Privacyconvenant

Gemeente Haarlem

&

Paswerk & Werkpas holding BV

Inhoudsopgave

Privacyconvenant tussen gemeente Haarlem en Paswerk & Werkpas Holding.

Contractpartijen:

1. Verwerkingsverantwoordelijke te weten: gemeente Haarlem.
   KvK-nummer: 34369366
   statutair gevestigd te: Grote Markt 2, 2011 RD Haarlem
   vertegenwoordigd door: mw. C. Lenstra, gemeentesecretaris-algemeen directeur, namens het college van burgemeester en wethouders van de gemeente Haarlem

hierna te noemen: **'Verwerkingsverantwoordelijke 1'**,

en

2. Verwerkingsverantwoordelijke te weten: Paswerk & Werkpas Holding BV.
   KvK-nummers: 34340686 / 34139650
   statutair gevestigd te: Spieringweg 835, 2130 AG Cruquius
   vertegenwoordigd door: dhr. C. Boon, algemeen directeur

hierna te noemen: **'Verwerkingsverantwoordelijke 2',**

gezamenlijk aan te duiden als: '**Partijen**';

Overwegende dat:

Partijen hebben verschillende dienstverleningsovereenkomsten gesloten. Ter uitvoering van deze Overeenkomsten worden Persoonsgegevens verwerkt. Partijen hechten grote waarde aan het beschermen van deze Persoonsgegevens. Om die reden leggen Partijen in dit Privacyconvenant, hierna te noemen 'het Convenant", de wederzijdse verantwoordelijkheden vast in de gevallen waarin persoonsgegevens tussen partijen worden gedeeld. Het Convenant is van toepassing in de volgende gevallen:

- in het kader van een gegevensuitwisseling waarbij Partijen ieder voor hun eigen deel verwerkingsverantwoordelijk zijn en partijen afspraken rond de gegevensbescherming wensen te maken zoals bedoeld in artikel 24 van de AVG;
- in het kader van gezamenlijke verwerkingsverantwoordelijkheid zoals bedoeld in artikel 26 van de AVG;
- in het kader van een verwerkersrelatie tussen partijen zoals bedoeld in artikel 28 van de AVG waarbij verwerkingsverantwoordelijke 2 als verwerker kan worden aangemerkt.

1. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

1. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de Betrokkene‘); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

2. Verwerking: 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.

3. Gezamenlijke verwerkingsverantwoordelijkheid: wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijk verantwoordelijk.

4. Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verantwoordelijke is of volgens welke criteria deze wordt aangewezen.

5. Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegevens betrekking hebben.

6. Overeenkomsten: de hoofdovereenkomsten zijnde de dienstverleningsovereenkomsten tussen beide partijen waarop dit Convenant van toepassing is.

7. Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (**‘Datalek’**).

8. Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

9. Register van Verwerkingen: registratie van verwerkingen volgens artikel 30 van de AVG

2. Totstandkoming, duur en beëindiging

a. Dit Convenant treedt in werking op de datum waarop Partijen dit Convenant ondertekenen.

b. Dit Convenant is onderdeel van alle Overeenkomsten en zal gelden voor zolang de Overeenkomsten duren.

c. Indien een der Overeenkomsten eindigt, eindigt dit Convenant automatisch voor desbetreffende Overeenkomst; het Convenant kan niet apart worden opgezegd.

d. Na beëindiging van dit Convenant zullen de lopende verplichtingen, zoals het melden van Datalekken waarbij Persoonsgegevens van Partijen zijn betrokken en de plicht tot geheimhouding blijven voortduren.

e. Na het beëindigen van dit Convenant verwijderen Partijen de persoonsgegevens met het in acht nemen van doelen en bewaartermijnen.

3. Verwerken Persoonsgegevens

a. Partijen verwerken Persoonsgegevens conform de Europese Privacywetgeving en volgens afspraken die in dit Convenant zijn overeengekomen. Zij zullen Persoonsgegevens niet op een andere manier verwerken, tenzij Partijen dit gezamenlijk overeenkomen.

b. Partijen dienen te beschikken over een actueel Register van Verwerkingen. In het Register van Verwerkingen van Partijen is opgenomen welke persoonsgegevens, voor welk doel en op welke grondslag tussen Partijen wordt gedeeld.

c. Partijen houden zich bij het verwerken van Persoonsgegevens aan de wettelijke grondslag en de gegevens worden verwerkt op een behoorlijke, zorgvuldige en transparante wijze.

