

Bijlagen

- I. Protocol klachtbehandeling
- II. Privacybeleid juni, RADAR 2017
- III. Figuur 1, informatieverstrekking (website RADAR)
- IV. Observatie en gespreksverslag klachtbehandelaar Rotterdam
- V. Observatie en gespreksverslag klachtbehandelaar Brabant
- VI. Mailcorrespondentie bedrijfsbureau
- VII. Observatie en gespreksverslag Rotterdam-Brabant
- VIII. Conclusie observaties en gesprekken
- IX. Offerte Constant-IT
- X. Interview RADAR team onderzoek
- XI. E-mail encryptie
- XII. Stappenplan bewustwording privacy voor klachtbehandelaars
- XIII. Model verwerkersovereenkomst
- XIV. Privacy statement
- XV. Privacy-gegevensbeschermingsbeleid RADAR
- XVI. Toestemmingsformulier

I. Protocol Klachtbehandeling

1. Inleiding

Het protocol klachtbehandeling geeft de wijze aan waarop RADAR klachten behandelt.

De klachtbehandeling van RADAR heeft de volgende doelen:

1. Ondersteuning van gedupeerden
2. Bevordering van de zelfredzaamheid
3. Signalering van structurele patronen van discriminatie
4. Gedrags- en/of beleidsbeïnvloeding van personen of organisaties die zich bedoeld of onbedoeld schuldig hebben gemaakt aan discriminatie, gericht op voorkomen van herhaling
5. Toetsen van wetgeving
6. Ontwikkeling van jurisprudentie

1.1 Discriminatie

Onder discriminatie verstaan we gevallen en gevoelens waarbij personen of groepen op grond van voor de context irrelevante kenmerken (het vermoeden hebben) ongelijk (minder) behandeld (te) worden of uitgesloten worden.

Als uitgangspunt wordt de in Nederland geldende antidiscriminatie- en gelijke behandelingswetgeving gebruikt.

1.2 Melding

Onder een melding wordt een incident verstaan dat bij RADAR onder de aandacht wordt gebracht door slachtoffer, getuige of intermediair.

1.3 Klacht

Onder een klacht wordt elke melding verstaan waarbij RADAR door betrokkene of een getuige wordt gevraagd om advies en/of ondersteuning.

1.4 Werkgebied

Het werkgebied van RADAR omvat gemeenten in de regio's Rotterdam-Rijnmond, Midden- en West-Brabant, delen van Brabant-Noord en Zuid-Holland-Zuid.

Inwoners van gemeenten binnen het werkgebied die niet zijn aangesloten bij RADAR worden doorverwezen naar het bestuur van de betreffende gemeente.

2. Indiening melding of klacht

Inleiding

Voor het indienen van klachten is RADAR op werkdagen tussen 9.00 en 17.00 uur telefonisch bereikbaar. Meldingen die per mail/website/antwoordapparaat binnenkomen, kunnen 24 uur per dag, 7 dagen in de week ingediend worden.

2.1 Telefonisch

In het geval van een telefonische melding of klacht worden in ieder geval de persoonlijke gegevens alsmede een korte omschrijving van de klacht opgenomen en wordt de cliënt indien mogelijk te woord gestaan door een klachtbehandelaar, indien dit niet mogelijk is, wordt de cliënt dezelfde dag of de werkdag erna teruggebeld.

2.2 Persoonlijk

In het geval een cliënt zich persoonlijk bij RADAR meldt met een klacht worden in ieder geval de persoonlijke gegevens alsmede een korte omschrijving van de klacht opgenomen en wordt de cliënt indien mogelijk te woord gestaan door een klachtbehandelaar. Indien dit niet mogelijk is, wordt de cliënt dezelfde dag of de werkdag erna teruggebeld.

2.3 Antwoordapparaat, e-mail, brief of digitaal klachtenformulier (website)

Cliënten die zich melden via het antwoordapparaat, de e-mail, een brief of het digitaal klachtenformulier worden dezelfde dag of de werkdag erna benaderd.

2.4 Klachten en meldingen met een spoedeisend karakter

Klachten en meldingen met een spoedeisend karakter dienen per ommegaande in behandeling te worden genomen. Het spoedeisende karakter is ter beoordeling aan de klachtbehandelaar.

2.5 'Conflict of interest'

Indien voor of tijdens de klachtbehandeling blijkt dat er sprake is van een 'conflict of interest' (over het incident waarover de klacht is ingediend blijkt door de wederpartij ook al een klacht ingediend), dan wordt de klacht in beginsel niet verder in behandeling genomen. Daar kan van afgeweken worden indien er mogelijkheden zijn tot bemiddeling. Indien dat niet mogelijk is zal de persoon in kwestie worden doorverwezen.

3. Eerste analyse en behandeling

Inleiding

Tijdens het eerste contact van de klachtbehandelaar met een cliënt beoordeelt de klachtbehandelaar, in samenspraak met de cliënt, of deze bij RADAR aan het juiste adres is. Indien dit niet het geval is, wordt de cliënt doorverwezen. Indien er mogelijkheden voor behandeling zijn, zijn er vier opties:

1. Registratie en luisterend oor
2. Eenmalig informatie of advies
3. Eigen actie RADAR op grond van melding
4. Ondersteuning en begeleiding cliënt

Bovengenoemde opties kunnen elkaar ook opvolgen. Wat begint als alleen een luisterend oor, kan eindigen met een procedure bij [het College voor de Rechten van de Mens](#).

3.1 Alleen registratie/luisterend oor

'Alleen registratie' houdt in dat de melding wordt opgenomen en geregistreerd. Er vinden geen vervolgacties plaats. De registratie is van belang omdat RADAR daarmee inzicht kan krijgen in structurele patronen van discriminatie.

In het geval van 'alleen registratie' vindt er in de meeste gevallen een gesprek plaats over het incident. Deze gesprekken nemen in de regel de nodige tijd in beslag. Zeker als het gaat om personen die zelf slachtoffer zijn van discriminatie. Voor hen is het feit dat ze gehoord worden heel belangrijk. Ze voelen zich daardoor meer ondersteund. Deze gesprekken zijn er ook op gericht het probleem te verhelderen zodat de cliënt er mee verder kan. Dit bieden van een 'luisterend oor' is dan ook een belangrijke taak van RADAR.

3.2 Eenmalige informatie en advies

Hierbij gaat het om het geven van informatie of advies aan een cliënt op basis waarvan deze zelf besluit al dan niet nadere stappen te ondernemen.

Doorgaans geldt dit o.a. voor zaken waarin cliënten aangeven zelf actie te willen ondernemen én zaken waarbij de klachtbehandelaar beoordeelt dat er waarschijnlijk geen sprake is van discriminatie.

3.3 Eigen actie op grond van melding

'Eigen actie' betreft al die zaken waarbij RADAR op eigen titel handelt.

3.4 Ondersteuning en begeleiding cliënt

Hierbij gaat het om die gevallen waarbij RADAR samen met cliënt vervolgstappen onderneemt. Daarbij kan het gaan om:

- Empowerment
- Bemiddeling
- Ondersteuning bij procedures
- Voorlichting en beleidsadvisering

4. Intakegesprek

Inleiding

Na de melding volgt soms een persoonlijk intakegesprek. In het geval van taalproblemen wordt gebruik gemaakt van een tolkenvoorziening. Voor het gesprek wordt gemiddeld een uur uitgetrokken. Indien nodig wordt een afspraak voor een vervolgesprek gemaakt.

