

# Intern Privacybeleid ExpatTeam

Versie	Datum	Samengesteld door	Omschrijving
0.1	03-05-2018	C.M. Heeroms	Eerste versie

<b>Inhoudsopgave</b>	
<b>Inleiding</b> .....	3
<b>Hoofdstuk 1 – Intern gebruik van gegevens</b> .....	4
<b>1.1 Wat zijn persoonsgegevens?</b> .....	4
<b>1.2 Verwerken van gegevens</b> .....	4
<b>1.3 Rolverdeling</b> .....	4
<b>1.4 Soorten persoonsgegevens</b> .....	5
<b>1.5 Doeleinden verwerken gegevens</b> .....	7
<b>1.6 Verzenden van gegevens</b> .....	7
<b>1.7 Bewaren van gegevens</b> .....	8
<b>1.8 Verwijderen van gegevens</b> .....	10
<b>Hoofdstuk 2 – Beveiligen van gegevens</b> .....	11
<b>2.1 Beveiligingsmaatregelen en handleidingen</b> .....	11
<b>2.2 Beperkte toegang tot gegevens</b> .....	12
<b>2.3 Datalek</b> .....	12
<b>Hoofdstuk 3 – Rechten van mensen</b> .....	12
<b>Hoofdstuk 4 – Contact</b> .....	14

## **Inleiding**

Dit intern privacybeleid fungeert als leidraad hoe binnen onze organisatie wordt omgegaan met privacy gerelateerde gegevens, zogeheten persoonsgegevens. Dit beleid is door ExpatTeam opgesteld mede als handvat bij het gebruik van persoonsgegevens, maar ook om naar buiten toe aan te kunnen tonen dat wij zorgvuldig met persoonsgegevens omgaan.

In dit beleid wordt uitgelegd wat persoonsgegevens zijn, welke regels er gelden bij het gebruik van deze gegevens en welke maatregelen onze medewerkers moeten nemen bij het gebruik van deze gegevens. Het is belangrijk dit beleid strikt na te leven. Door als organisatie dit beleid na te leven wordt de privacy van alle betrokkenen (waaronder klanten, medewerkers en bezoekers/gebruikers van de websites vallen) gewaarborgd.

Houden wij ons als organisatie niet aan dit beleid, dan bestaat er een kans dat gegevens van betrokkenen bijvoorbeeld verloren raken en hun privacy hierdoor wordt geschonden. Als organisatie willen wij dit voorkomen. Houd je daarom altijd aan de regels van dit beleid wanneer je met persoonsgegevens werkt.

Dit beleid heeft een dynamisch karakter en kan van tijd tot tijd worden aangevuld of herzien. Dit kan naar aanleiding van veranderingen in onze organisatie, bedrijfsprocessen, aanpassingen van informatiesystemen of wetswijzigingen. Indien het beleid aangepast wordt, zullen wij je dit laten weten via onze website [www.expatteam.nl](http://www.expatteam.nl).

## **Hoofdstuk 1 – Intern gebruik van gegevens**

### **1.1 Wat zijn persoonsgegevens?**

Om duidelijk aan te geven hoe binnen onze organisatie wordt omgegaan met persoonsgegevens, is het van belang eerst duidelijk te definiëren wat persoonsgegevens precies zijn.

Persoonsgegevens zijn de gegevens over een persoon die ervoor zorgen dat een persoon identificeerbaar is, of geïdentificeerd kan worden. Een persoonsgegeven kan direct of indirect naar een persoon herleiden.

Aan de hand van een naam of adres is zonder veel omwegen vast te stellen om welke persoon het gaat. Maar ook als er meerdere gegevens gecombineerd moeten worden om vast te stellen om wie het gaat, kan er sprake zijn van een persoonsgegeven. Zo kan een postcode of IP-adres naar een persoon herleid worden, daar zijn echter wel aanvullende gegevens voor nodig, zoals bijvoorbeeld een huisnummer.

In onze systemen zijn vrijwel alle gegevens gekoppeld aan een persoon. Hierdoor is het eenvoudig te achterhalen bij welke persoon de gegevens horen. Daarom zijn de gegevens die gebruikt worden in onze systemen aan te merken als persoonsgegevens. Persoonsgegevens kunnen uiteraard ook gegevens van onze eigen medewerkers zijn.

Voorbeelden van veelgebruikte persoonsgegevens zijn:

- NAW-gegevens;
- Telefoonnummer;
- E-mailadres;
- Geslacht;
- Geboortedatum.

