat ook aandachtspunten voor medewerkers, gebruikers, beheerders en ontwerpers van systemen om niet alleen nu, maar ook in de toekomst de privacy te waarborgen.

1.3 Systemen

Rooth verwerkt persoonsgegevens in de volgende systemen. De systemen worden gehost op internetservers van Rooth in uitsluitend Nederlandse datacenters. Al onze programmatuur staat op een server en deze server staat geïnstalleerd op onze Cloudserver.
Prima IT ondersteunt ons op het gebied van de ICT. Zij kunnen de functionaliteit van de programma's controleren en herstellen waar nodig. Echter hebben zij geen inloggegevens van de applicaties.

1.3.1 ItsClean

ItsClean, dit is de administratieve applicatie van Rooth en wordt gebruikt door alle kantoormedewerkers van de organisatie. In diverse onderdelen binnen deze applicatie worden persoonsgegevens gekoppeld ten behoeve van de verloning van medewerkers alsmede voor de planning op de diverse projecten. Deze applicatie is geïnstalleerd op onze eigen server. AARiverside ondersteunt ons bij de applicatie van ItsClean. Zij kunnen op afstand meekijken via remote support zodat problemen kunnen worden opgelost.

Toestemming support door AaRiverside: de remote support voor ItsClean kan alleen worden opgestart door de medewerker van Rooth Dit kan niet door een medewerker van AaRiverside zelf worden gedaan. Door het opstarten van de remote support geeft Rooth Multiservice b.v. toestemming aan AaRiverside om problemen met ItsClean op te lossen. De remote support wordt door de medewerker van Rooth weer beëindigd.
De medewerkers hebben toegang tot de personele portal (webapplicatie gekoppeld aan ItsClean), hierin kunnen zij hun personele inzien en deels wijzigen. Zij hebben toegang tot deze portal via een eigen weblogin.

1.3.2 Outlook
Microsoft Outlook wordt gebruikt voor ons e-mailverkeer. Wij gebruiken dit e-mailsysteem met als doel een snelle en efficiëntere communicatie. Dit systeem wordt gebruikt door alle kantoormedewerkers van de organisatie. Dit systeem wordt gebruikt voor het versturen van informatie onder de diverse afdelingen binnen ons bedrijf. Dit is een losse applicatie en is onderdeel van Microsoft Office.

1.3.3 Checkmarket
Voor onderzoeksdoeleinden en evaluatie van diverse processen binnen de organisatie maakt Rooth gebruik van Checkmarket. Ruwe onderzoek data (voornaam, achternaam, e-mailadres) worden hierin opgeslagen. Evaluatierapporten worden gearchiveerd op de interne H. schijf en worden 5 jaar bewaard zodat er gegevens met elkaar kunnen worden vergeleken. De antwoorden welke deelnemers geven worden geanonimiseerd. Zodra er een onderzoek is afgerond/afgesloten worden de gegevens na 1 maand verwijderd uit het systeem van Checkmarket. De medewerkers van de ‘administratie’ (zie permissiematrix) hebben toegang tot deze applicatie.

1.3.4 Zijlstra beroepskleding
Rooth maakt gebruikt van een online bestelsysteem voor bedrijfskleding. In dit systeem wordt de naam van de medewerker vastgelegd en zijn kledingmaten. In het systeem kun je tevens de bestelhistorie terugkijken. Indien de medewerker uit dienst treedt worden zijn gegevens verwijderd. Alle kantoormedewerkers hebben toegang tot dit bestelsysteem.

1.3.5 Fooxonline
Wij bestellen onze producten/ artikelen online via www.fooxonline.nl. In dit systeem wordt er rechtstreeks bij de klant afgeleverd. Alleen de klantnaam en het afleveradres wordt in dit systeem vastgelegd. Alle kantoormedewerkers hebben toegang tot deze applicatie met een eigen inlognaam en wachtwoord. Als wij geen diensten meer voor een betreffende klant uitvoeren, worden de gegevens direct uit het systeem verwijderd.