De cliënt ontvangt informatie over de dienstverlening en wijze van klachtbehandeling van het RADAR. Tevens wordt de cliënt gevraagd relevante documenten mee te nemen.

Indien de klacht wordt ingediend via derden (familie of vrienden van het slachtoffer, getuigen of via een instantie) wordt aangegeven dat de zaak in de regel pas in behandeling kan worden genomen nadat het slachtoffer zelf contact heeft opgenomen met het ADB.

Het intakegesprek heeft de bedoeling:

1. De cliënt zijn of haar verhaal en gevoelens te laten uiten
2. Inzicht te krijgen in de aard van de klacht
3. Te bepalen wat de verwachtingen zijn die de cliënt heeft ten aanzien van de verdere behandeling van zijn of haar klacht
4. De cliënt te informeren over de werkwijze bij het behandelen van klachten
5. Afspraken te maken over het verdere verloop

De verschillende doelen van het intakegesprek worden hiernavolgend nader toegelicht.

4.1 Uiten van verhaal en gevoelens

Tijdens het intakegesprek krijgt de cliënt de tijd en ruimte om zijn of haar verhaal te doen.

4.2 Inzicht in de aard van de klacht

Tijdens het gesprek worden aantekeningen gemaakt over het incident. In elk geval worden persoonlijke gegevens genoteerd en alle mogelijke informatie over klacht (datum, tijdstip, plaats, betrokkenen, namen en adressen van eventuele getuigen). Er worden kopieën gemaakt van voor de klacht relevante documenten (correspondentie, inschrijvingsbewijzen, betalingsbewijzen, proces-verbaal en dergelijke). Indien deze niet zijn meegenomen dan wordt de cliënt verzocht deze zo snel mogelijk aan te leveren.

Er wordt geïnformeerd naar andere door de cliënt ingeschakelde instanties of eerder ondernomen stappen ten aanzien van deze specifieke klacht. Ook wordt gevraagd of de cliënt al eerder dezelfde klacht heeft gehad en welke stappen er toen zijn ondernomen. Als de cliënt zijn/haar verhaal heeft gedaan wordt de klacht samengevat en wordt gecontroleerd of de cliënt zich daarin kan vinden. Hierbij wordt aandacht besteed aan het discriminatieaspect, emotionele aspecten, praktische aspecten en structurele aspecten.

4.3 Verwachtingen cliënt

Nadat de klacht is geformuleerd, wordt de cliënt gevraagd wat zijn of haar concrete verwachtingen zijn ten aanzien van het eindresultaat van de klachtbehandeling. Zo nodig worden de meest voorkomende mogelijkheden genoemd.

Dit zijn op individueel niveau: een praktische oplossing van het probleem/conflict, excuses van de aangeklaagde partij, disciplinaire maatregelen, materiële/financiële tegemoetkoming of een gerechtelijke uitspraak.

Op structureel niveau kan het gaan om: voorlichting, beleidsbeïnvloeding, politieke of publicitaire aandacht, onderzoek naar soortgelijke klachten of collectieve actie.

De verwachtingen van de cliënt worden samengevat en er wordt gecontroleerd of deze zich daarin kan vinden.

4.4 Werkwijze

Het gesprek wordt voortgezet met een korte beschrijving van de werkwijze van RADAR. De cliënt wordt in de gelegenheid gesteld om nadere vragen te stellen naar aanleiding van de informatie over de werkwijze. De volgende zaken dienen in het gesprek voor zover van toepassing aan de orde te komen:

1. Principe van hoor en wederhoor
2. Vormen van ondersteuning
3. Beperkingen van RADAR
4. Procedure behandeling klacht
5. Klachtenreglement
6. Eigen verantwoordelijkheid cliënt
7. Kostenaspect
8. Registratie en privacybescherming

Hiernavolgend worden deze punten nader toegelicht.

4.4.1 Principe van hoor en wederhoor

In de eerste plaats moet worden gewezen op het principe van hoor en wederhoor. Dit principe betekent dat de wederpartij om diens visie op het gebeurde wordt gevraagd, voordat wordt besloten tot eventuele actie.

De cliënt dient te worden gewezen op het feit dat hoor en wederhoor tot gevolg kan hebben dat de naam van de cliënt bekend zal worden bij de aangeklaagde partij. De verhouding tussen de cliënt en de aangeklaagde partij is hierbij van belang. De cliënt moet gewezen worden op eventuele risico's zoals victimisatie.

In die gevallen dat de cliënt te kennen geeft (gezien de risico's) toch anoniem te willen blijven, zullen de bemoeienissen met de zaak door het ADB beperkt dienen te blijven tot het bieden van morele/emotionele ondersteuning, informatie en advies.

4.4.2 Vormen van ondersteuning

Het gaat bij de hoor-wederhoor procedure primair om het instellen van een onderzoek op basis waarvan RADAR kan overgaan tot bemiddeling, hulp bij een klachtenprocedure of hulp bij een juridische procedure. Bij het verlenen van ondersteuning heeft RADAR een zelfstandige rol bij de behandeling van de klacht op basis van ervaring en deskundigheid.

In het geval dat de cliënt het bureau vraagt om namens hem of haar de correspondentie te voeren dient de cliënt, of diens wettig vertegenwoordiger(s), een machtigingsformulier in te vullen. Hiermee verleent de cliënt RADAR toestemming om namens hem of haar op te treden.

Afhankelijk van de klacht kan RADAR ook ondersteuning bieden bij het verkrijgen van publicitaire en/of politieke aandacht voor de zaak, het opzetten van een onderzoek naar soortgelijke klachten, het ontwikkelen van voorlichtingsactiviteiten, het beïnvloeden van het beleid van een instelling en het organiseren van collectieve actie.

4.4.3 Beperkingen van RADAR

De cliënt dient op de beperkingen bij de behandeling van zijn of haar klacht te worden gewezen. Belangrijk is de cliënt te wijzen op het ontbreken van formele bevoegdheden. Indien een aangeklaagde persoon of instantie weigert mee te werken aan een onderzoek dan heeft RADAR geen mogelijkheden dit af te dwingen. In het geval van een civiele of strafrechtelijke procedure moet de cliënt, in verband met de verplichte procesvertegenwoordiging, geadviseerd worden een advocaat in te schakelen. Voor een procedure bij het College voor de Rechten van de Mens geldt het vereiste van verplichte procesvertegenwoordiging niet, hier kan RADAR de cliënt derhalve zonder tussenkomst van een advocaat ondersteunen.

RADAR kan ook geen ondersteuning bieden aan cliënten bij de verwerking van ernstige psychische problemen die voortvloeien uit de aard van de klacht. In dat geval dient de cliënt te worden gewezen op de mogelijkheid van ondersteuning door derden.

4.4.4 Procedure behandeling klacht

Er worden geen stappen ondernomen zonder toestemming van de cliënt.

In het geval RADAR besluit de zaak niet in behandeling te nemen, dan wel de behandeling te beëindigen, wordt de cliënt daarvan in kennis gesteld.

