

Privacy Policy MASTUM bv

1. INLEIDING

MASTUM bv verzamelt en verwerkt persoonlijke informatie van haar klanten, leveranciers en personeel. Voor MASTUM bv (hierna te noemen: MASTUM) is het beschermen van de privacy een belangrijk doel en MASTUM zet zich in voor het respecteren van de privacy en het op gepaste wijze beschermen van de persoonsgegevens.

Het waarborgen van de naleving van de algemene verordening gegevensbescherming vormt de basis van betrouwbare zakelijke relaties en is essentieel voor de reputatie van MASTUM als een aantrekkelijke zakenpartner en werkgever. Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht en is zij van toepassing op MASTUM en op iedereen die in opdracht van MASTUM persoonsgegevens verwerkt.

Het privacy beleid ('Beleid') definieert de aanpak van MASTUM om de bescherming en het beheer van persoonsgegevens in overeenstemming met de AVG te waarborgen en biedt duidelijke richtlijnen voor éénieder die zich bezighoudt met de verwerking van persoonsgegevens in opdracht van MASTUM.

Het doel van dit Beleid bestaat erin om de persoonsgegevens te beschermen door de betrokkenen instructies te geven over het verzamelen en het verwerken van deze persoonsgegevens.

Dit Beleid is bijkomstig aan, en vervangt noch vernietigt, specifieke vereisten inzake gegevensbescherming of regels met betrekking tot de vertrouwelijkheid die van toepassing kunnen zijn op een specifiek bedrijfsdomein of functie, ingevolge de hierop van toepassing zijnde wetgeving.

2. TOEPASSINGSGBIED

Dit Beleid is geschreven voor MASTUM en voor éénieder die persoonsgegevens verwerkt in opdracht van MASTUM, inclusief werknemers, studenten, stagiaires, uitzendkrachten, zelfstandige medewerkers, onderaannemers, freelancers en aandeelhouders. Dit Beleid is bedoeld voor één ieder uit elke discipline die professionele diensten verstrekt aan klanten alsook voor één ieder die interne diensten verstrekt.

3. DEFINITIES

Persoonsgegevens zijn alle gegevens met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon ('betrokkene'). Als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een gegeven zoals een naam, een identificatienummer, locatiegegevens, een online gegeven of één of meerdere elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijk persoon. Gevoelige Persoonsgegevens zijn persoonsgegevens in verband met een natuurlijke persoon waaruit zijn ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, gezondheid, seksueel gedrag, seksuele geaardheid, genetische en biometrische gegevens blijken, enkel en alleen met het doel de persoon te identificeren. Verwerking betekent een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Verwerkingsverantwoordelijke betekent een

natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Verwerker is een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Europa betekent, voor de doeleinden van dit Beleid, “de Europese Economische Ruimte en Zwitserland”. Gegevensverwerkingsovereenkomst betekent een overeenkomst of elk ander type juridisch instrument dat voorwaarden bevat met betrekking tot de verwerking van persoonsgegevens, als onderdeel van een overeenkomst voor professionele diensten. Inbreuk in verband met persoonsgegevens betekent een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

4. PRINCIPES VOOR DE VERWERKING VAN PERSOONSGEGEVENS

Zoals hierboven aangehaald, is het doel van dit Beleid om richtlijnen te verschaffen met betrekking tot het correct verwerken van Persoonsgegevens. Ongeacht welk type van Persoonsgegevens wordt verwerkt en ongeacht op welke manier deze Persoonsgegevens worden verwerkt moet éénieder de volgende 8 basisprincipes naleven:

4.1 Persoonsgegevens moeten rechtmatig en behoorlijk verwerkt worden

Persoonsgegevens moeten verzameld en verwerkt worden op een rechtmatige en behoorlijke wijze. In praktijk betekent dit dat MASTUM:

- een gerechtvaardigde en wettelijke basis moet hebben voor het verzamelen en gebruiken van Persoonsgegevens;
- transparant moet zijn over de manier waarop de Persoonsgegevens verwerkt zullen worden, en natuurlijke personen (klanten, werknemers of andere) voldoende moet inlichten over hun privacy rechten wanneer hun Persoonsgegevens worden verzameld;
- moet omgaan met Persoonsgegevens op een manier die redelijkerwijze verwacht kan worden;
- zich ervan moet verzekeren dat de Persoonsgegevens niet op een onwettige manier gebruikt worden.