### **1.2 Verwerken van gegevens**

Als er persoonsgegevens gebruikt worden, wordt dit het verwerken van persoonsgegevens genoemd, of gegevensverwerking. Aan het verwerken van persoonsgegevens zijn wettelijke rechten en plichten verbonden. Onder verwerken vallen alle handelingen die met persoonsgegevens worden verricht zoals:

- Het opslaan van gegevens;
- Het verwijderen van gegevens;
- Het kopiëren van gegevens;
- Het delen van gegevens met bijvoorbeeld de Belastingdienst.

Aangezien de gegevens van onze klanten die we bij onze dagelijkse werkzaamheden verwerken persoonsgegevens zijn, is het van belang bij het verwerken van deze gegevens voortdurend rekening te houden met de wettelijke rechten en plichten. Wij zijn als ExpatriationTeam namelijk verantwoordelijk voor het zorgvuldig verwerken van deze gegevens.

### **1.3 Rolverdeling**

In de privacywetgeving wordt bij de verwerking van persoonsgegevens uitgegaan van een bepaalde rolverdeling. In deze rolverdeling is er sprake van drie verschillende

partijen, namelijk de betrokkene (de natuurlijk persoon aan wie de persoonsgegevens toebehoren), de verwerkingsverantwoordelijke (de partij die de persoonsgegevens van de betrokkene besluit voor een bepaald doel te gaan verwerken en hiervoor het doel en de middelen aanwijst) en de verwerker (de partij die door de verantwoordelijke wordt ingeschakeld om te ‘ondersteunen’ bij de verwerking of de verwerking uit te voeren, maar niet onder diens directe gezag valt zoals bijvoorbeeld een werknemer dat wel doet).

Wanneer wij zelf weer derde partijen inschakelen om namens ons gegevens te verwerken, bijvoorbeeld een partij die gegevens voor ons opslaat, cookies faciliteert, nieuwsbrieven verstuurd of gegevens analyseert, dan noemen we dergelijke partijen ‘verwerkers’. Deze partijen verwerken dan in opdracht van ons persoonsgegevens. Met verwerkers wordt altijd een verwerkersovereenkomst gesloten. Een verwerkersovereenkomst is wettelijk verplicht als persoonsgegevens verwerkt worden ten behoeve van een ander. Hierin is opgenomen welke gegevens verstrekt worden en voor welke doeleinden zij deze gegevens mogen verwerken. Daarnaast moeten wij ook met onze klanten een verwerkersovereenkomst sluiten als we gegevens van ze ontvangen waarvoor we verwerker zijn.

Als je twijfelt of bepaalde persoonsgegevens wel gebruikt mogen worden, wanneer je gegevens moet verstrekken aan derde partijen, of indien je vragen hebt over specifieke gegevens, neem dan direct contact op met C.M. Heeroms

#### 1.4 Soorten persoonsgegevens

Er worden verschillende persoonsgegevens in onze systemen verwerkt. Dit zijn bijvoorbeeld gegevens van medewerkers die door de HR-afdeling worden ingevuld, of gegevens van onze klanten.

Voorbeelden van gegevens van klanten die in onze systemen worden verwerkt zijn:

- **Basisgegevens:**
  - NAW-gegevens;
  - Geboortedatum;
  - Geslacht;
  - Telefoonnummer;
  - E-mailadres;
  - Burgerservicenummer (BSN);
  - Kopie legitimatiebewijs;
  - Rekeningnummer;
  - Salarisinformatie;
  - Functie informatie;
  - Bedrijfsgegevens;
  - Btw-nummer;
  - IP-adres;
  - Cookie ID.
  -
- **Optioneel:**
  - BSN van een partner en/of kinderen;
  - Gegevens over alimentatie;
  - Eigen woning informatie;

- Overige informatie (zorgkosten, studiekosten, giften, leningen, verzekeringen etc.).

Wij maken gebruik van verschillende systemen/applicaties om bovenstaande gegevens in te verwerken. Gegevens mogen verwerkt worden in de volgende systemen:

- Middels de remote desk top via excel sheets
- In de map waarin HR gegevens worden opgeslagen
- De remote desktop, via the sourcing company;
- Alle gegevens van klanten dienen op de remote desktop via the sourcing company te worden opgeslagen.