1.3.6 Arbo Anders
Arbo Anders ondersteunt ons op het gebied van de ziekteverzuimbegeleiding en de re-integratie. Dit is een losse applicatie, de medewerkers van de ‘administratie’ en de medewerkers ‘projectleiders’ hebben toegang tot deze applicatie. Als er een medewerker uit dienst gaat, worden de gegevens direct uit het systeem verwijderd.

1.3.7 Website Rooth
De corporate website www.rooth.frl is het informatieportaal van het bedrijf. De informatie is openbaar toegankelijk. Okkinga Communicatie beheert deze website.

1.3.8 Facebook
Rooth heeft een Facebookpagina. Hier worden zaken opgezet als; vacatures, een foto van een diploma uitreiking, foto's diverse klussen. Uiteraard wordt er vooraf toestemming van de betreffende perso(o)n(en) gevraagd.

1.3.9 Twitter
Rooth heeft een Twitteraccount. Hier wordt af en toe een tekstbericht opgezet alsmede een foto. Uiteraard wordt er vooraf toestemming van de betreffende perso(o)n(en) voor gevraagd.

1.4 Privacy statement
Rooth verwerkt persoonsgegevens en wil daarover duidelijk en transparant communiceren. In het privacy statement wordt antwoord gegeven op de belangrijkste vragen over de verwerking van persoonsgegevens door Rooth. Het privacy statement is te vinden op de website (www.rooth.frl) en is als bijlage toegevoegd bij dit document.

1.5 Updates privacy beleid
Rooth behoudt zich het recht voor om wijzigingen aan te brengen in dit privacy beleid. Het verdient aanbeveling om dit privacy beleid regelmatig te raadplegen, zodat je van de wijzigingen op de hoogte bent. Je kunt dit privacy beleid zelf opslaan op raadplegen via www.rooth.frl

2. Registratie en zichtbaarheid persoonsgegevens

2.1 Gegevens matrix
De volgende persoonsgegevens worden door Rooth geregistreerd. Alle kantoormedewerkers hebben toegang tot deze informatie.
Klanten kunnen eventuele gegevens mondeling bij ons opvragen, zij hebben op geen enkele wijze digitale toegang tot deze gegevens. De medewerkers hebben toegang tot hun eigen gegevens via de personele portal webapplicatie gekoppeld aan ItsClean.

Welke gegevens verwerken wij:	
PERSOONSGEGEVENS:	Medewerker kan zelf aanpassen:
Voorna(a)m(en)	
Achtern(a)m(en)	
Geslacht	
Postcode, straatnaam + huisnr	Ja
Woonplaats	Ja
Geboorteplaats	
Geboortedatum	
Telefoonnummer	Ja
Mobielnummer	Ja
E-mailadres	Ja
BSN nummer	
Nationaliteit	
Weblogin	Ja
EENMALIG bij indiensttreding:	
Soort identificatiedocument	

Identificatiedocumentnummer	
Identificatiedocument geldigheid	
FINANCIEEL:	
Bankrekeningnummer	Ja
Machtigingen	
FUNCTIES:	
Functie	
Soort dienstverband	
Datum in dienst	
Data ziektedag(en)	
PROFIEL:	
Kopie Basisdiploma schoonmaak	
Kopie werk gerelateerde diploma's	
Kopie VOG	
Foto's vanaf werklocatie	
Zakelijke auto	
Kledingmaten	
Zakelijk tlf	
Zakelijk pc/tablet	
Zakelijk e-mailadres	
KLANTGEGEVENS	
Klantnaam	
Postcode, straatnaam + huisnr (bedrijfslocatie)	
Woonplaats (bedrijfslocatie)	
Naam contactpersoon	
e-mailadres (persoonlijk)	
e-mailadres (algemeen)	
mobiel of direct telefoonnummer	
alarmprocedure/ sleutelhouder	
bankrekeningnummer	

2.2 Registratie van aanvullende gegevens

Rooth kan aanvullende gegevens definiëren en registreren. Dit kan van belang zijn als er een medewerker onder bewind voering komt te staan. Dan dienen wij als werkgever het loon van een medewerker over te maken naar een derdenrekening. Deze aanvullende gegevens worden zes maanden nadat het traject is afgerond verwijderd uit ons systeem.