d. Partijen mogen zonder voorafgaande schriftelijke toestemming van elkaar geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens in het kader van de Overeenkomsten. De eventuele verwerkers worden opgenomen in het Register van Verwerkingen

e. Wanneer Partijen met toestemming van elkaar andere organisaties inschakelen, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in dit Convenant.

f. Wanneer Partijen een verzoek van een Betrokkene ontvangen ten aanzien van het uitoefenen van zijn of haar rechten, zullen Partijen voor het deel waar zij verantwoordelijk voor zijn, zorgen dat de Betrokkene zijn of haar rechten effectief kan uitoefenen. Deze rechten bestaan uit een verzoek om inzage, correctie, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens. Partijen zijn zelf verantwoordelijk om de betrokkenen hierover te informeren.

g. Partijen dienen op duidelijke en eenvoudige wijze te communiceren waar de Betrokkene voor het uitoefenen van zijn rechten terecht kan. Hierbij geven partijen aan welke

Medeverwerkingsverantwoordelijken er zijn en wie voor welk deel verantwoordelijk is.

4. Exporteren Persoonsgegevens

Partijen mogen geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van de andere Medeverwerkingsverantwoordelijke.

5. Geheimhouding

a. Partijen zullen de verstrekte Persoonsgegevens geheimhouden, tenzij dit op basis van een wettelijke verplichting niet kan.
b. Partijen zorgen ervoor dat het personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-)contracten op te nemen. De geheimhouding geldt ook na beëindiging van het Convenant.

6. Beveiliging en Datalekken

a. Partijen zorgen voor passende technische en organisatorische maatregelen. De wijze waarop Partijen de passende technische en organisatorische maatregelen aantonen staan in Bijlage 2.

b. Partijen informeren elkaar uiterlijk binnen 24 na vaststelling van een (vermoedelijk) Datalek en treffen de nodige maatregelen. Partijen zullen elkaar op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek (zie bijlage 1). Ook zullen Partijen de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan elkaar.

c. Partijen doen elk voor dat deel waar zij verantwoordelijk voor zijn de melding van een Datalek bij de Toezichthouder voor zover dit nodig is. Hetzelfde geldt voor de melding aan de Betrokkenen.

d. Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van de partij die het ontstaan en/of het laten voortduren van het Datalek heeft veroorzaakt.

7. Aansprakelijkheid

a. Als één van de Partijen de verplichtingen uit dit Convenant of de (privacy-)wetgeving niet nakomt, kunnen zij voor de daaruit vloeiende schade aansprakelijk gesteld worden.

b. Partijen vrijwaren elkaar over en weer voor alle schades, claims, eisen, acties, schikkingen, rente, kosten, procedures, uitgaven, verliezen en/of opgelegde bestuursrechtelijke sancties, zoals, maar niet beperkt tot, bestuurlijke boetes en of (verbeurde) dwangsommen, in verband met het niet (tijdig en/of correct) nakomen door een Partij van de afspraken op grond van dit Convenant en/of het handelen of nalaten van een Partij en/of diens Subverwerkers in strijd met de privacywetgeving.

8. Verwerkersrelatie

Indien er naar aanleiding van één der Overeenkomsten sprake is van een verwerkersrelatie tussen partijen waarbij Verwerkingsverantwoordelijke 2 moet worden aangemerkt als verwerker in de zin artikel 28 van de AVG, is het Convenant van overeenkomstige toepassing. In aanvulling op de bepalingen van het Convenant gelden in geval van een verwerkersrelatie nog de aanvullende bepalingen die zijn opgenomen in bijlage 3.

9. Slotbepalingen

a. Het Convenant is onderdeel van de Overeenkomsten. Alle rechten en verplichtingen uit deze Overeenkomsten zijn daarom ook van toepassing op dit Convenant.

b. Bij eventuele tegenstrijdigheden tussen de bepalingen in dit Convenant en de Overeenkomsten, ten aanzien van de verwerking van Persoonsgegevens, gelden de bepalingen uit dit Convenant.

c. Afwijkingen van dit Convenant zijn slechts geldig wanneer Partijen dit samen schriftelijk overeenkomen.

d. Op verzoek van een van de partijen stellen zij binnen redelijke termijn alle benodigde informatie aan elkaar ter beschikking omtrent de nakoming van de afspraken in dit convenant.

e. Op dit Convenant is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Overeenkomsten.