Het is niet toegestaan de gegevens in een ander systeem te verwerken dan hierboven aangegeven. Is het nodig gegevens toch in een ander systeem te verwerken? Neem dan contact op met C.M. Heeroms

### **Bijzondere persoonsgegevens**

Persoonsgegevens kunnen daarnaast nog aangemerkt worden als ‘bijzonder’. Bijzondere persoonsgegevens zijn gegevens die direct of indirect iets zeggen over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Het is mogelijk dat mensen aan ons bijzondere persoonsgegevens verstrekken bijvoorbeeld middels brieven, mails en/of telefoontjes. Denk hierbij aan klanten die terloops ook iets over hun gezondheid vermelden.

Het is van belang dat wij zorgvuldig omgaan met dit soort gegevens en dit zo min mogelijk vastleggen. Noteer enkel wat hoogstnoodzakelijk is, bijvoorbeeld de afspraak kan niet doorgaan wegens ziekte. Treedt hierbij niet in detail. Het is voor ExpatTeam namelijk in veel gevallen niet toegestaan om deze gegevens te verwerken, ondanks dat een klant vrijwillig deze gegevens aan ons verstrekt. Het verwerken van dergelijke persoonsgegevens is namelijk aan strenge eisen verbonden, aangezien het om gevoelige informatie over personen gaat.

Van onze medewerkers worden ook bijzondere persoonsgegevens verwerkt. Het is voor ExpatTeam toegestaan deze gegevens te verwerken indien dat noodzakelijk is voor de goede uitvoering van de arbeidsovereenkomst of bij re-integratie of begeleiding van een werknemer in verband met ziekte of arbeidsongeschiktheid.

Dit is het geval als een medeweker bijvoorbeeld epilepsie heeft. Hiervan dienen wij op de hoogte te zijn, zodat wij op een juiste wijze kunnen handelen in een acute situatie. Het is echter niet toegestaan altijd bij een ziekmelding te noteren waarom iemand afwezig is, dit wordt daarom ook niet door de directie gedaan.

### **Register**

Om dit allemaal inzichtelijk te krijgen en te houden, zijn wij verplicht een register bij te houden. Dit register bevat continu een up-to-date overzicht van alle soorten persoonsgegevens die wij verwerken. De registers zijn te vinden bij C.M. Heeroms. Omdat wij verplicht zijn om deze registers up-to-date te houden vragen wij je om eventuele wijzigingen zo spoedig mogelijk door te geven via C.M. Heeroms.

### 1.5 Doeleinden verwerken gegevens

De gegevens van o.a. onze klanten en medewerkers worden verwerkt, zodat wij onze diensten kunnen aanbieden en onze administratie kunnen beheren. Dit is het zogeheten doeleinde voor het verwerken van de gegevens.

- het verlenen van toegang tot onze website en het gebruikmaken hiervan;
- het opnemen van contact met een klant, indien hierom wordt verzocht;
- het bieden van onze verschillende vormen van dienstverlening zoals het doen van aangiftes, verzorgen van de administratie en geven van advies over uiteenlopende onderwerpen, het verzorgen en onderhouden van de Internationale salarisadministratie;
- het maken van berekeningen voor het bepalen van het in Nederland te belasten loon;
- het verkrijgen van inzicht in het gebruik van onze website en het verbeteren en evalueren van onze website en diensten;
- het voldoen aan onze fiscale bewaarplicht.

De gegevens die verzameld worden van klanten, mogen enkel voor bovenstaande doeleinden gebruikt worden. Het is uitdrukkelijk niet toegestaan de gegevens van klanten voor andere doeleinden te gebruiken. Mocht je gegevens voor andere doeleinden willen verwerken, verifieer dat dan eerst bij C.M. Heeroms.

Vanzelfsprekend worden gegevens van onze medewerkers verwerkt om de personeelsadministratie op een juiste manier uit te voeren. Gegevens van medewerkers mogen enkel door ExpatTeam gebruikt worden voor de taken die zij toegewezen hebben gekregen, of andere afdelingen indien zij ook concrete taken toegewezen hebben gekregen waarbij het verwerken van gegevens van medewerkers noodzakelijk is. Gegevens van medewerkers worden verwerkt voor onder andere:

- Het verwerken van de loonadministratie;
- Het regelen van ziekte en verlof; en
- Het regelen van in- en uitdiensttreding.