2.3 Registratie van bijzondere gegevens

Bijzondere gegevens mogen alleen geregistreerd worden als hiervoor een noodzaak bestaat. Binnen Rooth mag volgens de wet alleen het BSN nummer worden gevraagd. Dit gegeven gebruiken wij voor onze communicatie richting de Belastingdienst (aangifte loonheffing) en APG (aangifte bedrijfspensioenfonds). Alle andere gegevens zijn uitdrukkelijk niet toegestaan te registreren, tenzij hiervoor een duidelijke aanleiding is én de medewerker expliciete toestemming geeft.
Sommige gegevens zijn extra gevoelig. Denk hierbij aan bijvoorbeeld gegevens over iemands gezondheid of godsdienst. Deze gegevens vormen een extra risico voor de privacy van onze medewerkers, aangezien aan de hand van deze gegevens ongewenste koppelingen kunnen worden gemaakt.

2.3.1 Definitie bijzondere gegevens
Onder bijzondere gegevens vallen:

- Gezondheid;
- Burger Service Nummer;
- Ras;
- Godsdienst of levensovertuiging;
- Strafrechtelijk verleden;
- Seksualiteit;
- Politieke gezindheid;
- Lidmaatschap vakvereniging.

2.3.2 Geheimhouding
Personen die permissie hebben persoonsgegevens (zowel algemeen als bijzondere gegevens) te registreren en te raadplegen, zijn verplicht tot geheimhouding tenzij er een wettelijk of redelijke noodzaak toe bestaat gegevens te verstrekken.

2.3.3 Vervaltermijn
Bijzondere gegevens mogen alleen voor een vooraf bepaalde en kenbaar gemaakte periode worden geregistreerd en moeten na deze periode worden verwijderd.

2.3.4 Controle
Aan het einde van ieder jaar worden dossiers gecontroleerd op bijzondere gegevens. Afgehandelde dossiers worden verwijderd.

2.4 Systeembeheer
De applicaties die gebruikt worden binnen Rooth zijn aan onderhoud onderhevig. Prima IT voert het systeembeheer uit. Prima IT heeft geen inloggegevens voor de verschillende applicaties waarin persoonsgegevens worden verwerkt.

2.5 Gegevensbeheer
De toegang wordt zoveel mogelijk beperkt en alleen aan die mensen verstrekt die daadwerkelijk toegang tot deze systemen nodig hebben. Binnen Rooth hebben wij een systeembeheerder die zorgdraagt voor de updates. Tevens kan Prima IT achterhalen wie, wanneer, hoe laat, op welke datum, waar vandaan heeft ingelogd.

2.6 Permissies
Het toekennen van permissies binnen de ontwikkelde applicaties is opgenomen in het permissiemodel. Veelal zijn de permissies gekoppeld aan de functie die een persoon vervult binnen Rooth. Bij verandering van functie, worden ook de permissies meegenomen. Binnen de applicaties is het gebruikelijk dat het toekennen van rechten gebeurt op het bovenliggende niveau en dus nooit door de gebruiker zelf kan gebeuren (toe-eigenen van rechten).

3. Verstrekken, uitwisselen en gebruik van persoonsgegevens
Naast strenge privacywetgeving, gelden onderstaande beleidsafspraken rondom het verstrekken van gegevens. De afspraken staan per niveau beschreven.

3.1 Algemeen

3.1.1 Wie verwerkt?

- Directeur en administratie;
  Zij kunnen allen persoonsgegevens invoeren, wijzigen, opslaan, kortom verwerken. En zij hebben toegang tot alle applicaties.
- Projectleiders en de objectleider,
  Zij kunnen persoonsgegevens invoeren, wijzigen, opslaan, kortom verwerken. Zij hebben geen toegang tot de 'AAsalaris' applicatie. Tot de overige applicaties hebben zij wel toegang. Tevens is dit vastgelegd in ons permissiemodel.