4.4.5 Klachtenreglement

De cliënt wordt gewezen op de mogelijkheid en de wijze waarop bezwaar kan worden gemaakt tegen het besluit zijn of haar klacht niet in behandeling te nemen. De cliënt wordt tevens geïnformeerd over de mogelijkheid een klacht in te dienen over de wijze waarop de zaak is behandeld.

4.4.6 Eigen verantwoordelijkheid cliënt

De cliënt wordt gewezen op de eigen verantwoordelijkheid die hij of zij heeft bij de aanpak van de klacht. RADAR adviseert en ondersteunt de cliënt bij het nemen van stappen, en kan ook namens de cliënt optreden. Cliënt en RADAR bepalen in onderling overleg welke stappen er ondernomen moeten worden. Van de cliënt wordt verwacht dat hij of zij de noodzakelijke documenten tijdig aanlevert. Indien de cliënt dit achterwege laat wordt hij/zij hiertoe nogmaals schriftelijk in de gelegenheid gesteld. Ontvangt RADAR opnieuw geen reactie, dan wordt de klacht afgesloten.

4.4.7 Kostenaspect

De ondersteuning die RADAR biedt is kosteloos voor inwoners van betalende gemeenten in het RADAR werk-gebied. De cliënt wordt echter gewezen op mogelijke kosten, indien hij of zij kiest voor bijvoorbeeld een juridische of geschillenprocedure.

- Een procedure bij het College voor de Rechten van de Mens is kosteloos.
- Bij een gerechtelijke procedure moet rekening gehouden worden met de kosten van een advocaat, griffierechten e.d.

4.4.8 Registratie en privacybescherming

De cliënt wordt geïnformeerd over de wijze van dossiervorming en hoe met deze gegevens wordt omgegaan. De persoonsgegevens blijven vertrouwelijk. De cliënt wordt verteld dat deze nooit zonder zijn of haar persoonlijke toestemming beschikbaar worden gesteld aan derden. De cliënt heeft na afspraak recht op inzage in het eigen dossier.

RADAR is gebonden aan de Wet Bescherming Persoonsgegevens.

4.4.9 Grensoverschrijdend gedrag

Bij grensoverschrijdend gedrag van cliënt heeft de klachtbehandelaar het recht om de klachtbehandeling te staken. Dit geldt bij alle contactmomenten. RADAR accepteert niet dat haar medewerkers onbeschoft, beledigend of discriminerend behandeld worden.

4.5 Concrete afspraken maken over verder verloop

Het gesprek wordt beëindigd met een samenvatting van de tijdens het gesprek gemaakte afspraken o.a. over aanvullende informatie die de cliënt nog dient aan te leveren. De cliënt wordt verzocht het materiaal binnen één week, dan wel zo spoedig mogelijk, aan te leveren. Ook worden zo nodig afspraken gemaakt over het opvragen van nadere informatie door RADAR bij derden.

5. Onderzoek

Inleiding

Er wordt na het intakegesprek een onderzoek ingesteld. Het onderzoek richt zich primair op het verkrijgen van aanvullend feitenmateriaal, verklaringen van getuigen, mogelijkheden van aanpak en procedures. Daarbij moet worden gekeken naar het discriminatieaspect, de praktische aspecten en mogelijk structurele oorzaken. Op basis van het onderzoek beslist de klachtbehandelaar of en op welke wijze de klacht kan worden behandeld.

5.1 Beslissing over verdere behandeling

Op basis van het onderzoek beslist de klachtbehandelaar of behandeling van de klacht mogelijk is en van welke strategie of strategieën gebruik kan worden gemaakt.

6. Aanpak

Inleiding

Op basis van de resultaten van het onderzoek en de gekozen strategie wordt een plan van aanpak opgesteld.

Hierin wordt aan de volgende aspecten aandacht besteed:

1. Beoogd resultaat
2. Plan
3. Termijn

6.1 Beoogd resultaat

Het beoogde resultaat wordt bepaald aan de hand van de bewijsbaarheid van discriminatie, de praktische hulpvraag en de structurele kant van de zaak. De gestelde doelen dienen haalbaar en toetsbaar te zijn.

De verwachtingen van de cliënt en de werkwijze van RADAR zijn uitgangspunt bij het vaststellen van het beoogde resultaat. Hierover dienen cliënt en RADAR consensus te bereiken. Indien er geen overstemming kan worden bereikt over het te behalen resultaat dient de behandeling te worden beëindigd. Zo mogelijk en gewenst wordt de cliënt in dat geval doorverwezen.

6.2 Plan

Op basis van het beoogde resultaat wordt een stappenplan opgesteld. Hierin komen de concrete stappen aan de orde die moeten worden ondernomen om het beoogde resultaat te bereiken en wat er nog nader moet worden onderzocht of nagevraagd voordat kan worden overgegaan tot het uitvoeren van de stappen.

In het plan wordt aangegeven wie welke stappen moet nemen: de cliënt, een andere instantie of RADAR. In het stappenplan wordt zo nodig opgenomen wat er dient te gebeuren indien de aangeklaagde persoon of instantie niet, afwijzend of positief reageert.

6.3 Termijn

In het plan wordt vastgelegd wat de termijnen zijn waarbinnen de door RADAR te nemen stappen moeten zijn gerealiseerd en wordt opgenomen binnen welke termijn een reactie wordt verwacht van de aangeklaagde persoon of instantie.

Uitgangspunt is dat een hoor en wederhoor brief binnen twee weken dient te worden beantwoord. Indien de brief niet is beantwoord, volgt een rappelbrief. Indien er opnieuw geen reactie volgt, wordt afhankelijk van het stappenplan bepaald wat de volgende stap dient te zijn.

6.4 Klachtbehandelaar

In principe wordt niet ingegaan op specifieke wensen van een cliënt ten aanzien van bijvoorbeeld geslacht van de klachtbehandelaar tenzij die wens in directe relatie staat tot de aard van de klacht (bijvoorbeeld een verzoek om een vrouwelijke dienstverlener in geval van seksuele intimidatie). Per geval zal worden beoordeeld of aan een dergelijk verzoek kan worden voldaan.

7. Uitvoering

Inleiding

Bij de uitvoering worden de volgende zaken in acht genomen.

1. Het verloop van de procedure
2. Termijnbewaking
3. Voortgangsbespreking met cliënt
4. Dossiervorming
5. Correspondentie
6. Afsluiting van de klacht

7.1 Het verloop van de procedure

RADAR zorgt ervoor dat de met de cliënt gemaakte afspraken worden nagekomen. Indien een gemaakte afspraak niet wordt nagekomen, dient dit te worden gemotiveerd richting de cliënt. Indien de cliënt bezwaar heeft tegen de gang van zaken kan deze daarover een klacht indienen.

Er wordt van de cliënt verwacht dat hij of zij de gemaakte afspraken nakomt. Indien de cliënt de gemaakte afspraken niet nakomt, wordt hij of zij gewezen op het feit dat dit ten koste kan gaan van het behalen van het beoogde resultaat en kan leiden tot beëindiging van de behandeling van de klacht.

Indien de cliënt de gemaakte afspraken niet nakomt, of niets van zich laat horen, wordt deze benaderd met het verzoek de gemaakte afspraken alsnog na te komen, dan wel contact op te nemen met RADAR.