Aldus door Partijen overeengekomen en ondertekend:

Verwerkingsverantwoordelijke 1 :
Ondertekend voor en namens gemeente Haarlem
Naam: mw. C. Lenstra
Functie: gemeentesecretaris-algemeen directeur gemeente Haarlem
Datum en plaats:
Handtekening:

Verwerkingsverantwoordelijke 2:
Ondertekend voor en namens Paswerk & Werkpas Holding
Naam: dhr. C. Boon
Functie: algemeen directeur
Datum en plaats:
Handtekening:

Bijlage 1: Proces rondom het melden van Datalekken

Waar meld je het datalek?
Als en van de Partijen een datalek constateert, dienen zij binnen 24 uur contact op te nemen met de andere partij:

Verwerkingsverantwoordelijke 1:
Naam: mw. C. Konijnenbelt
FG gemeente Haarlem en Zandvoort
Telefoon: 023-5113064
E-mail:fg@haarlem.nl

Verwerkingsverantwoordelijke 2:
Naam: dhr. F.J. Duyne
FG Paswerk en Werkpas Holding B.V.
Telefoon: 06-30480642
E-mail: fg@paswerk.nl

De onderstaande vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt wanneer er van het Datalek een melding gemaakt moet worden.

De volgende vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/Datalek: wat is er gebeurd?
   Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen Persoonsgegevens zijn betrokken bij het beveiligingsincident?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het beveiligingsincident?
   Geef a.u.b. een minimum en maximum aantal personen.
4. Omschrijving groep personen om wiens gegevens het gaat.
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend?
   Het kan zijn dat Betrokkenen geïnformeerd moeten worden over het Datalek, kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
   Geef dit a.u.b. zo specifiek mogelijk aan.

Bijlage 2: Aantonen passende technische en organisatorische maatregelen

Verwerkingsverantwoordelijke 1:

Informatiebeveiligingsbeleid (technische en organisatorische maatregelen):

De informatiebeveiliging vindt plaats volgens algemeen erkende overheidsnorm zijnde de Baseline Informatiebeveiliging Overheid (BIO). De BIO omvat technische en organisatorische normen en te nemen maatregelen.
De BIO gaat uit van de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat zij op voorhand keuzes en continu afwegingen maken of informatie in bestaande en nieuwe processen adequate beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

De gemeente onderschrijft de 10 principes voor informatiebeveiliging. De 10 principes zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die het college aan zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur;

2. Informatiebeveiliging is van iedereen;

3. Informatiebeveiliging is risicomanagement;

4. Risicomanagement is onderdeel van de besluitvorming;

5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;

6. Informatiebeveiliging is een proces;

7. Informatiebeveiliging kost geld;

8. Onzekerheid dient te worden ingecalculeerd;

9. Verbetering komt voort uit leren en ervaring;

10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. De betrokkenheid van het bestuur is essentieel, en laat zien

dat de gemeente informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Naast het informatiebeveiligingsbeleid zijn er nog de volgende maatregelen:

- Privacybeleid en privacyreglement;
- Geheimhoudingsplicht medewerkers opgenomen in de ambtseed voor ambtenaren of integriteitsverklaring voor niet-ambtenaren;
- Protocol (procesbeschrijving) datalekken;
- Privacy- en cookiestatement op website;
- Bewustwording medewerkers

Verwerkingsverantwoordelijke 2:

Technische maatregelen.

De volgende technische maatregelen zijn genomen om oneigenlijk gebruik van gegevens tegen te gaan:

- Informatiebeveiligingsbeleid (IB-beleid);

Het IB-beleid is gebaseerd op de 'Code voor Informatiebeveiliging' (NEN/ISO 27001 en 27002) en in lijn met de geldende wet- en regelgeving welke van toepassing zijn op de gemeenschappelijke regeling Werkvoorzieningsschap Zuid-Kennemerland, Paswerk & Werkpas Holding BV en haar werkmaatschappijen.
Het IB-beleid is vastgesteld en goedgekeurd door de directie. De directie herijkt tweejaarlijks, of na grote organisatorische veranderingen, het IB-beleid op aangeven en advies van de verantwoordelijke Manager en de Functionaris Gegevensbescherming (FG) en het continue veranderende risico-landschap.
Het IB-beleid past de drie principes toe van Beschikbaarheid, Integriteit en Vertrouwelijkheid:

- Beschikbaarheid: Informatie, middelen en diensten zijn beschikbaar en toegankelijk voor geautoriseerde individuen, afdelingen en/of processen op de momenten dat daar vraag naar is.
- Integriteit: Informatie, middelen en diensten zijn accuraat en compleet en worden beschermd tegen oneigenlijke en ongeautoriseerde aanpassingen.
- Vertrouwelijkheid: Informatie, middelen en diensten zijn enkel beschikbaar voor de daarvoor geautoriseerde individuen, afdelingen en/of processen

Het IB-beleid is een risico gebaseerde benadering. Beveiligingsmaatregelen worden getroffen op basis van een risicoanalyse.

Organisatorische maatregelen.

De volgende organisatorische maatregelen zijn genomen om oneigenlijk gebruik van gegevens tegen te gaan:

- Privacybeleid en privacyreglement;
- Protocol geheimhoudingsplicht medewerkers;
- Integriteitsverklaring;
- Protocol datalekken;
- Privacy- en cookiestatement op website;
- Bewustwording medewerkers;

Bovenstaande organisatorische maatregelen zijn in lijn met de Europese Privacy Wetgeving (AVG).

Bijlage 3: Aanvullende bepalingen Verwerkersrelatie

Indien er naar aanleiding van één der Overeenkomsten sprake is van een verwerkersrelatie tussen partijen waarbij Verwerkingsverantwoordelijke 2 moet worden aangemerkt als verwerker in de zin artikel 28 van de AVG, is het Convenant van overeenkomstige toepassing.
In aanvulling op de bepalingen van het Convenant gelden in geval van een verwerkersrelatie nog de volgende bepalingen. Deze bepalingen zijn in lijn met bepalingen van de VNG Standaard verwerkersovereenkomst.

1. Onderwerp van deze Verwerkersovereenkomst

a. Verwerkingsverantwoordelijke 2 verwerkt in de rol als verwerker in de zin van de AVG de door of via Verwerkingsverantwoordelijke 1 ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke 1 voor de uitvoering van de Overeenkomsten en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke 1.
b. Het bepaalde in voornoemd lid is niet van toepassing indien een op Verwerkingsverantwoordelijke 2 van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerkingsverantwoordelijke 2, voorafgaand aan de verwerking, de Verwerkingsverantwoordelijke 1 daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
c. De door Verwerkingsverantwoordelijke 2 uit te voeren verwerkingen staan beschreven in een tabel zoals in deze bijlage beschreven. De ingevulde tabel wordt als bijlage gevoegd bij de betreffende (hoofd-) overeenkomst die onderdeel uitmaakt van de Overeenkomsten.

2. Beveiliging en Datalekken

a. In aanvulling van artikel 6 van het Convenant verleent Verwerkingsverantwoordelijke 2
b. alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen het Convenant, deze aanvullende verwerkersovereenkomst en Bijlagen, tenzij Verwerkingsverantwoordelijke 2 door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat de gemaakte afspraken worden nagekomen. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke 1 (zowel eigen kosten als kosten van Verwerkingsverantwoordelijke 2), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerkingsverantwoordelijke 2 constateert die ten nadele zijn van Verwerkingsverantwoordelijke 1.
c. Op verzoek van Verwerkingsverantwoordelijke 1 werkt Verwerkingsverantwoordelijke altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.
d. In geval van een Datalek beslist Verwerkingsverantwoordelijke 1 of het Datalek moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerkingsverantwoordelijke 2 ondersteunt de Verwerkingsverantwoordelijke 1 waar nodig bij de melding aan de Toezichthoudender en/of Betrokkenen.

Formulier overzicht Verwerkingen, te voegen bij de hoofdovereenkomst

Op de verwerkingen is van toepassing:

- het Convenant tussen gemeente en Paswerk & Werkpas Holding;
- bijlage 3 bij het Convenant, Aanvullende bepalingen Verwerkersrelatie.

verwerking, doeleinden categorieën van betrokkenen, soort persoonsgegevens en eventuele doorgifte naar derde landen.

Naam verwerking	Verwerkings-doeleinden	Categorieën van Betrokkenen	Categorie Persoonsgegevens (waaronder bijzondere persoonsgegevens)	Doorgifte naar derde landen

Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen	Toepassing