4.2 Persoonsgegevens moeten verzameld worden voor uitdrukkelijk omschreven doeleinden en niets anders

Persoonsgegevens moeten verzameld worden voor uitdrukkelijk omschreven doeleinden. In de praktijk betekent dit dat MASTUM:

- vanaf het begin duidelijk dient te zijn over welke Persoonsgegevens verzameld worden en voor welke doeleinden deze gebruikt zullen worden;
- zich ervan moet verzekeren dat, indien de Persoonsgegevens voor andere dan de aanvankelijk omschreven doeleinden gebruikt worden, de betrokken persoon hiervan in kennis wordt gesteld en het gebruik gerechtvaardigd is.

4.3 Persoonsgegevens moeten toereikend, ter zake dienend en beperkt te zijn tot wat noodzakelijk is

Persoonsgegevens moeten toereikend zijn, ter zake dienend zijn en beperkt zijn tot wat noodzakelijk is. In praktijk betekent dit dat MASTUM zich ervan moet verzekeren dat:

- er enkel Persoonsgegevens worden gevraagd en verzameld die relevant zijn voor een specifiek doeleinde;
- er niet meer Persoonsgegevens mogen worden bijgehouden dan nodig voor een specifiek doeleinde.

4.4 Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd

Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd. Onnauwkeurige en verouderde gegevens moeten worden verwijderd of aangepast. In de praktijk betekent dit dat MASTUM:

- moet zorgen dat de bron van de Persoonsgegevens duidelijk is;
- redelijke stappen dient te ondernemen om zich ervan te verzekeren dat de verkregen Persoonsgegevens juist zijn;
- moet nagaan of het nodig is de Persoonsgegevens te actualiseren.

4.5 Persoonsgegevens mogen niet langer bewaard worden dan nodig

Persoonsgegevens mogen niet langer bewaard worden dan nodig is. Van zodra de persoonsgegevens niet meer nodig zijn voor het doeleinde waarvoor zij verzameld werden, dient deze informatie gewist te worden, tenzij er een andere basis is om deze Persoonsgegevens te bewaren. In de praktijk betekent dit dat MASTUM:

- de duur voor het bijhouden van Persoonsgegevens zal moeten nagaan;
- zal moeten overwegen voor welk doel de Persoonsgegevens worden bijgehouden en hoe lang de Persoonsgegevens hiervoor dienen te worden bijgehouden;
- de Persoonsgegevens op een veilige manier dient te wissen indien zij niet meer noodzakelijk is voor het vooropgestelde doel.

4.6 Persoonsgegevens moeten verwerkt worden overeenkomstig de individuele rechten

Persoonsgegevens moeten verwerkt worden rekening houdend met de rechten van natuurlijke personen, met name:

- het recht om geïnformeerd te worden
- het recht op inzage
- het recht op rectificatie
- het recht op wissing van gegevens
- het recht op beperkte Verwerking
- het recht op gegevensoverdraagbaarheid
- het recht om bezwaar te maken
- rechten gebaseerd op automatische beslissingen en profilering. Elke betrokkene waarvan Persoonsgegevens worden verwerkt, heeft deze rechten. Voor verdere verduidelijking in dit verband verwijzen we naar hoofdstuk 4.7.