7.2 Termijnbewaking

RADAR is verantwoordelijk voor het bewaken van de gestelde termijnen en zorgt ervoor dat de aangeklaagde persoon of instantie wordt geattendeerd op het overschrijden van een gestelde termijn.

Uitgangspunt daarbij is de termijn die wordt gehanteerd in de regeling van de organisatie waar de klacht aanhangig is gemaakt. Ook in het geval van een klachtenprocedure of een civiele of juridische procedure is de klachtbehandelaar verantwoordelijk voor het bewaken van de termijnen. Indien een termijn dreigt te worden overschreden, wordt de betreffende instantie daarop geattendeerd.

7.3 Voortgangsbespreking met cliënt

Er wordt op regelmatige basis contact onderhouden met de cliënt over de voortgang van de zaak. Indien in de loop van het proces blijkt dat het plan van aanpak moet worden bijgesteld, wordt hierover overleg gepleegd met de cliënt. Hierover dient opnieuw consensus te worden bereikt tussen de cliënt en RADAR.

7.4 Dossiervorming

Er wordt een dossier van de klacht aangelegd waarin alle documentatie is opgenomen. De documentatie betreft in elk geval het intakeverslag, verslagen van alle relevante gesprekken (telefonisch, persoonlijk), alle correspondentie, ontvangen alsmede verzonden documenten en het plan van aanpak. De cliënt heeft, na afspraak, inzage in zijn/haar dossier (zie ook 4.4.8).

7.5 Correspondentie

Van alle correspondentie die RADAR met de aangeklaagde partij voert, krijgt de cliënt een afschrift.

7.6 Afsluiting van de klacht

Een klacht wordt afgesloten:

- indien de cliënt geen verdere behandeling meer wenst;
- indien de cliënt, na rappel, niets meer van zich laat horen;
- indien RADAR vindt dat er niets meer te bereiken valt. RADAR zal dan tegenover de cliënt motiveren waarom dit het geval is en wijzen op de mogelijkheid een beroep te doen op de klachtenprocedure;
- indien RADAR het niet eens is met de wijze van klachtbehandeling die de cliënt voorstaat;
- indien het doel van de klachtbehandeling bereikt is.

Als een cliënt geen verdere behandeling wenst, wordt deze wens gerespecteerd. De cliënt wordt geïnformeerd over het afsluiten van de klacht. Ook de wederpartij krijgt zo nodig bericht over het afsluiten van de klacht.

8. Evaluatie

De evaluatie van de behandeling kan zowel mondeling als schriftelijk plaatsvinden. In het geval dat de evaluatie schriftelijk plaatsvindt, gebeurt dat via het speciaal daarvoor bestemd evaluatieformulier. De evaluatie heeft tot doel de kwaliteit van de klachtbehandeling te bewaken en zonodig te verbeteren. In elk geval dient, zo mogelijk in samenspraak met de cliënt, te worden vastgesteld of en in welke mate de gestelde doelen zijn gerealiseerd. Tevens wordt de cliënt gevraagd naar de mate van tevredenheid over de wijze van de klachtbehandeling.

9. Registratie

De meldingen en klachten worden geregistreerd in een registratiesysteem.

10. Archivering

Het dossier wordt gedurende de behandelperiode opgeslagen in het lopend archief. Het dossier wordt tenminste 5 jaar bewaard, te rekenen vanaf het moment van indiening van de klacht.

II. Privacybeleid RADAR, juni 2017

In verschillende organisatiedocumenten zijn afspraken rondom privacy en vertrouwelijkheid opgenomen. Hierbij een opsomming:

In het actuele **personeelsreglement** is het volgende opgenomen:

4.1 Privacy

In de arbeidsovereenkomst is bepaald dat de medewerker geen mededelingen mag doen aan derden omtrent zaken die betrekking hebben op de behandeling van individuele of collectieve klachten, tenzij dit gebeurt in overleg met de teamleider en/of tenzij dit noodzakelijk is voor correcte en doelmatige behandeling van zaken.

Inzage in dossiers door derden kan alleen plaatsvinden na toestemming door de teamleider of de medewerker klachtbehandeling. Dit geldt ook voor andere interne zaken die als vertrouwelijk moeten worden gekenmerkt. Voorts draagt de medewerker er zorg voor dat privacy-gevoelige gegevens vertrouwelijk worden behandeld en op zodanige wijze worden geadministreerd en gearhiveerd dat de vertrouwelijkheid optimaal is gewaarborgd. Dat houdt concreet in dat dossiers buiten kantoor tijden worden bewaard in een afgesloten kluis. Toch kunnen er zich omstandigheden voor doen dat dossiers mee worden genomen buiten het kantoor en buiten werktijd. In principe wordt een kopie met de noodzakelijke gegevens meegenomen. Met dossiers en dossiergegevens moet buiten kantoor uiterst zorgvuldig worden omgegaan. Dat wil zeggen niet uit het oog verliezen en thuis op een veilige plek opbergen. Als het niet anders mogelijk is dan dat dossiers meegenomen worden naar buiten, dient zich altijd een kopie van de eerste pagina (met contactgegevens) op kantoor in de kluis te bevinden. Deze privacybepaling geldt ook ten aanzien van wachtwoorden voor het computerprogramma's, telebankieren en dergelijke vertrouwelijke gegevens. Deze wachtwoorden worden niet doorgegeven en er wordt zorgvuldig mee om gegaan.

In het **arbeidscontract** van elke medewerker, stagecontract en vrijwilligerscontract is het volgende artikel opgenomen:

De werkneemster verplicht zich geen mededelingen aan derden te doen omtrent zaken die betrekking hebben op de behandeling van individuele of collectieve klachten, tenzij zulks geschiedt in overleg met de directeur bestuurder en/of tenzij zulks noodzakelijk is voor een correcte en doelmatige behandeling van zaken.

Deze bepaling geldt ook voor andere interne zaken die als vertrouwelijk moeten worden gekenmerkt. Voorts draagt de werkneemster er zorg voor dat privacygevoelige gegevens vertrouwelijk worden behandeld en op zodanige wijze worden geadministreerd dat de vertrouwelijkheid optimaal is gewaarborgd.

In het **protocol klachtbehandeling**, toegankelijk via onze website

<https://radar.nl/read/protocol-klachtbehandeling-2014?sublist=507>

is hierover het volgende opgenomen:

4.4.8 Registratie en privacybescherming

De cliënt wordt geïnformeerd over de wijze van dossiervorming en hoe met deze gegevens wordt omgegaan. De persoonsgegevens blijven vertrouwelijk. De cliënt wordt verteld dat deze nooit zonder zijn of haar persoonlijke toestemming beschikbaar worden gesteld aan derden. De cliënt heeft na afspraak recht op inzage in het eigen dossier. RADAR is gebonden aan de Wet Bescherming Persoonsgegevens.

In 2009 is de volgende gedragscode opgesteld t.a.v. het omgaan van gegevens van cliënten. Een snelle blik laat zien dat dit nog steeds, in hoofdlijnen, van toepassing is.