Twijfel je of gegevens van medewerkers voor een specifiek doel gebruikt mogen worden? Neem dan contact op met C.M. Heeroms

### 1.6 Verzenden van gegevens

Het is eenvoudig bestanden te verzenden via je werkmail. Het is echter mogelijk dat deze bestanden persoonsgegevens bevatten van mensen. Wanneer je bestanden via je werkmail verzendt is het van belang met het volgende rekening te houden:

- **Intern:** Voor het intern verzenden van bestanden via je werkmail naar andere medewerkers, is dit geen probleem indien de bestanden worden verzonden via ons interne netwerk naar de werkmail van een andere medewerker. Let daarbij wel op dat je enkel gegevens verstuurt naar een andere medewerker, die voor deze medewerker noodzakelijk zijn om te ontvangen. Verwijs ook altijd naar de systemen waarin de gegevens beschikbaar zijn, indien de medewerker daar ook toegang toe heeft. Dat voorkomt het onnodig verzenden van gegevens. Twijfel je of je bepaalde gegevens mag afgeven aan een collega? Neem dan contact op met C.M. Heeroms.

- **Extern:** Voor het verzenden van bestanden naar externe personen/organisaties is het van belang dat, indien de inhoud van deze bestanden gevoelig is, deze bestanden versleuteld verzonden worden. Denk hierbij aan bestanden waar het BSN van klanten in staat, zoals loonstroken en kopieën van een aangifte. Daarnaast kan ook de omvang aanleiding geven tot het versleuteld versturen van e-mailinhoud. Denk bijvoorbeeld aan e-mails met mailinglijsten of meerdere CV's. Versleutel bestanden enkel op een door ExpatTeam aangeboden wijze. Deze wijze is momenteel onze digitale beveiligde kluis. Verstuur bovendien enkel gegevens wanneer hiervoor de juiste afspraken zijn gemaakt met de ontvanger, zoals een verwerkersovereenkomst als dat noodzakelijk is. Of er een verwerkersovereenkomst is gesloten kun je navragen bij C.M. Heeroms. Twijfel je of je bestanden mag versturen en/of moet versleutelen, of heb je hier vragen over? Neem dan contact op met C.M. Heeroms.

**Let op!** Verstuur enkel bestanden via je werkmail en het interne netwerk van ExpatTeam, of via een andere door ExpatTeam aangeboden beveiligde verzendwijze. Verstuur geen bestanden met je privé mail, en gebruik geen 'openbare' applicaties zoals Dropbox en GoogleDocs. Download en upload enkel bestanden met je werkapparatuur, en niet met je privé laptop/telefoon/tablet.

### 1.7 Bewaren van gegevens

Wat betreft het bewaren van gegevens hanteren wij de volgende minimale eisen:

- De gegevens moeten tijdens de opslag voldoende beschermd zijn. Dit is mede afhankelijk van de aard van de gegevens. De bescherming dient te voldoen aan de verplichte wet- en regelgeving. Denk hierbij aan het beveiligd opslaan van documenten op je computer/laptop/smartphone, of het afsluiten van kasten waarin papieren documenten worden bewaard;
- De gegevens moeten opgeslagen worden binnen Europese grenzen. Indien gegevens buiten de Europese grenzen worden opgeslagen dan moeten hiervoor speciale afspraken worden gemaakt. Maak daarom nooit zonder overleg gebruik van applicaties van partijen zoals Google;
- Het moet bekend zijn waar welke gegevens zijn opgeslagen, dit houdt in dat het duidelijk moet zijn in welke systemen of op welke apparatuur gegevens opgeslagen staan; en
- Er moet een mogelijkheid zijn om de opgeslagen gegevens over te dragen aan de betreffende persoon.

Wat betreft de termijn dat de gegevens bij ons bewaard worden geldt dat alle gegevens die door de Belastingdienst wettelijk verplicht zijn om te bewaren, voor een termijn van zeven jaar worden bewaard. Hieronder vallen de volgende gegevens:

- het grootboek;
- de debiteuren- en crediteurenadministratie;
- de in- en verkoopadministratie;
- de loonadministratie.