3.1.2 Voorwaarden gebruik van persoonsgegevens

Het gebruik van gegevens dient aan de volgende voorwaarden te voldoen:

- Er moet een duidelijk doel worden gesteld waartoe de gegevens gebruikt gaan worden, waarbij duidelijk wordt wie voor welke periode toegang heeft tot welke gegevens;
- Er mogen enkel relevante gegevens gebruikt worden. Met andere woorden, er mogen geen onnodige of bovenmatige gegevens verzameld of gebruikt worden;
- Er dient een permissiemodel opgesteld te worden waarin wordt vastgelegd welke personen toegang krijgen tot welke gegevens. Tevens dient er een gedegen beveiliging te worden aangebracht op het gebruik van de gegevens;
- De gegevens mogen niet aan derden worden verstrekt tenzij daar expliciet toestemming voor gegeven is door de medewerker of daartoe een wettelijke verplichting bestaat;
- De gegevens mogen alleen voor een vastgestelde periode worden gebruikt en dienen daarna verwijderd te worden. Tussentijds moeten gegevens op het verzoek van een medewerker verwijderd kunnen worden. Langer gebruik dan de vooraf vastgestelde periode kan alleen met expliciete toestemming van de medewerker;
- Bijzondere gegevens, waaronder godsdienst, gezondheid of strafrechtelijke gegevens, mogen alleen verzameld worden indien daartoe een strikte noodzaak bestaat en met expliciete consensus van de medewerker. Deze gegevens dienen volledig te worden verwijderd na afloop van de gestelde periode;
- Het gebruik van gegevens gebeurt conform het privacy beleid en de AGV.

3.2 Externe partijen

- Verstrekken van persoonsgegevens, adresgegevens en e-mailadressen van de medewerkers aan een niet gecontracteerde organisatie cq. externe organisatie (zowel commercieel als non-profit) is in geen enkel geval toegestaan.

4.Muteren van persoonsgegevens

De gegevens van een medewerker kunnen door de kantoormedewerkers worden gemuteerd. Wie welke gegevens kan muteren staan beschreven in een permissiematrix (hieronder).

Permissiematrix					
Toekennen rechten AARIverside	**Directeur**	**Administratie**	**Projectleider**	**Objectleider**	**Systeembeheerder**
AARelatie	x	x	x	x	x
Itsclean	x	x	x	x	x
AAPersoneel	x	x	x	x	x
AAFinancieel	x	x	x	x	x
AASalaris	x	x	x	x	x
Algemeen: historie e-mail	x	x	x	x	x
Algemeen: overig					x
Onderhoud tabellen					x
Itstrade	x	x	x	x	x
Update applicatie					x
Er is geen onderscheid gemaakt in verschillende handelingen per applicatie. Kortom heb je toegang tot een applicaite, heb je naast de raadpleegfunctie ook de muteerfunctie.					

5. Bewaren van persoonsgegevens

AARiverside heeft in- en export mogelijkheden om bijvoorbeeld een lijst te maken van projecten met haar adresgegevens en contact(persoons)gegevens erbij zodat de objectleider deze onderweg bij haar heeft. Het is expliciet niet de bedoeling lijsten te exporteren en deze voor langere tijd te bewaren of door te geven aan mensen die normaliter geen toegang hebben tot die gegevens.

5.1 Lijsten maken

Op het moment dat er door een gebruiker gegevens geëxporteerd mogen worden uit AARiverside kun je hiervoor op de exportknop drukken.

Als er een lijst geëxporteerd wordt is dit zoals al eerder aangeven alleen voor een beperkte tijd. Persoonsgegevens zijn aan verandering onderhevig, een lijst die bewaard wordt kan dus verouderde gegevens bevatten. Tevens kan het bewaren een potentieel beveiligingsprobleem zijn, aangezien de gegevens dan opgeslagen worden in een documentenmap en er vanuit de organisatie geen zicht is op virussen, spyware, etc.
Het is dan ook geheel de verantwoording van degene die de lijst exporteert en opslaat om te zorgen dat deze gegevens correct en veilig worden bewaard. Het betreft hier een lijst die specifiek voor de betreffende gebruiker van belang is. Iedere gebruiker heeft een eigen deel beschikbaar op de server voor zijn/haar documenten. Dit is een persoonlijke documentenmap.