Gedragscode omgaan met persoonsgegevens van klachtindieners/melders bij RADAR, oktober 2009

In het personeelsreglement staat de volgende passage over de geheimhoudingsplicht van medewerkers

Personeelsreglement, juli 2008

4.1 Privacy

In de arbeidsovereenkomst is bepaald dat de medewerker geen mededelingen mag doen aan derden omtrent zaken die betrekking hebben op de behandeling van individuele of collectieve klachten, tenzij dit gebeurt in overleg met de locatiemanager en/of tenzij dit noodzakelijk is voor correcte en doelmatige behandeling van zaken. Inzage in dossiers door derden kan alleen plaatsvinden na toestemming door de locatiemanager of de stafmedewerker klachtbehandeling. Dit geldt ook voor andere interne zaken die als vertrouwelijk moeten worden gekenmerkt. Voorts draagt de medewerker er zorg voor dat privacy-gevoelige gegevens vertrouwelijk worden behandeld en op zodanige wijze worden geadministreerd en gearchiveerd dat de vertrouwelijkheid optimaal is gewaarborgd. Dat houdt concreet in dat dossiers buiten kantoortijden worden bewaard in een afgesloten kluis. Toch kunnen er zich omstandigheden voor doen dat dossiers mee worden genomen buiten het kantoor en buiten werktijd. In principe wordt een kopie met de noodzakelijke gegevens meegenomen. Met dossiers en dossiergegevens moet buiten kantoor uiterst zorgvuldig worden omgegaan. Dat wil zeggen niet uit het oog verliezen en thuis op een veilige plek opbergen. Als het niet anders mogelijk is dan dat dossiers meegenomen worden naar buiten, dient zich altijd

een kopie van de eerste pagina (met contactgegevens) op kantoor in de kluis te bevinden.

Deze privacybepaling geldt ook ten aanzien van wachtwoorden voor het computerprogramma's,

telebankieren en dergelijke vertrouwelijke gegevens. Deze wachtwoorden worden niet doorgegeven en er wordt zorgvuldig mee om gegaan.

Naast deze bepalingen die voor iedere medewerker gelden is er nog de Wet Bescherming Persoonsgegevens. RADAR mag op grond van de Wet bescherming persoonsgegevens (Wbp) gegevens alleen verzamelen met het uitdrukkelijke doel klachtbehandeling, registratie en monitoring. Eén van de eisen die het Cbp stelt bij het inrichten van de gegevensverwerking is dat steeds nagegaan moet worden of het gebruik van persoonsgegevens noodzakelijk is voor het doel waarvoor de toestemming is verleend.

Dat betekent dat we ons telkens moeten afvragen of niet met minder gegevens hetzelfde doel bereikt kan worden en of niet langs een andere weg hetzelfde resultaat bereikt kan worden, bijvoorbeeld door met behulp van technische hulpmiddelen te bewerkstelligen dat we geen of zo min mogelijk persoonsgegevens gebruiken,

Wat noodzakelijk is voor het doel, kan in de publieke sector anders uitpakken dan in de private sector. Dit hangt samen met de verschillende rollen die partijen hebben in de maatschappij.

Aan welke kwaliteitseisen moet de gegevensverwerking voldoen?

De Wbp bevat een algemene norm over de kwaliteit van uw gegevensverwerking. De gegevens moeten gelet op het doel waarvoor ze worden verwerkt:

- *niet bovenmatig;*
- *toereikend; en*
- *ter zake dienend zijn.*

Er moet voor gezorgd worden dat er voldoende en adequate gegevens verwerkt worden voor ons doel. We mogen niet te gedetailleerde gegevens verwerken als dat voor uw doel niet noodzakelijk is (niet bovenmatig).

Beveiligen

De Wbp verplicht ons om onze persoonsgegevensverwerking te beveiligen. ***We moeten passende technische en organisatorische maatregelen nemen om het verlies van gegevens of onrechtmatige verwerking tegen te gaan.***

Organisatorische maatregelen kunnen bijvoorbeeld inhouden dat maar een beperkt aantal personen toegang heeft tot uw computersysteem. ***De (technische en organisatorische) maatregelen die we nemen, moeten een passend beveiligingsniveau garanderen.***

Passende beveiliging betekent dat in de keuze voor de methode van beveiliging de volgende elementen moet meewegen:

- De risico's van de verwerking en de aard van de te beschermen gegevens. Hoe gevoeliger de gegevens, hoe zwaarder de toegepaste beveiliging moet zijn. Zijn de gegevens minder gevoelig, dan hoeft je niet steeds de zwaarst mogelijke beveiligingsmaatregelen nemen.
- Je moet rekening houden met de stand van de techniek en de kosten van de maatregelen. Als de kosten van extra maatregelen uitzonderlijk hoog zijn ten opzichte van de toename in beveiligingsniveau, dan zijn die maatregelen niet passend en hoeft je ze dus niet te nemen. Kunt je echter tegen geringe kosten komen tot

een beduidend veiliger systeem, dan moet je deze maatregelen zeker nemen.

De beveiliging moet steeds adequaat zijn. Dat betekent ook dat je periodiek moet nagaan of het systeem aanpassing behoeft, bijvoorbeeld door technologische ontwikkelingen.

In de praktijk

Op basis van de privacywetgeving zijn de databestanden waar de klachtbehandelaars mee werken alleen voor hen toegankelijk. De klachtbehandelaars werken ermee en voor hen is er een doel om toegang te hebben tot deze gegevens. Ook de monitormedewerkers hebben toegang tot de klachtgegevens omdat zij de informatie hieruit controleren en verwerken.

Verder is het zo georganiseerd dat medewerkers alleen toegang hebben tot de klachten en meldingen van de vestiging waar zij werken.

Daarnaast moeten we ons telkens afvragen of het noemen van namen een doel heeft. Als je in het teamoverleg signalen van klachten wilt doorgeven heeft het geen toegevoegde waarde om te weten hoe de persoon heet (het is ook niet erg om het wel te weten, maar het hoeft niet).

Bij het zorgvuldig omgaan met gegevens van mensen moet je dus telkens stilstaan.

Gegevensverwerking

Een persoon wiens persoonsgegevens worden verwerkt, moet altijd kunnen nagaan wat er met die gegevens gebeurt. De Wbp bevat daarom een regeling over informatieverstrekking aan de betrokkene. De informatieverstrekking aan de betrokkene moet in ieder geval omvatten voor welk doel of doeleinden waarvoor de gegevens worden verzameld en verwerkt.

Inzage

Iedereen mag met redelijke tussenpozen vragen of, en zo ja welke persoonsgegevens ten aanzien van hem zijn verwerkt. Als de betrokkene ons buitensporig vaak met een dergelijk verzoek benadert, hoeft daaraan geen gehoor te gegeven te worden. Op een verzoek om inzage moet binnen vier weken geantwoord worden. Het antwoord moet schriftelijk zijn, tenzij een gewichtig belang van de betrokkene vergt dat je een andere vorm kiest, bijvoorbeeld mondeling.

Een per e-mail verzonden antwoord is ook schriftelijk. Het antwoord moet in een begrijpelijke vorm bevatten:

- een volledig overzicht van de verwerkte gegevens van de betrokkene;
- een omschrijving van het doel of de doeleinden van de gegevensverwerking;
- de categorieën van gegevens waarop de verwerking betrekking heeft;
- de ontvangers of categorieën van ontvangers;
- alle beschikbare informatie over de herkomst van de gegevens.