4.7 Persoonsgegevens moeten op een veilige wijze bewaard worden

Persoonsgegevens moeten op een veilige wijze bewaard worden. In de praktijk betekent dit dat MASTUM de beveiliging dient te organiseren in overeenstemming met de aard van de Persoonsgegevens (werknemers, partners, klanten of andere) die bewaard worden en de mogelijke schade die kan voortvloeien uit een inbreuk op de beveiliging.

4.8 Persoonsgegevens mogen niet overgedragen worden aan derde landen zonder toereikende bescherming

Persoonsgegevens mogen niet overgedragen worden aan andere landen buiten Europa zonder toereikende bescherming. Dit betekent dat MASTUM:

- zorgvuldig dient na te gaan of de overdracht naar een land buiten Europa nodig is en of er een toereikende bescherming zal zijn vooraleer de Persoonsgegevens over te dragen;
- dient te zorgen voor toereikende bescherming bij de overdracht van Persoonsgegevens buiten Europa.

5. PERSOONSGEGEVENS BIJ MASTUM EN RICHTLIJNEN OM DEZE TE BESCHERMEN

De meeste Persoonsgegevens die we verwerken zijn deze van onze klanten, leveranciers, sollicitanten, werknemers, zelfstandigen en onderaannemers. Hieronder worden de belangrijkste categorieën van Persoonsgegevens opgelijst die verwerkt worden en de doeleinden waarvoor deze verwerkt worden.

5.1 Klantengegevens

We verzamelen en verwerken de Persoonsgegevens van onze klanten en onderscheiden hierbij drie types van 'Verwerking':

- om onze diensten te kunnen verstrekken;
- voor administratieve doeleinden (facturatie, overeenkomsten, wettelijke vereisten);
- voor commerciële doeleinden.

Persoonsgegevens verkregen van onze klanten voor het verstrekken van onze diensten

Er worden Persoonsgegevens verwerkt in het kader van de overeenkomst die de klant met ons heeft afgesloten. Wanneer we diensten verstrekken aan onze klanten ontvangen en verwerken we Persoonsgegevens van hun werknemers, hun leveranciers en hun klanten (bijvoorbeeld huurders). Dit is het geval bij de meeste diensten. Bij sommige diensten, worden Persoonsgegevens op regelmatige basis verwerkt. Dit is bijvoorbeeld het geval bij salarisverwerking, waar gegevensbescherming nog meer aandacht verdient. Wanneer we Persoonsgegevens verwerken van onze klanten om onze diensten te verstrekken, zijn we een zogenaamde 'verwerker' van Persoonsgegevens. Bijgevolg dient de Gegevensverwerkingsovereenkomst duidelijk de rol en verantwoordelijkheden te bepalen met betrekking tot de Verwerking van Persoonsgegevens. Deze Gegevensverwerkingsovereenkomst wordt standaard toegevoegd aan de algemene voorwaarden van onze overeenkomsten met onze klanten. Alleen verantwoordelijken voor de klant krijgen toegang tot en kunnen de Persoonsgegevens van de klant raadplegen in het kader van de verstrekking van diensten aan de klant. De toegang tot klantgegevens wordt geregistreerd en 'ongeoorloofde toegang' tot Persoonsgegevens zal gerapporteerd worden. Verder dienen we ons ervan te verzekeren dat de Persoonsgegevens zorgvuldig behandeld worden. In concreto betekent dit dat:

- De gegevens goed beschermd dienen te worden: toereikende beschermingsmaatregelen dienen genomen te worden om ervoor te zorgen dat enkel 'geautoriseerde' personen toegang hebben tot de gegevens en dat er geen ongeoorloofde toegang mogelijk is.
- De gegevens moeten met de nodige zorgvuldigheid behandeld worden, er dienen maatregelen genomen te worden om te voorkomen dat de gegevens verloren geraken (bijvoorbeeld: het verlies van USB stick, laptops, papieren dossiers).
- Gegevens mogen enkel gekopieerd worden op andere systemen, apparaten (bijvoorbeeld laptops) of locaties wanneer dit werkelijk vereist is. Gekopieerde gegevens dienen eveneens beschermd te worden.
- Wij delen deze gegevens niet met andere partijen (extern of binnen ons netwerk), tenzij met de expliciete toestemming van de klant.
- Wij vragen en verzamelen enkel Persoonsgegevens van onze klanten die echt nodig zijn voor de te bereiken doeleinden, we informeren de klant over deze doeleinden en zullen de Persoonsgegevens enkel gebruiken voor deze doeleinden.
- Wij bewaren de Persoonsgegevens enkel zo lang wij deze nodig hebben. Het archiveringsbeleid zal in dit opzicht bekeken worden. Voor sommige diensten wordt dit bepaald door regelgeving en professionele richtlijnen.

Het dient opgemerkt te worden dat sommige van deze principes niet alleen relevant zijn voor 'Persoonsgegevens' maar voor 'gegevens in het algemeen' die we van onze klanten ontvangen.

Persoonsgegevens verzameld van onze klanten voor administratieve doeleinden

Voordat wij diensten leveren aan nieuw klanten, zijn wij ingevolge onze acceptatieprocedures verplicht om bepaalde gegevens van de klant te verzamelen. Sommige van deze gegevens zijn Persoonsgegevens, zoals contactgegevens, informatie met betrekking tot het bestuur, kopieën van identiteitskaarten (in het kader van anti-witwaswetgeving). Deze gegevens worden bijgehouden in onze systemen. Gelet op de gevoeligheid dienen deze gegevens goed beschermd te worden. Zodra wij onze diensten leveren, worden deze gegevens gebruikt voor facturatie en administratieve doeleinden en worden zij bijgehouden in onze interne ERP systemen en databanken. Onze klanten verwachten dat wij deze gegevens bijhouden om onze diensten aan hen te kunnen verstrekken. Deze gegevens betreffen voornamelijk administratieve gegevens. Het gevoeligheidsniveau is derhalve eerder beperkt. We dienen er echter zorg voor te dragen dat wij deze gegevens up-to-date houden en dienen te voorkomen dat deze publiek beschikbaar worden.

Persoonsgegevens verzameld voor commerciële doeleinden voor bestaande klanten en prospecten

We bewaren ook klantgegevens voor commerciële doeleinden in ons CRM systeem. Dit omvat gegevens van onze bestaande klanten, ex-klanten en prospecten. Deze gegevens worden gebruikt om commerciële opportuniteiten op te volgen, alsook voor direct marketing en mailings. De klant moet geïnformeerd worden met betrekking tot het gebruik van zijn/haar gegevens voor commerciële doeleinden. Indien de klant het gebruik van zijn/haar gegevens niet toestaat voor commerciële doeleinden kunnen de gegevens hier ook niet langer voor gebruikt worden. De beste praktijk bestaat erin dat de toestemming een positieve actie van de betrokken persoon vereist (bijvoorbeeld: het aanvinken van een vakje in een formulier).

Voor bestaande klanten is het toegestaan contactgegevens te gebruiken voor doeleinden van direct marketing aangezien we reeds een contractuele overeenkomst hebben met hen. Het belangrijkste

aandachtspunt bestaat erin dat we geen boodschappen aan klanten meer toesturen indien zij er voor geopteerd hebben geen direct marketing boodschappen meer te ontvangen (een zogenaamde 'optout'). Wanneer klanten voor deze 'opt-out' opteren mogen zij niet meer gecontacteerd worden. Persoonsgegevens van prospecten en ex-klanten kunnen enkel verwerkt worden op basis van hun toestemming.

Persoonsgegevens die worden achtergelaten door individuen op de website mogen verwerkt worden teneinde hen relevante informatie te verstrekken over onze diensten. Indien we hen direct marketing boodschappen willen sturen die niet gelinkt zijn aan hun vragen moeten we hiervoor hun expliciete toestemming verkrijgen.