Voor alle andere gegevens geldt dat deze slechts bewaard mogen blijven zolang de gegevens daadwerkelijk voor ons noodzakelijk zijn. Daarbij hanteren wij de volgende tabel:



### Medewerkers

Soort gegevens	Bewaartermijn
Personeelsdossier	Tot twee jaar na einde dienstverband
Loonbelastingverklaringen en kopie identiteitsbewijs	Tot vijf jaar na einde dienstverband
Afstandsverklaring woon-werkverkeer werknemer	Zolang reiskostenvergoeding betaald plus zeven jaar
Tijdsregistratie werknemer	52 weken vanaf dag van registratie
Verslaglegging in het kader Wet Verbetering Poortwachter	Tot twee jaar na einde dienstverband of vijf jaar bij eigenrisicodragerschap
Verslagen van functionerings- en beoordelingsgesprekken, arbeidsovereenkomsten en wijzigingen hierin, correspondentie over benoeming, promotie, degradatie en ontslag, afspraken over werkzaamheden voor de ondernemingsraad, getuigschriften en administratieve verzuimgegevens.	Tot einde dienstverband

### Leveranciers

Soort gegevens	Bewaartermijn
Facturen in verband met omzetbelasting	Zeven jaar vanaf dag van opstellen
Debiteuren- en crediteurenadministratie	Zeven jaar vanaf 1 januari van het jaar na opstellen

### Klanten

Als we ten aanzien van de gegevens zijn aan te merken als verwerker, bepaalt de klant hoe lang we deze gegevens bewaren. Gebruikelijk is dit tot het einde van de afname van onze dienstverlening. Als we ten aanzien van de gegevens zijn aan te merken als verwerkingsverantwoordelijke, gelden de volgende bewaartermijnen:

Soort gegevens	Bewaartermijn
NAW-gegevens	7 jaar
Contactgegevens	7 jaar
Kopie paspoort	7 jaar
Kopie aangiftes	7 jaar
Correspondentie	7 jaar
Salarisstroken/salarisinformatie	7 jaar
Betaalgegevens	7 jaar
Facturen in verband met omzetbelasting	Zeven jaar vanaf dag van opstellen
Debiteuren- en crediteurenadministratie	Zeven jaar vanaf 1 januari van het jaar na opstellen

## Overig

Soort gegevens	Bewaartermijn
Contactgegevens websitebezoekers	Tot één jaar na afhandelen contact
Cookies website	Afhankelijk van de gebruikte cookies tussen direct na einde bezoek website en tot één jaar daarna.
Camerabeelden bezoekers pand	Tot vier weken na opname
Bezoekersregistratie	Tot één week na bezoek

Bij alle andere gegevens die je gebruikt en dus zelf opslaat, is het van belang dat je zelf controleert of deze gegevens verwijderd moeten worden. Verwijder direct e-mails die niet langer noodzakelijk zijn, en loop minimaal eens per kwartaal de inbox van je werkmail na om de niet noodzakelijke e-mails te verwijderen. Belangrijke e-mails kunnen bewaard blijven en opgeslagen worden in specifieke mappen, alle andere e-mails moeten verwijderd worden. Door dit periodiek te doen, voorkom je dat e-mails onnodig eindelijk bewaard blijven.

Hetzelfde geldt uiteraard voor alle andere digitale documenten die op jouw computer/laptop zijn opgeslagen en tevens voor papieren documentatie. Zorg ervoor dat alle papieren documenten die nog noodzakelijk zijn, op de juiste wijze zijn opgeborgen zoals bijvoorbeeld in een afgesloten kast. Alle papieren documenten die niet meer noodzakelijk zijn, dienen direct versnipperd te worden. Zorg ook dat papieren documentatie minimaal eens per kwartaal wordt nagelopen om te controleren of alle documenten écht noodzakelijk zijn om te bewaren.

### 1.8 Verwijderen van gegevens

Het is mogelijk dat wij in opdracht van een klant gegevens moeten verwijderen van hem of haar, bijvoorbeeld omdat hij/zij geen gebruik meer wil maken van onze diensten. Denk bijvoorbeeld aan iemand die een verzoek indient om zijn/haar e-mailadres uit onze database te verwijderen, omdat hij/zij geen nieuwsbrief meer wenst te ontvangen. Het verwijderen van (een grote hoeveelheid) gegevens (niet enkel persoonsgegevens) wordt uitgevoerd door C.M. Heeroms. Zo kunnen wij erop toezien dat het verwijderen van gegevens volgens de juiste regels wordt uitgevoerd.

Voor het verwijderen van gegevens waarvoor jij zelf moet bepalen of deze nog noodzakelijk zijn of niet (zie ook paragraaf 1.7), zoals jouw e-mails of papieren documenten, ben jij zelf verantwoordelijk. Zorg ervoor dat papieren documenten met persoonsgegevens, die niet meer noodzakelijk zijn, versnipperd worden, of op een andere veilige wijze verwijderd worden.