Margriet Maris, versie 6 oktober 2009

III. Figuur 1, informatieverstrekking (website RADAR)

Figuur 1: Informatieverstrekking (website RADAR)

The screenshot shows the RADAR website interface. At the top, there is a navigation bar with links: home, Over ons, Klacht, Sponsors/partners, Opinie, Voor de gemeente, and Con. Below this is the RADAR logo and the text 'vóór gelijke behandeling tegen discriminatie'. A search bar and social media icons are also present. The main navigation menu includes: Kennisbank, Discriminatie, Wetgeving, Cijfers, Oordelen, Trainingen, Projecten, and Publicaties. The current page is 'Uw privacy', which is highlighted in the left sidebar. The content of the 'Uw privacy' page includes a heading 'Uw privacy' and a paragraph explaining that RADAR collects personal data when using the website, such as the date and time of the visit, the IP address, and the browser. It also mentions that this data is used to improve the website and service. The footer contains links for Copyright Radar 2017, Disclaimer, Uw privacy, RSS Feeds, Links, Mail de webmaster, and Veelgestelde vragen.

home Over ons Klacht Sponsors/partners Opinie Voor de gemeente Con

RADAR vóór gelijke behandeling tegen discriminatie

zoeken

Kennisbank Discriminatie Wetgeving Cijfers Oordelen Trainingen Projecten Publicaties

Uw privacy

Hoofdpagina / Uw privacy:

Uw privacy

Welke informatie RADAR van u verzamelt, hangt af van hetgeen u doet wanneer u onze website bezoekt. Via de site worden geen persoonsgegevens verzameld, tenzij u ervoor kiest deze informatie te verschaffen via een informatieverzoek of klachtenformulier.

Bij uw bezoek aan de website worden per opgevraagde pagina standaardgegevens verzameld en opgeslagen zoals de datum en tijd waarop de pagina is opgevraagd, het IP-adres en de browser. Deze gegevens worden uitsluitend gebruikt om de website te kunnen verbeteren en de dienstverlening te optimaliseren.

Indien u per e-mail of via webformulieren persoonsgegevens aan RADAR verstrekt, worden deze verzameld en gebruikt voor het doel waarvoor u ze achterlaat en eventueel voor interne kwaliteitsonderzoeken om de dienstverlening te kunnen meten. Geanonimiseerd worden de gegevens gebruikt voor analyse, rapportage en onderzoek.

Naar boven

Copyright Radar 2017 Disclaimer Uw privacy RSS Feeds Links Mail de webmaster Veelgestelde vragen

IV. Observatie en gespreksverslag klachtbehandelaar Rotterdam

In onderstaande tekst wordt er gesproken van observator en geobserveerde. Echter zijn er ook vragen gesteld tijdens de observaties en zijn deze vragen beantwoordt. Observator heeft geen vragenlijst aangehouden. De vragen zijn vanuit de handelingen van de geobserveerde ontstaan.

Observatie- en gespreksverslag		
Datum: 10 oktober 2017 te Rotterdam		Naam geobserveerde: Klachtbehandelaar Rotterdam
Tijd: 12:00		
Situatie: Klacht behandelen / Team Klachtbehandeling		Naam observator: Amy van de Klundert
Algemene gegevens RADAR anti-discriminatiebureau Team: Klachtbehandeling Locatie: Rotterdam Regio's: Rotterdam-Rijnmond Zuid-Holland-Zuid		
Vraagstelling Wat is de huidige werkwijze m.b.t. het behandelen van een klacht en de verwerking van persoonsgegevens.		
Trefwoorden		
-Klacht uit de infobox	-Correspondentie	-Machtiging
-Veroorzaker/tegenpartij	-Herkomst*	-Fysiek registratieboek
-Anoniem	-Inzagerecht	-Archief

Verslag

Observator heeft het proces bekeken hoe een klacht wordt ingediend en in behandeling wordt genomen door de geobserveerde klachtbehandelaar. Bij de geobserveerde is een klacht via de infobox binnengekomen. De infobox wil zeggen dat er een klacht via de site is gemeld. Het klachtformulier op de site is ingevuld en komt binnen op het algemene email-adres van RADAR (namelijk info@radar.nl). Vanuit het dienstrooster is er een verdeling gemaakt wie op welke dag de klachten behandelt. De desbetreffende klachtbehandelaar leest de mail en beoordeelt hoe er met deze klacht moet worden omgegaan. Is het verhaal redelijk duidelijk?, dan kiest de behandelaar ervoor om een e-mail te sturen met de mogelijkheden. Mocht het zo zijn dat de klacht niet geheel duidelijk is, dan kan er worden gebeld naar de cliënt indien er een telefoonnummer is achtergelaten. Bij het eerste contact met cliënt worden alle gegevens geïnventariseerd. De klachtbehandelaar vult het registratiesysteem in voor het deel wat mogelijk is. Indien de cliënt een deugdelijke omschrijving van de klacht heeft gestuurd wordt dit gekopieerd en geplakt onder het kopje "klachtomschrijving". Indien er geen deugdelijke melding van cliënt is weergegeven in de mail, maakt de klachtbehandelaar zelf een samenvatting van de klacht. In alle gevallen wordt er een luisterend oor geboden aan de cliënt. Mochten de gegevens van de veroorzakers alias tegenpartij helder zijn wordt deze door de desbetreffende klachtbehandelaar niet ingevuld in LBA-net. Het tabblad correspondentie wordt tevens niet ingevuld. De geobserveerde wikkelt zaken vrijwel digitaal of telefonisch af. Er is zelden een bemiddelingsgesprek. Als er een zaak wordt afgesloten en er is een bemiddelingsgesprek geweest, dan wordt er door geobserveerde gewezen op het inzagerecht. Tijdens het invullen van de gegevens in LBA-net kom je bij alle partijen een veld met herkomst* tegen. Dit is een verplicht onderdeel, maar kan ook met onbekend worden ingevuld. De geobserveerde vult dit veld alleen naar waarheid in als de desbetreffende klacht gaat over het ras van de persoon. Is dit niet het geval dan wordt er onbekend ingevuld. In Rotterdam wordt er een fysieke map bijgehouden met de klachten die van dat kalenderjaar gemeld zijn. Dit zijn alleen de klachten die hebben plaatsgevonden in Rotterdam-Rijnmond en Zuid-Holland-Zuid. Er worden hier een aantal gegevens opgeschreven:

- LBA-nummer;
- eigen logboeknummer;
- aantallen;
- naam melder;
- datum;

- klachtbehandelaar;
- afsluitdatum.

De klachtbehandelaars van locatie Rotterdam maken alleen gebruik van deze map. In Brabant werken ze met een digitale lijst. Tot slot deelt de klachtbehandelaar mee dat alle klachtbehandelaars de inlogcodes van het registratiesysteem van alle regio's ter beschikking heeft. Dit is gedaan om een goede achtervang te bieden als er sprake is van ziekteverzuim.

V. Observatie en gespreksverslag klachtbehandelaar Brabant

In onderstaande tekst wordt er gesproken van observator en geobserveerde. Echter zijn er ook vragen gesteld tijdens de observaties en zijn deze vragen beantwoordt. Observator heeft geen vragenlijst aangehouden. De vragen zijn vanuit de handelingen van de geobserveerde ontstaan.