Bescherming:
De betreffende medewerker krijgt toestemming voor het maken van dergelijke lijsten.
Door de lijst in de persoonlijke documentenmap te bewaren (afgeschermd omdat je moet inloggen en de map niet voor anderen zichtbaar en/of toegankelijk is) zijn de gegevens beschermd.

5.2 Kopiëren

Het is uitdrukkelijk verboden de geëxporteerde gegevens te vermenigvuldigen of te kopiëren op elke mogelijke manier. De export is strikt persoonlijk en hier dient dan ook zorgvuldig mee omgegaan te worden.

5.3 Publiceren

Is niet aan de orde bij Rooth.

5.4 Verwijderen

Een export moet zo kort mogelijk bewaard worden. Diegene die de export maakt is er persoonlijk verantwoordelijk voor om deze dusdanig te verwijderen dat deze niet meer te herstellen is door onbevoegden.

5.5 Bewaren van gegevens in AARiverside

De gegevens blijven hier in staan zolang de medewerker in dienst is. Dit omvat zowel de persoonsgegevens als bijvoorbeeld diploma's en bankgegevens. Na uitdiensttreding is de bewaartermijn:
Fiscale bewaarplicht: loonheffingenformulier en kopie identiteitsbewijs: 5 jaar. Voor overige documenten geldt een bewaartermijn van 2 jaar nadat je uit dienst bent. De (aanvullende gegevens) van medewerkers die uit dienst zijn worden direct verwijderd.

6. Berichten verzenden

6.1 E-mail

E-mail is een doeltreffend middel om doelgroepen binnen Rooth op een directe manier te bereiken. Het draagt bij aan de bewaking van onze kwaliteit en processen. Het is dan ook niet vreemd dat hier zeer regelmatig gebruik van wordt gemaakt.
Bij het verzenden van deze e-mails is er géén OPT-Out mogelijkheid. Rooth gebruikt het middel 'E-mail' niet voor marketing- en / of andere doeleinden.
Wij maken ook gebruik van functionele e-mails, zoals de verzending van de loonstrook via de e-mail (vanuit ITSClean).

7. Online media Rooth

Online communicatie kan ook binnen Rooth niet meer ontbreken. Naast de vele voordelen van online media, zijn er ook aandachtspunten, waaronder wetgeving op het gebied van cookies.

7.1 Analytics

Op basis van Google Analytics kunnen wij een aantal zaken uitlezen over onze website:

- Bijhouden van het aantal bezoekers op onze webpagina's;
- Bijhouden van de tijdsduur die elke bezoeker doorbrengt op onze webpagina's;
- Het bepalen van de volgorde waarin een bezoeker de verschillende pagina's van onze website bezoekt;
- Het beoordelen welke delen van onze site aanpassing behoeven;
- Het optimaliseren van de website.

Anders dan deze cookie gebruikt Rooth niet op haar website.

7.2 Links

Zonder voorafgaande schriftelijke toestemming van Rooth is het niet toegestaan links naar dergelijke sites op de website te zetten.

7.3 Uitsluiting van aansprakelijkheid

Rooth aanvaardt geen enkele aansprakelijkheid ten aanzien van directe, indirecte, bijzondere, incidentele, immateriële of gevolgschade, ongeacht of Rooth op de mogelijkheid van deze schade gewezen is, die op enigerlei wijze voortvloeit uit maar niet beperkt hoeft te zijn tot (I) defecten, virussen of overige onvolkomenheden aan apparatuur en andere software in verband met de toegang tot of het gebruik van deze internetsite, (II) de informatie die op of via deze internetsite wordt aangeboden, (III) het onderscheppen, wijzigen of oneigenlijk gebruik van informatie die aan Rooth of aan u wordt gezonden, (IV) de werking of het niet-beschikbaar zijn deze internetsite, (V) misbruik van deze internetsite, (VI) verlies van gegevens, (VII) het downloaden of gebruiken van software die via deze internetsite beschikbaar wordt gesteld of (VIII) aanspraken van derden in verband met gebruik van deze internetsite.