Wat betreft digitale documenten, dien je er zorg voor te dragen dat deze verwijderd worden uit de mailbox, of van de door jou gebruikte apparatuur.

Draag er daarnaast zorg voor dat er geen werkgerelateerde documenten op eigen (privé) apparatuur terecht komen, bijvoorbeeld door het downloaden van bestanden uit je werkmail op jouw eigen laptop.

## Hoofdstuk 2 – Beveiligen van gegevens

### 2.1 Beveiligingsmaatregelen en handleidingen

Indien er persoonsgegevens worden verwerkt verplicht de wet dat deze gegevens beschermd worden tegen verlies of onrechtmatige verwerking. Om de gegevens op een juiste manier te beveiligen worden er binnen de organisatie verschillende maatregelen toegepast.

Dit kunnen technische maatregelen zijn, zoals het gebruik van Transport Layer Security (TLS) op onze websites en een beveiligde interne verbinding. C.M. Heeroms ziet er op toe dat deze beveiligingsmaatregelen goed worden uitgevoerd en up-to-date zijn.

Daarnaast is het van belang dat alle medewerkers zelf de juiste maatregelen nemen om ongeoorloofde toegang, of het verlies van data te voorkomen. Er kunnen namelijk veel technische maatregelen gehanteerd worden om gegevens te beveiligen, maar zolang medewerkers niet bewust omgaan met de beveiliging van gegevens kan het alsnog misgaan.

Let daarom op de volgende punten tijdens je dagelijkse werkzaamheden:

1. Laat je scherm nooit onbeveiligd achter als je je werkplek verlaat. Ook al verlaat je je werkplek maar voor heel even, zorg ervoor dat je altijd je scherm vergrendeld hebt. Doe je dit niet, dan kan iemand met een kwade wil zichzelf zonder enige moeite toegang verschaffen tot onze systemen.

2. Gebruik sterke wachtwoorden en zorg er ook voor dat al jouw apparatuur met een wachtwoord beveiligd is.

Een aantal tips voor het gebruik van wachtwoorden:

- Gebruik geen wachtwoorden zoals 1234, je eigen naam, geboortedatum of woonplaats. Ook geen combinatie hiervan zoals Marie1985 maar wissel af met tekens, hoofdletters en cijfers.
- Gebruik geen woorden uit het woordenboek. Hackers kunnen namelijk gebruik maken van zogenaamde ‘dictionary attacks’ waarbij alle woorden uit het woordenboek worden uitgetest als wachtwoord. Weet dit daarom te voorkomen door niet één eenvoudig woord als wachtwoord te gebruiken.
- Deel inloggegevens niet met een ander, ook niet met een kennis. Schrijf je inloggegevens ook niet op bijvoorbeeld een briefje en deel ze niet in een e-mail. Wil je toch ergens je wachtwoord noteren, zorg er dan voor dat dit nooit doet in de buurt van je computer.
- Gebruik niet overal hetzelfde wachtwoord voor.

3. Zorg ervoor dat je computer of laptop niet pal voor een raam staat. Zo voorkom je dat mensen ongevraagd mee kunnen kijken, maar zo voorkom je ook mogelijke diefstal.

4. Indien je gebruik maakt van werkapparatuur, zoals een laptop of mobiele telefoon, gebruik je werkapparatuur dan voor zover mogelijk uitsluitend voor werkdoeleinden. Zorg er bovendien voor dat C.M. Heeroms, jouw apparatuur gecontroleerd heeft op beveiliging.

5. Indien je buiten jouw werkomgeving gebruik maakt van privé- en/of werkapparatuur om werkzaamheden voor ExpatTeam te verrichten, maak dan geen verbinding met een

openbaar Wi-Fi netwerk zoals bijvoorbeeld in de trein, of in openbare ruimtes. Zo voorkom je dat er via een onbeveiligd netwerk toegang verkregen wordt tot jouw apparatuur.

5. Accepteer enkel bijlagen van e-mails indien je zeker weet dat dit van een betrouwbare afzender afkomt en het een betrouwbaar bestand is. Hetzelfde geldt voor het openen van links naar websites die zijn opgenomen in e-mails en dergelijke berichten afkomstig van derden.