5.2 Gegevens van sollicitanten

We verzamelen en verwerken Persoonsgegevens van potentiële kandidaten voor rekruteringsdoeleinden. In het rekruteringsproces worden Persoonsgegevens van sollicitanten ontvangen (bijvoorbeeld wanneer individuen hun CV uploaden op de website of hun CV via e-mail toesturen). De Persoonsgegevens van sollicitanten zullen bestaan uit identificatiegegevens en gegevens over onderwijs en opleiding. Deze gegevens kunnen verwerkt worden op basis van de toestemming van de sollicitant in kwestie en kan gedeeld worden met personen betrokken bij het rekruteringsproces binnen MASTUM.

De gegevens mogen niet gedeeld worden met andere partijen buiten MASTUM. Indien de sollicitant wordt aangeworven dienen zijn/haar gegevens verwerkt te worden in het kader van de arbeidsrelatie of de zelfstandige samenwerking. Indien de sollicitant wordt afgewezen, dienen zijn/haar gegevens gewist te worden met inachtneming van de vereiste retentieperiode, tenzij de sollicitant ermee heeft ingestemd dat zijn/haar gegevens bewaard blijven met het oog op toekomstige rekruteringsprocessen.

5.3 Gegevens van werknemers

We verzamelen en verwerken Persoonsgegevens van onze eigen werknemers voor HR doeleinden. Alle organisaties, inclusief MASTUM, beheren Persoonsgegevens van hun werknemers ten behoeve van salarisadministratie, evaluatie en loopbaanontwikkeling. De privacy verklaring voor werknemers verduidelijkt de gegevens verwerkt door MASTUM, alsook hun doeleinden en de rechten van de betrokkenen. Specifieke richtlijnen zijn verstrekt aan de interne HR afdeling om deze gegevens op de juiste wijze te beheren.

5.4 Gegevens zelfstandigen en onderaannemers

We verzamelen en verwerken Persoonsgegevens van de zelfstandigen en onderaannemers voor facturatie doeleinden. De gegevens worden gebruikt voor facturatie en administratieve doeleinden en worden bijgehouden in onze interne ERP systemen en databanken. De privacy verklaring voor zelfstandigen en onderaannemers verduidelijkt de gegevens verwerkt door MASTUM, alsook hun doeleinden en de rechten van de betrokkenen. Specifieke richtlijnen zijn verstrekt aan de interne boekhouding afdeling om deze gegevens op de juiste wijze te beheren.

6. INBREUK IN VERBAND MET PERSOONSgegevens

Als organisatie die Persoonsgegevens verwerkt, heeft MASTUM de verplichting om bepaalde inbreuken met betrekking tot Persoonsgegevens te melden aan de bevoegde toezichthoudende overheid uiterlijk 72 uur nadat zij er kennis van genomen heeft. MASTUM moet eveneens een

register bijhouden met Inbreuken op Persoonsgegevens. Een inbreuk op Persoonsgegevens bevat meer dan louter het verliezen van Persoonsgegevens.

Een inbreuk in verband met Persoonsgegevens betekent een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Voorbeelden van inbreuken op Persoonsgegevens zijn:

- het verlies van een USB stick, documenten of GSM;
- het versturen van Persoonsgegevens naar een fout of ongewenst adres (bijvoorbeeld via e-mail);
- computerapparatuur die Persoonsgegevens bevat en die verloren raakt of wordt gestolen;
- het verliezen van een hard copy bestand;
- het openen van een bijlage van een e-mail met virus die ertoe leidt dat de computerapparatuur niet meer beschikbaar is;
- het verkeerd reageren op fishing pogingen die leiden tot het openbaar maken van wachtwoorden.

7. WIE TE CONTACTEN BIJ VRAGEN OF BEDENKINGEN?

Indien u vragen of bedenkingen heeft met betrekking tot dit Beleid kunt u contact opnemen met privacy@mastum.nl