De uitsluiting van aansprakelijkheid strekt mede ten gunste van bestuurders en medewerkers van Rooth.

7.4 Toepasselijk recht

Op deze internetsite is het Nederland recht van toepassing.

7.5 Wijzigingen

Rooth behoudt zich het recht voor de op of via deze internetsite aangeboden informatie te allen tijde te wijzigen zonder hiervan nadere aankondiging te doen. Het verdient aanbeveling periodiek na te gaan of de op of via deze internetsite aangeboden informatie is gewijzigd.

7.6 Documenten, illustraties (foto)materiaal en content

Alle content, documenten, beschikbaar gestelde illustraties, logo’s, fotomateriaal en overige inhoud van deze website zijn copywright Rooth en diverse illustratoren, fotografen of partners. Wilt u iets van dit (foto)materiaal, illustraties, logo’s of teksten, downloads en overige media gebruiken, neem dan contact op met info@rooth.frl

8. Datalekken

Uiteraard doet Rooth er alles aan om de in dit document genoemde persoonsgegevens niet in handen van derden die geen toegang tot die gegevens zouden mogen hebben te laten vallen. Gebeurt dit wel, dan spreken we over een datalek. In artikel 34a van de Wet Bescherming Persoonsgegevens is sinds 1 januari 2016 geregeld dat als er een datalek plaats vindt dit gemeld moet worden. Er wordt hier echter met klem gesproken over het lekken van persoonsgegevens als gevolg van beveiligingsproblemen. Deze datalekken moeten – als ze voldoende ernstig zijn- onverwijld worden gemeld aan de toezichthouder, de Autoriteit Persoonsgegevens (AP), voorheen het CBP.

8.1 Procedure datalekken herkennen

Een datalek kan op verschillende manieren herkend worden. Over het algemeen zal het een melding zijn van Prima IT dat er een manier is om buiten de beveiliging om data op te vragen die niet publiek beschikbaar zou mogen zijn. Dit houdt echter nog niet in dat deze kwetsbaarheid gebruikt is door derden. Doordat er een logging plaats vindt kan er hierna gekeken worden of er daadwerkelijk een datalek heeft plaatsgevonden.

Prima IT voert intern audits uit. Als hier kwetsbaarheden aan het licht komen zal hier verder hetzelfde mee omgegaan worden als bij een melding door Prima IT.

8.2 Procedure datalekken communiceren

8.2.1 Aan de toezichthouder

Zodra er een datalek is geconstateerd zal binnen 72 uur dit gemeld moeten worden bij de toezichthouder. De melding hieraan bevat tenminste:

- De aard van de inbreuk;
- De instanties waar meer informatie over de inbreuk kan worden verkregen;
- De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- Een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van de persoonsgegevens;
- De maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.

8.2.2 Aan de medewerker

Nadat er een datalek heeft plaatsgevonden en het waarschijnlijk is dat het lek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokken medewerker, dient deze medewerker een melding te ontvangen. In deze melding zal tenminste de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken bevatten.

9. Misbruik van persoonlijke gegevens

9.1 Misbruik voorkomen

Wanneer persoonsgegevens gebruikt worden op een andere manier dan is toegestaan volgens wet en beleid, dan is er sprake van ongeoorloofd gebruik. Het ongeoorloofd gebruik kan onopzettelijk zijn, omdat men niet op de hoogte is van de regels. Er kan ook sprake zijn van opzet. In het kader van dit beleid verstaan we onder het begrip ‘misbruik’ zowel opzettelijk als onopzettelijk ongeoorloofd gebruik. Misbruik kan leiden tot schade aan personen of de organisatie.

We spreken over misbruik, wanneer:
- een persoon die daartoe niet gerechtigd is gegevens verkrijgt en gaat gebruiken.
- Een in principe gerechtigd persoon de gegevens gebruikt voor een ander doel dat (hem) is toegestaan.
- Gegevens gebruikt worden die niet geregistreerd of gebruikt mogen worden.

