# Privacy beleid

# Inhoudsopgave

# 1 Inleiding

Het beveiligen van persoonsgegevens is steeds belangrijker geworden, en de introductie van de Algemene Verordening Gegevensverwerking (AVG) betekent dat bedrijven serieus met privacy om moeten gaan.

De beleidsregels in dit Privacy Beleid helpen TMI om zo goed als mogelijk te voldoen aan vereisten uit de AVG en de richtlijnen hieromtrent van de Autoriteit Persoonsgegevens (AP).
Dit TMI Privacy beleid zal elk jaar worden herzien en eventueel aangepast en wordt gecommuniceerd binnen de gehele organisatie.

De Functionaris Gegevensverwerking (FG) is verantwoordelijk voor het Privacy Beleid binnen TMI.

# 2 Definities

- **Persoonsgegeven**: elk gegeven betreffende een geïdentificeerd of identificeerbare, individuele natuurlijke persoon;
- **Verantwoordelijke:** de natuurlijke persoon of rechtspersoon die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
- **Verwerker:** degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
- **Betrokkene:** degene op wie een persoonsgegeven betrekking heeft;
- **Verwerking van persoonsgegevens:** elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens (oa verzamelen, wijzigen, gebruiken, doorzending, verspreiding, met elkaar in verband brengen, uitwissen of vernietigen van gegevens).

# 3 Privacy uitgangspunten

## 3.1 Transparantie

Informeer de kandidaat tijdig en volledig over het gebruik van zijn gegevens.

Een kandidaat wiens gegevens worden verwerkt, moet kunnen nagaan wat er met die gegevens gebeurt. Daarom moet hij worden geïnformeerd over (in ieder geval) de identiteit van de verantwoordelijke (TMI) en de doeleinden waarvoor de gegevens worden verzameld en verwerkt.

TMI verstrekt deze informatie op haar website door middel van haar privacy verklaring. Zorg ervoor dat kandidaten altijd op het privacy statement worden gewezen vóórdat zij (nieuwe) gegevens aan TMI verstrekken. De kandidaat moet namelijk voorafgaand aan de verwerking worden geïnformeerd. De informatie moet op zodanige wijze worden verstrekt dat de kandidaat daadwerkelijk de beschikking over de informatie krijgt. Een algemene verwijzing naar elders verkrijgbare informatie is dus niet voldoende. Zorg ook dat de privacy policy (website) door de kandidaat kan worden geprint en opgeslagen.

Als persoonsgegevens via een andere weg worden verkregen, dus buiten de kandidaat om, dan moet de kandidaat worden geïnformeerd (i) op het moment dat de gegevens worden vastgelegd, of (ii) als de gegevens worden verzameld om aan een derde te verstrekken. De plicht tot informeren geldt uiterlijk op het moment van de eerste verstrekking aan die derde.

## 3.2 Doelbinding

Persoonsgegevens mogen alleen worden verzameld en gebruikt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. Er mogen bovendien niet meer gegevens worden verwerkt dan voor het doel noodzakelijk is (Data minimalisatie). Verwerk dus geen overbodige gegevens. Zorg er aan de andere kant wel voor dat ook weer niet te weinig gegevens worden verwerkt, omdat hierdoor een onvolledig beeld van de kandidaat kan ontstaan.

Zorg voor een goed overzicht van persoonsgegevens die in uw organisatie verwerkt worden, waarom deze worden verwerkt en op welke grondslag deze verwerking kan worden gebaseerd.

Als het voornemen bestaat gegevens die al beschikbaar zijn voor een ander/nieuw doeleinde te gebruiken, check dit dan altijd met de Functionaris Gegevensbescherming. Mogelijk moet de privacy statement en/of de melding bij de Autoriteit Persoonsgegevens worden aangepast of moet toestemming worden verkregen van de kandidaat.

## 3.3 Rechtmatige grondslag

Het verwerken van persoonsgegevens mag alleen gebeuren als daar een rechtmatige grondslag voor is.

**Toestemming** kan bijvoorbeeld worden verkregen door een apart vakje in te voegen dat de kandidaat moet aanvinken (“ja, ik geef toestemming voor ...”). Het is niet toegestaan een dergelijk hokje alvast voor de kandidaat aan te vinken, dit moet door de gebruiker zelf (actief) gedaan worden (Active opt-in). Houd er rekening mee dat een toestemming altijd weer moet kunnen worden ingetrokken. Na het intrekken van de toestemming zal de verwerking moeten worden beëindigd.

Als gegevens voor een ander doeleinde worden gebruikt dan waarover kandidaten zijn geïnformeerd voordat zij toestemming gaven, dan moet opnieuw toestemming worden verkregen van de kandidaat.