## **2.2 Beperkte toegang tot gegevens**

Een andere wijze om de gegevens te beschermen is door het hanteren van beperkte toegang tot de gegevens. Om deze reden hebben medewerkers van Expatteam slechts toegang tot de systemen en gegevens die nodig zijn voor het uitvoeren van een specifieke functie.

Toegang gaat op basis van een gecontroleerde autorisatie waardoor het mogelijk is te herleiden wie er precies toegang heeft verkregen. Op deze manier wordt misbruik en/of fraude met gegevens beperkt.

De aanvraag van een (tijdelijke) autorisatie verloopt altijd via C.M. Heerrooms. Wil je toegang tot een specifieke database, of jouw autorisatie wijzigen? Dan kun je contact opnemen met C.M. Heerrooms.

## **2.3 Datalek**

Ondanks de beveiligingsmaatregelen die binnen ExpatTeam worden gehanteerd, kan een kans op ongeautoriseerde toegang tot gegevens of verlies en/of diefstal van gegevens (een datalek) nooit volledig worden uitgesloten. Een datalek kan zich op verschillende wijzen voordoen. Denk bijvoorbeeld aan een laptop die gestolen wordt, papieren dossiers die bij de verkeerde persoon terecht komen, het verzenden een e-mail met daarin persoonsgegevens naar de verkeerde ontvanger of iemand die onrechtmatig toegang verkrijgt tot onze systemen.

Om de betrouwbaarheid van Expatteam hoog te houden, vragen wij alle medewerkers alert te zijn op mogelijke verdachte zaken en/of overtredingen. Met onze beveiligingsmaatregelen en de medewerking van het personeel wordt de kans op een datalek verkleind. Meld het daarom direct indien apparatuur is kwijtgeraakt of gestolen (doe dit ook wanneer het privé apparatuur betreft, maar je hierop wel je werk e-mail hebt geïnstalleerd). Laat het ons uiteraard ook weten wanneer er zich andere situaties voordoen waarbij persoonsgegevens mogelijk gelekt zijn, zoals een verloren USB-stick, klachten van klanten of vreemde meldingen in systemen.

Mocht een dergelijke situatie zich voordoen, laat dit dan direct weten aan C.M. Heerrooms. Wij zullen controleren of het een lek is dat wij moeten melden aan de toezichthouder en/of de betrokken personen.

## **Hoofdstuk 3 – Rechten van betrokkenen**

Voor iedereen van wie wij persoonsgegevens verwerken is in de privacy- en cookieverklaring op onze websites beschreven wat ze kunnen verwachten bij het gebruik van onze websites en diensten, wat wij met hun gegevens doen en wat hun rechten zijn.

Betrokkenen hebben volgens de wet verschillende rechten. Zo heeft men bijvoorbeeld het recht bij ons zijn of haar gegevens op te vragen, deze in te zien en/of deze te laten wijzigen en/of verwijderen of te verplaatsen naar een andere belastingadviespraktijk. Daarnaast wordt, voor de mailings, in elke e-mail altijd een afmeldmogelijkheid opgenomen.

Deze aanvragen komen in de eerste instantie bij C.M. Heerrooms terecht. Indien je de vraag van iemand krijgt om inzage in gegevens te verlenen, of deze te wijzigen of te verwijderen, dan kun je deze aanvraag doorzetten naar C.M. Heerrooms.

Wanneer een dergelijk verzoek binnenkomt, verifieer dan altijd of de verzoeker wel is wie hij zegt te zijn. Vraag bijvoorbeeld naar aanvullende identificerende gegevens zoals een adres of geboortedatum. Zo wordt voorkomen dat aan de verkeerde persoon persoonsgegevens worden afgegeven (dit is namelijk weer aan te merken als een datalek!).

#### **Hoofdstuk 4 – Contact**

Wij doen ons best toegankelijk en beschikbaar te zijn voor al jouw vragen of meldingen omtrent privacy en beveiliging. Indien er sprake is van een overtreding, verlies of diefstal van gegevens of indien je verdachte zaken constateert, vragen wij jou hier direct een melding van te maken.

Voor dergelijke meldingen en/of vragen is C.M. Heeroms het aanspreekpunt, en persoonlijk bereikbaar of via e-mail en telefoon.

Indien een privacy- of beveiligingsprobleem actief is binnen onze organisatie, zullen wij dit aan alle medewerkers doorgeven. Hierbij kunnen tips, advies en mogelijk te nemen maatregelen medegedeeld worden. Op deze manier proberen wij de medewerkers up-to-date te houden en actief te betrekken.