Om misbruik te voorkomen is het belangrijk dat een aantal maatregelen getroffen worden. Zo is het belangrijk om beleid op het gebied van privacy en persoonsgegevens te hebben, afspraken te maken en dit ook duidelijk te communiceren. Duidelijkheid over goed gebruik van gegevens voorkomt in ieder geval onopzettelijk misbruik. Naast beleid en communicatie daarover is dit voor onze kantoormedewerkers vastgelegd in de arbeidsovereenkomst.

9.1.1 Controle

In onze personeelsadministratie kunnen alleen de bevoegde personen bij de gegevens. Met de partij die onze ICT zaken beheert en de partij(en) die onze applicaties leveren is een verwerkersovereenkomst afgesloten.

9.1.2 Arbeidsovereenkomst
Personen die breed toegang hebben tot gegevens moeten bij de start van hun dienstverband een arbeidsovereenkomst ondertekenen met hierin opgenomen een paragraaf over het verstrekken van (persoons)gegevens. Hierin staat beschreven dat er zorgvuldig moet worden omgegaan met gegevens, waaronder persoonsgegevens.

9.2 Misbruik melden
Wanneer iemand een vermoeden heeft dat er misbruik wordt gemaakt van persoonsgegevens binnen Rooth, dient dit gemeld te worden bij Rooth zodat er waar nodig maatregelen getroffen kunnen worden. Zie voor contactgegevens en procedure hoofdstuk 10.

9.3 Maatregelen
Misbruik van gegevens zal – afhankelijk van de ernst - aanleiding geven tot een van de volgende maatregelen: waarschuwing, ontzeggen toegang tot gegevens, beëindigen functie of taak en eventueel zelfs einde lidmaatschap of dienstverband. Er zal daarnaast ook steeds worden onderzocht of dit misbruik voorkomen kan worden.

10 Vragen en klachten
Vragen over Privacy bij Rooth Multiservice b.v. kun je stellen via info@rooth.frl

Ook voor een klacht of melding kun je hier terecht. Van elke melding zullen we de nodige gegevens registreren. Daardoor kunnen we tijdens behandeling het nodige contact onderhouden met degene die contact met ons heeft opgenomen.
Bij elke melding zullen we proberen te achterhalen:
- waar de gebruikte gegevens vandaan komen;
- Wat er met de gegevens is gebeurd;
- Wie er betrokken is;
- Of er schade is ontstaan en hoe die zoveel mogelijk te herstellen is;
- Of er stappen nodig zijn om herhaling te voorkomen.

Privacy statement

Rooth verwerkt persoonsgegevens. Wij willen je hierover graag duidelijk en transparant informeren. In dit privacy statement geven wij je antwoord op de belangrijkste vragen over de verwerking van persoonsgegevens door Rooth.

Wat zijn persoonsgegevens?

Er zijn gegevens die iets over jou zeggen. Bijvoorbeeld je naam, adres, leeftijd. Wanneer (een combinatie van) deze gegevens naar jou herleid kunnen worden spreken we over persoonsgegevens. Bijvoorbeeld je adres of e-mailadres. Maar bijvoorbeeld ook je voornaam samen met je geboortedatum. Wanneer anderen die persoonsgegevens hebben, moeten ze daar zorgvuldig mee omgaan. Ook foto's en video's worden gezien als persoonsgegevens.

Van wie verwerkt Rooth?

Rooth verwerkt persoonsgegevens van mensen met wie wij direct of indirect een relatie hebben, willen krijgen of hebben gehad. Dat zijn bijvoorbeeld gegevens van:

- Bedrijven of partijen die een offerte aanvragen;
- Medewerkers en leveranciers, waar wij een relatie mee hebben, willen krijgen of hebben gehad.

Wie is verantwoordelijk voor de verwerking van mijn persoonsgegevens?

Alle kantoormedewerkers van Rooth verwerken persoonsgegevens in ItsClean, de administratieve applicatie van Rooth en de daaraan gerelateerde applicaties zoals het planningssysteem en het verloningssysteem.