Voor sommige gegevensverwerkingen is geen toestemming nodig van de kandidaat of werknemer omdat er een **wettelijke grondslag** is voor het verzamelen van die gegevens. Denk hierbij aan persoonsgegevens die HR nodig heeft voor de personeelsadministratie en de salaris uitbetaling.

## 3.4 Bijzondere persoonsgegevens en persoonsnummers

Als er geen wettelijke bepaling is die aan TMI verplichtingen oplegt of de bevoegdheid verleent om persoonsnummers zoals BSN-nummers te gebruiken, is het verwerken daarvan niet toegestaan (HR is een wettelijke uitzondering).

Voor gegevens die extra gevoelig kunnen zijn, zoals gegevens over godsdienst of levensovertuiging, ras (welke kan worden afgeleid uit een profielfoto en nationaliteit, die daarom ook als bijzondere persoonsgegevens gelden), politieke gezindheid, gezondheid, seksuele leven, het lidmaatschap van een vakvereniging en/of strafrechtelijke persoonsgegevens geldt dat deze in principe alleen mogen worden verwerkt als daarvoor uitdrukkelijke toestemming is verkregen, tenzij een specifieke uitzondering van toepassing is.

## 3.5 Recht op inzage, correctie en verwijdering

Iedereen heeft het recht om met redelijke tussenpozen aan TMI te vragen of, en zo ja welke persoonsgegevens van hem/haar worden verwerkt (hieronder vallen ook gegevens die zijn opgeslagen door TMI, maar nergens voor worden gebruikt). Op een dergelijk verzoek van de kandidaat om inzage moet binnen 30 dagen worden geantwoord.

Het antwoord moet in begrijpelijke vorm een overzicht van de verwerkte gegevens van de kandidaat bevatten. Daarnaast dienen ook (i) het doel of de doeleinden van de verwerking, (ii) de categorieën van gegevens, (iii) de (categorieën van) ontvangers en (iv) alle beschikbare informatie over de herkomst van de gegevens, te worden medegedeeld aan de kandidaat.

Kandidaten kunnen ook verzoeken om hun gegevens te corrigeren. Het verzoek hoeft slechts te worden ingewilligd als de gegevens feitelijk onjuist, onvolledig of niet relevant zijn voor het doel van de verwerking. Uiterlijk binnen vier weken moet worden aangeven aan de kandidaat of, en zo ja in hoeverre, aan het correctieverzoek gehoor wordt gegeven. Een weigering tot correctie moet gemotiveerd worden.

Tenslotte kan een kandidaat ook een verzoek indienen tot het laten verwijderen van zijn persoonsgegevens door TMI. Ook op dit verzoek dient binnen 30 dagen gehoor te worden gegeven. Hierbij dienen alle persoonlijke gegevens van de kandidaat in alle gegevensverwerkingen bij TMI en bij gerelateerde Verwerkende partijen te worden verwijderd. Het recht op verwijdering geldt niet voor die persoonsgegevens die wettelijk gezien bewaard moeten worden (voor een bepaalde termijn).

## 3.6 (ICT) Beveiliging

Persoonsgegevens moeten op “passende wijze” worden beveiligd. De AVG specificeert niet welke maatregelen er precies genomen moeten worden. Wel geldt in het algemeen: hoe gevoeliger de gegevens, hoe zwaarder de toegepaste beveiliging moet zijn.

Dit geldt bijvoorbeeld voor bijzondere/extra gevoelige persoonsgegevens, zoals gegevens over iemands financiële, economische of medische situatie, gegevens die betrekking hebben op mensen uit kwetsbare groepen en gebruikersnamen en/of wachtwoorden.

De Autoriteit Persoonsgegevens heeft richtsnoeren gepubliceerd voor de beveiliging van persoonsgegevens. In het algemeen dient in ieder geval het volgende stappenplan aan te worden gehouden:

- Beoordeel de risico’s. Inventariseer de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen daarvan en de kans dat deze gevolgen zich zullen voordoen.
- Maak gebruik van algemeen geaccepteerde beveiligingsnormen, zoals de NEN - ISO 27002 richtlijnen;
- Controleer en evalueer regelmatig of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Pas, waar nodig, de beveiligingsmaatregelen aan.
- In de praktijk zijn de volgende (beveiligings-)maatregelen in ieder geval gebruikelijk:
- Het hebben van een informatiebeveiligingsbeleid en het toewijzen van een verantwoordelijke voor informatiebeveiliging;
- Procedures op gebied van IT Incidentenbeheer en Continuiteitsbeheer;
- Beveiligingsbewustzijn voor alle medewerkers, o.a. door regelmatige training;
- Het afschermen van specifieke pagina’s met persoonsgegevens voor zoekmachines;
- Het gebruik van wachtwoorden om de doelgroep af te bakenen, al dan niet in combinatie met andere (fysieke) herkenningsmiddelen;
- Het beveiligen van het gegevenstransport, bijvoorbeeld door gebruik te maken van gesloten, beveiligde verbindingen;
- Het versleutelen van persoonsgegevens (encryptie);
- Het beveiligen van de machine(s) en achterliggende databases/ computersystemen tegen onbevoegde toegang door derden, bijvoorbeeld door het gebruik van authenticatiemiddelen;
- Het gescheiden opslaan van gegevens en het instellen van toegangscontrole;
- Logging en controle van activiteiten die gebruikers uitvoeren met persoonsgegevens;

- Het zoveel mogelijk aggregeren / anonimiseren / pseudonimiseren van gegevens. Zorg voor een protocol ‘datalekken’ dat gevolgd kan worden in het geval een inbreuk op de beveiliging plaatsvindt. Let op: indien gebruik wordt gemaakt van een verwerker, dan moet de verantwoordelijke ervoor zorgen dat ook deze voldoende beveiligingsmaatregelen treft.

## 3.7 Doorgeven van gegevens naar landen buiten de EU

Doorgifte van persoonsgegevens naar landen buiten de EU (waaronder ook wordt begrepen het opslaan van persoonsgegevens op servers buiten de EU) is alleen toegestaan onder bepaalde voorwaarden.

Een van de volgende situaties moet van toepassing zijn:

- Het betreffende land waarborgt een passend niveau van privacybescherming. Op de website van de AP kan worden nagegaan of er sprake is van een passend niveau;
- Indien het een doorgifte naar de VS betreft: het bedrijf waaraan de gegevens worden doorgegeven heeft de status verworven van “safe harbor”;
- Er wordt gebruikt gemaakt van een ongewijzigd modelcontract van de Europese Commissie;
- De kandidaat heeft ondubbelzinnige toestemming gegeven voor de doorgifte.

## 3.8 Bewaartermijnen

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor zij zijn verzameld.
De Autoriteit Persoonsgegevens vereist dat:

1. Per doeleinde is onderbouwd welke bewaartermijnen worden gehanteerd;
2. Deze termijnen niet langer zijn dan noodzakelijk; en
3. De termijnen zijn vastgelegd en geïmplementeerd in de interne bedrijfsprocessen.

**Let op:** Soms kan het ook juist noodzakelijk zijn om iemands gegevens wél te bewaren, bijvoorbeeld om ervoor te zorgen dat aan diegene géén mailingen meer worden verstuurd als iemand een opt-out daarvoor heeft gegeven.

## 3.9 Verwerkers en verwerkersovereenkomst

Alle partijen die in opdracht van TMI kandidaat gegevens verwerken (zoals technische dienstverleners als hosting providers, of marketing of HR partijen) moeten een verwerkersovereenkomst tekenen.

De verantwoordelijke (TMI) moet erop toezien dat de overeenkomst met de bewerker wordt nageleefd. In deze overeenkomst moeten in ieder geval de volgende bepalingen zijn opgenomen:

- De verplichting voor de verwerker om de persoonsgegevens uitsluitend te verwerken in opdracht van de verantwoordelijke en het afgesproken doel;

- De verplichting tot het nemen van adequate beveiligingsmaatregelen;
- De verplichting tot geheimhouding en vertrouwelijkheid;
- De verplichting tot het melden van eventuele datalekken op de kortst mogelijke termijn.

## 3.10 Versturen van commerciële berichten per e-mail / SMS / sociale media

Voor het versturen van commerciële berichten moet toestemming middels een opt-in van de geadresseerde zijn verkregen, tenzij onderstaande uitzondering van toepassing is. In ieder bericht moet bovendien de mogelijkheid tot een opt-out worden geboden.

Indien sprake is van een bestaande kandidaat-relatie dan mogen berichten aan kandidaten zonder opt-in worden verstuurd, mits aan de volgende voorwaarden is voldaan:

- Deze kandidaten moeten op het moment dat TMI hun contactgegevens verkrijgt worden geïnformeerd over i) het feit dat zij berichten van TMI zullen ontvangen en ii) om wat voor berichten het zal gaan, iii) daarbij moet tegelijk de mogelijkheid tot opt-out wordt geboden;
- In ieder verstuurd bericht wordt de mogelijkheid tot opt-out geboden
- De berichten bevatten alleen informatie over producten of diensten van TMI die vergelijkbaar zijn met de producten en diensten in het kader waarvan kandidaten hun contactgegevens hebben verstrekt. Er mogen dus bijvoorbeeld geen advertenties van derden in nieuwsbrieven worden geplaatst.