Observatie- en gespreksverslag

Datum: 4 oktober 2017 te Rotterdam		Naam geobserveerde: Klachtbehandelaar Brabant
Tijd: 16:00		
Situatie: Klacht behandelen / Team		Naam observator: Amy van de Klundert
Klachtbehandeling		
Algemene gegevens		
RADAR anti-discriminatiebureau		
Team: Klachtbehandeling		
Locatie: Tilburg		
Regio's: Midden-West-Brabant		
Vraagstelling		
Wat is de huidige werkwijze m.b.t. het behandelen van een klacht en de verwerking van persoonsgegevens		
Trefwoorden		
-Telefonische klacht	-Correspondentie	-Machtiging
-Veroorzaker/tegenpartij	-Herkomst*	-Digitaal registratieboek
-Anoniem	-Inzagerecht	-Archief

Verslag

Observator heeft het proces bekeken hoe een klacht wordt ingediend en in behandeling wordt genomen door de geobserveerde klachtbehandelaar. Bij de geobserveerde is een klacht telefonisch ingediend. Bij de betreffende telefonische klacht werd er door melder gebeld naar het algemene 010 nummer van RADAR. Als cliënten die contact opnemen in een andere gemeente wonen dan RADAR behandeld, worden ze doorverwezen naar de juiste antidiscriminatievoorziening. In alle gevallen krijgen de melders eerst het "secretariaat/bedrijfsbureau" aan de telefoon. In sommige gevallen kan het zo zijn dat de melder direct de klacht vertelt aan de persoon die ze op dat moment spreken. Degene die de telefoon bij RADAR opneemt is geen klachtbehandelaar. Het secretariaat kijkt op dat moment welke persoon in er telefoondienst heeft en in welke regio de klacht hoort. De melder wordt doorverbonden met de aangewezen klachtbehandelaar. Het is voor de melder ook mogelijk om via WhatsApp een klacht indienen. Bij deze klachten worden veelal geen persoonsgegevens uitgewisseld, ook omdat we de ervaring hebben dat mensen alleen anoniem (op het telefoonnummer na) een melding willen doen. De WhatsApp telefoon is in beheer van één medewerker klachtbehandeling. De klachtbehandelaar noteert enkele persoonsgegevens en biedt een luisterend oor. Vervolgens geeft de klachtbehandelaar een voorlopige visie/inschatting van wat hij heeft gehoord. Het telefoongesprek wordt beëindigd en er worden afspraken gemaakt over de vervolgstappen. De klachtbehandelaar gaat de klacht registreren in het geautomatiseerde systeem LBA-net. Er worden door de klachtbehandelaar een aantal gegevens ingevuld. De klachtbehandelaar geeft aan dat hij altijd het veld 'herkomst' invult. Enkele velden zijn namelijk verplicht om in te vullen, dit wordt aangeduid met een rode ster (*). Onderstaand is een printscreen genomen van de velden die ingevuld moeten worden in het registratiesysteem. De klachtbehandelaar gaat na registratie klacht onderzoek verrichten. Naar aanleiding van de uitkomst van het onderzoek kunnen er verschillende wendingen worden genomen. Er kan gekozen worden om een intakegesprek te plannen. Is de klacht duidelijk kan de melder er voor kiezen dat de klachtbehandelaar de tegenpartij gaat benaderen. Indien er wordt gekozen voor deze benadering, stelt de klachtbehandelaar een wederhoorbrief op. In deze brief komt te staan welke situatie zich heeft voorgedaan en of de tegenpartij wil meewerken met een eventuele bemiddeling. Bij deze melding was er geen bemiddelingsgesprek nodig. Er werden enkele hoor en wederhoor brieven gestuurd en daarmee werd de klacht opgelost. Om de registratie compleet te maken vult de klachtbehandelaar alle gegevens in van alle partijen. De herkomst van de melder en de veroorzaker (tegenpartij) zijn verplicht om in te vullen. Tot slot deelt de klachtbehandelaar mee dat hij nog nooit een melding heeft gedaan aan de AP.

Ten tijde van de observatie is er door onderzoeker en observant gekeken op de site van de AP. Hier staat inderdaad geen melding van Stichting RADAR. RADAR heeft nog nooit gemeld dat ze persoonsgegevens verwerken. De geobserveerde was ook niet bekend met de meldplicht over datalekken, omdat deze in de tijd dat hij er werkt nog niet zijn plaatsgevonden.

VI. Mailcorrespondentie bedrijfsbureau

Vraag infobox



[Redacted]

di 21-11, 16:21

Amy van de Klundert ✓



Allen beantwoorden | v

Hoi Amy,

Discriminatie.nl gaat naar de mailbox per regio, obv het ingevulde postcode. De mails voor Rotterdam komen in info@radar.nl uit ipv info Rotterdam.

De klachtformulieren van onze eigen website komen allemaal in de info@radar.nl uit.

Sommige mensen sturen ook zelf een mail naar een van de mailadressen.

Groet van Iris

mobiel: [Redacted]

intern: 601

...

VII. Observatie en gespreksverslag Rotterdam-Brabant

Observatie- en gespreksverslag

Datum: 10 oktober 2017 te Rotterdam		Naam geobserveerde: Klachtbehandelaar Rotterdam-Brabant	
Tijd: 15:00		Naam observator: Amy van de Klundert	
Situatie: Klacht behandelen / Team Klachtbehandeling			
Algemene gegevens			
RADAR anti-discriminatiebureau			
Team: Klachtbehandeling			
Locatie: Rotterdam			
Regio's: Rotterdam-Rijnmond Zuid-Holland-Zuid			
Trefwoorden			
-Telefonische klacht		-Correspondentie	
-Veroorzaker/tegenpartij		-Herkomst*	
-Anoniem		-Inzagerecht	
		-Machtiging	
		-Digitaal registratieboek	
		-Archief	