Waarvoor verwerkt Rooth persoonsgegevens?

Als je medewerker wilt worden van Rooth of een andere relatie met ons aan wilt gaan, hebben wij persoonsgegevens nodig. Met behulp van je gegevens kunnen we je op de juiste wijze inschrijven als medewerker, zorg dragen voor je verloning en ervoor zorgen dat de juiste gegevens bekend zijn bij de overheidsinstanties, zoals de Belastingdienst.

Als je eenmaal een medewerker of relatie van Rooth bent, dan willen we je goed van dienst zijn. Wij gebruiken je naam, je telefoonnummer en je e-mailadres om contact met je te onderhouden en je te informeren over zaken die jou aangaan. Maar ook als je een vraag stelt, verwerken wij je gegevens om je zo goed mogelijk te kunnen helpen. Tot slot zijn er praktische zaken waarvoor we gegevens verwerken. Bijvoorbeeld ter ondersteuning van administratieve processen rondom de uitbetaling van loon en het afhandelen van de aangifte loonheffingen aan de Belastingdienst.

Verwerkt Rooth ook bijzondere persoonsgegevens?

Bijzondere persoonsgegevens zijn gevoelige gegevens, bijvoorbeeld over gezondheid, strafrechtelijk verleden, etnische gegevens of gegevens betreffende ras.

Wij verwerken alleen bijzondere persoonsgegevens als wij dat moeten op basis van de wet, met jouw toestemming of als je dat ons vraagt. In dat laatste geval verwerken wij deze gegevens alleen als dat noodzakelijk is voor onze dienstverlening.

Binnen Rooth mag volgens de wet alleen het BSN nummer van een medewerker worden gevraagd. Dit gegeven gebruiken wij voor onze communicatie richting de Belastingdienst. Alle andere gegevens zijn uitdrukkelijk niet toegestaan te registreren, tenzij hiervoor een duidelijke aanleiding is én de medewerker expliciete toestemming geeft.

Hoe gaat Rooth met mijn persoonsgegevens om?

Je persoonsgegevens worden zorgvuldig bewaard en niet langer dan noodzakelijk is voor normaal gebruik binnen ons bedrijf of het doel waarvoor zij zijn, verwerkt.

Wie kan er bij mijn persoonsgegevens?

Je kunt uiteraard zelf bij je persoonsgegevens. Deze kun je te allen tijde zelf opvragen telefonisch of schriftelijk. Tevens kun je deze zelf raadplegen (en deels zelf wijzigen) op de personele portal.

Daarnaast kunnen de kaderleden je gegevens raadplegen.

Uitwisseling van persoonsgegevens binnen Rooth

Willen wij gegevens voor een ander doel gebruiken dan waarvoor ze oorspronkelijk verwerkt waren? Dan kunnen wij dat alleen wanneer er tussen beide doelen een nauwe verwantschap bestaat. Bijvoorbeeld als je een nieuwe functie krijgt binnen Rooth. Rooth kan en mag geen gegevens uitwisselen met externe partijen.

Hoelang worden mijn gegevens bewaard?

Gegevens gerelateerd aan je dienstverband worden in beperkte vorm na uit diensttreding bewaard om te voldoen aan de wettelijk bepaalde voorschriften.

Welke regels gelden bij de verwerking van persoonsgegevens?

Bij de verwerking van persoonsgegevens is Rooth gebonden aan de daarvoor geldende wet- en regelgeving.

Kan ik zien welke gegevens Rooth van mij verwerkt?

Je kunt te allen tijde telefonisch of schriftelijk opvragen welke gegevens wij verwerken. Tevens is dit beschreven in ons privacybeleid.

Waar kan ik terecht met een vraag of klacht?

Voor vragen of klachten over de verwerking van persoonsgegevens door Rooth Multiservice b.v. kun je bellen met 0515 424 545 of een e-mail sturen aan info@rooth.frl

Wijzigingen privacybeleid

Rooth behoudt zich het recht voor om wijzigingen aan te brengen in dit privacybeleid. Je kunt dit privacybeleid zelf opslaan of raadplegen via www.rooth.frl