## 3.11 Cookies

Onder cookies verstaat de wet alle informatie die wordt geplaatst op, of wordt uitgelezen van randapparatuur van eindgebruikers (ook mobiele apparaten).

Voor het gebruik van cookies is voorafgaande, geïnformeerde toestemming nodig, tenzij de cookies technisch noodzakelijk zijn.

## 3.12 Informatie verstrekken aan (overheids)instanties

Indien TMI te maken krijgen met een verzoek van een bepaalde instantie, bijvoorbeeld politie, belastingdienst of toezichthouders, om informatie te verschaffen over een kandidaat, relatie of medewerker, dan hoeft TMI daar niet altijd automatisch aan mee te werken. Op basis van verschillende wet- en regelgeving zal u hieraan al dan niet invulling moeten geven (Algemene wet bestuursrecht, Wet politiegegevens, Belastingwet, Telecomwet en uiteraard de Wet bescherming persoonsgegevens).

Over het algemeen kan gesteld worden dat gegevens waarvoor de Officier van Justitie een schriftelijke vordering heeft afgegeven, dienen te worden overlegd. Daarnaast is in de fiscale wetgeving een zogenoemde informatieplicht opgenomen. Je bent in principe verplicht om mee te werken. Toch heeft de inspecteur hierbij niet alle vrijheid. Bij weigering zal er een informatiebeschikking volgen.

# 4 Privacy organisatie en maatregelen om aan de AVG te voldoen

## 4.1 Privacy office

TMI heeft twee medewerkers tot Functionaris Gegevensbescherming (FG) benoemd en aangemeld in het Register bij de Autoriteit Persoonsgegevens. De FG heeft een officiële functie en takenlijst en rapporteert rechtstreeks aan de Directeur. De FG kan worden gecontacteerd op fg@tmi-interim.nl.

## 4.2 Verwerkingsregister

TMI heeft een verwerkingsregister opgesteld waarin alle verschillende verwerkingen van persoonsgegevens zijn geregistreerd. Per gegevensverwerking zijn onder andere de volgende zaken geïnventariseerd:

- Welke persoonsgegevens er worden verwerkt;
- Wat de bewaartermijn is;
- Welke verwerkende partij eventueel betrokken is;
- Of er een verwerkersovereenkomst is gesloten met de verwerkende partij;
- Welk systeem/tool er betrokken is bij de gegevensverwerking;
- Wat de rechtmatige grondslag is voor de verwerking;
- Etc.

Het verwerkingsregister dient altijd up-to-date te zijn en wordt bijgehouden en aangevuld/gewijzigd door de FG.

## 4.3 Procedure datalekken

Binnen TMI is er een procedure datalekken ontwikkeld en gecommuniceerd. In deze procedure wordt omschreven welke acties er door wie binnen de organisatie dienen te worden genomen bij (het vermoeden van) een datalek. Hiermee wordt ondervangen dat de meldingstermijn van 72 uur wordt overschreden.

## 4.4 Privacy beleid en Privacy statement

TMI heeft haar Privacy activiteiten en uitgangspunten vastgelegd in dit Privacy beleid. Een afgeleide van het Privacy beleid is het Privacy statement, die op de website van TMI is te vinden. In de Privacy statement staat exact welke gegevens er worden verzameld en voor welke doeleinden. Daarnaast worden er een aantal uitgangspunten toegelicht, zoals bewaartermijnen en IT-beveiligingsmaatregelen.

## 4.5 Privacy bewustzijn medewerkers

Om er voor te zorgen dat alle medewerkers van TMI zich voldoende bewust zijn van de AVG en de consequenties hiervan op hun werk heeft TMI de volgende maatregelen genomen:

- Privacy documentatie wordt gecommuniceerd - Zowel dit Privacy Beleid als de procedure Datalekken is naar alle medewerkers gecommuniceerd, en elke medewerker wordt geacht zich aan deze privacy regels te houden;

- Alle kantoor medewerkers hebben een AVG-bewustwording training gevolg, en hun aanwezigheid bij de training is vastgelegd. De sheets van de training zijn verspreid onder de medewerkers. De training zal ook worden gebruikt voor toekomstige nieuwe medewerkers;

## 4.6 ICT-beveiliging

TMI heeft een informatiebeveiligingsbeleid dat voldoet aan de richtlijnen zoals genoemd in 3.6 van dit privacy beleid.

Daarnaast wordt de werking van het informatiebeveiligingsbeleid ieder jaar onafhankelijk getoetst en beoordeeld.