Verslag

Observator heeft het proces bekeken hoe een klacht wordt ingediend en in behandeling wordt genomen door de geobserveerde klachtbehandelaar. Bij de geobserveerde is een klacht in eerste instantie anoniem ingediend. Betrokkene heeft gebeld en de klachtbehandelaar heeft de klacht aangehoord en zijn voorlopige visie gegeven. De melder heeft een woonplaats doorgegeven dus kon de melding geregistreerd worden in LBA-net. De melder heeft later een e-mail gestuurd met zijn eigen naam om op de klacht terug te komen. Er is door de betreffende klachtbehandelaar een reactie op de mail gegeven. De melder heeft vervolgens aangegeven dat hij graag voor een gesprek op het kantoor wil komen. Mocht er iemand persoonlijk langskomen worden de gegevens genoteerd op een notitieblok. De NAW-gegevens worden genoteerd. Het emailadres en het telefoonnummer ook. De melder maakte zich in eerste instantie ernstige zorgen over zijn privacy/geheimhouding. De cliënt gaf aan dat hij vanuit de werkgever een geheimhoudingsplicht zou gelden. Daarnaast maakte de cliënt zich druk of RADAR contact zou opnemen met de werkgever omdat de melding over de werkgever betrof. De klachtbehandelaar heeft mondeling toegelicht dat er geen gegevens aan derden wordt verstrekt zonder toestemming. Dit zegt de klachtbehandelaar overigens niet tegen elke cliënt, alleen als er om wordt gevraagd. Daarnaast geeft de klachtbehandelaar aan dat er conform de privacywetgeving wordt gewerkt en dat er daarom wel een woonplaats nodig is om het incident te registreren. Verder wordt er door klachtbehandelaar het registratiesysteem uitgelegd. In LBA-net is het invullen van de veroorzaker geen verplicht veld. Als het bijv. in de plus is gebeurd, dan is de organisatie aansprakelijk en niet de manager van de plus. Je schrijft wel de team manager aan in een brief. Maar de veroorzaker is de plus zelf. (voor bijvoorbeeld team onderzoek kan de veroorzaker wel van invloed zijn. Vooral waar het is gebeurd, waar het slachtoffer woont en op welke grond of terrein het is gebeurd.) Daarnaast is de klachtbehandelaar van mening dat er meer mensen zomaar zouden moeten langskomen daarmee wordt duidelijker dat RADAR laagdrempelig is en geen virtueel klachtenbureau is. Op sommige locaties is dit niet toereikend i.v.m. de veiligheid. Er zijn te weinig soms geen mensen aanwezig om de veiligheid te waarborgen. Er zijn op de locaties Tilburg en 's-Hertogenbosch geen intakeruimtes. In geval van inlooptagen komen er meer fysieke stukken binnen. Dit probeert radar te voorkomen i.v.m. het archief. Team klachtbehandeling heeft een lopend archief en een normaal archief. In het lopende archief zou alleen de lopende zaken in moeten zitten, maar dit is in praktijk niet zo. Er zitten meerdere jaren in en ook open en gesloten dossiers. In het andere archief worden zaken 5 jaar bewaard. In 2017 wordt het archief van 2012 vernietigt. Het zijn allebei kluisen. Het lopende archief ligt in een kluis bij twee klachtbehandelaars op de kamer. Een aantal personen hebben deze sleutel, indien de kluis wordt opengemaakt blijft deze gedurende dag openstaan. Het andere archief is op slot met een sleutel die het bedrijfsbureau beheert. In dit archief zitten alleen verouderde gesloten zaken. Klachtbehandelaar geeft aan het digitale archief nog nooit is verwijderd. LBA-net is in 2012 opgezet en alles kan worden ingezien, er is niet geanonimiseerd. Tot slot maakt Rotterdam gebruik van een fysieke

registratiemap. De map wordt rondgedeeld en de gegevens worden door elke klachtbehandelaar zelf opgeschreven.

Tot slot geeft klachtbehandelaar aan dat Brabant gebruik maakt van een digitale lijst die op de gezamenlijke SharePoint te vinden is. Elke klachtbehandelaar vult hier zelf de klachten aan. In dit lijstje worden verschillende gegevens bewaard:

- aanmelddatum;
- naam cliënt;
- gemeente melder en plaats incident;
- omschrijving klacht;
- klachtbehandelaar;
- vervolgstappen (wat te doen).

VIII. Conclusie observaties en gesprekken

Conclusie observaties

Situatie: Klacht behandelen / Team
Klachtbehandeling

Naam geobserveerde: Klachtbehandelaars Brabant,
Rotterdam en Rotterdam-Brabant

Naam observator: Amy van de Klundert

Algemene gegevens

RADAR anti-discriminatiebureau

Team: Klachtbehandeling

Locatie: Tilburg

Regio's: Rotterdam-Rijnmond, Zuid-Holland-Zuid, Brabant-Noord en Midden-West-Brabant.

Conclusie:

In de werkwijze van de klachtbehandelaars per regio zijn een aantal verschillen te herkennen. Zo is het dat de klachtbehandelaar in Brabant werkt met termen als hoor- en wederhoorbrieven. Dit wordt ook in LBA-net op deze manier verwerkt. In het kopje 'stapoverzicht' zet de klachtbehandelaar in de beschrijving erbij of het een hoor of wederhoorbrief betreft. De velden van slachtoffer en veroorzaker worden door de klachtbehandelaar direct ingevuld indien er over deze informatie wordt beschikt. Daarnaast wordt door de klachtbehandelaar in Brabant het kopje 'herkomst' gezien als een verplicht veld. Hier kun je uit verschillende landen kiezen die is gebaseerd op eerdere meldingen en de algehele bevolking in Nederland. Herkomst wordt beschouwd als het land van herkomst, of het land van herkomst van de ouders. Verder is door de klachtbehandelaar die in alle regio's werkzaam is, aangegeven dat Brabant werkt met een digitale registratielijst. In deze lijst worden o.a. de volgende gegevens genoteerd:

- aanmelddatum;
- naam cliënt;
- gemeente melder en plaats incident;
- omschrijving klacht;
- klachtbehandelaar;
- vervolgstappen (wat te doen).

De klachtbehandelaar van Brabant deelt de cliënt verder niet uitdrukkelijk mee hoe er wordt omgegaan met zijn/haar gegevens. Ook wordt er van uit gegaan door de eigen benadering van de cliënt dat de gegevens verwerkt mogen worden. De klachtbehandelaar die in alle regio's actief is, heeft dit bevestigd. Indien een cliënt uit dat hij/zij zich zorgen maakt over zijn/haar privacy wordt er mondeling of digitaal medegedeeld dat er zonder toestemming geen gegevens worden verstrekt aan derden. Deze klachtbehandelaar meldt tevens dat er conform de privacywetgeving wordt gewerkt en dat er daarom wel een woonplaats nodig is om het incident te registreren. De klachtbehandelaar vult voor het afsluiten van de zaak, de gegevens van de veroorzaker in. Team klachtbehandeling heeft een lopend archief en een normaal archief. In het lopende archief zou alleen de lopende zaken in moeten zitten, maar dit is in praktijk niet zo. Er zitten meerdere jaren in en ook open en gesloten dossiers. In het andere archief worden zaken 5 jaar bewaard. In 2017 wordt het archief van 2012 vernietigd. Het zijn allebei kluizen. Het lopende archief staat hele dag open in een kamer. Het andere archief is op slot met een sleutel die maar een aantal mensen hebben. In Tilburg is onlangs het lopende archief volledig gedigitaliseerd. Enkele dossiers zijn bewaard in de kluis, andere dossiers zijn gedigitaliseerd en vervolgens vernietigd. In 's-Hertogenbosch is er geen archief en ook geen kluis. Het digitale archief is bij alle partijen nooit verwijderd noch geanonimiseerd.

De klachtbehandelaar die werkzaam is in Rotterdam geeft allereerst aan dat zij voornamelijk digitaal op klachten reageert. In het registratiesysteem vult zij de gegevens van de veroorzaker vrijwel nooit in. Ze is van mening dat dit geen toegevoegde waarde heeft qua registratie. Klachtbehandelaar geeft aan dat er alleen op het inzagerecht word gewezen als er een bemiddelingsgesprek is geweest. Daarnaast geeft zij aan dat de kolom van 'herkomst' alleen naar waarheid wordt ingevuld als de klacht is gericht op gebied 'ras'. Is dit niet het geval vult zij onbekend in. Tot slot gebruiken ze in Rotterdam een fysieke registratiemap. In de map worden een aantal gegevens genoteerd namelijk:

- het LBA-nummer;
- eigen logboeknummer;
- aantallen;

- naam melder;
- datum;
- klachtbehandelaar;
- afsluitdatum.

IX. Offerte Constant-IT

Registratiesysteem
"AllAequalis"
Constant IT



Bureau Lelystad
De Veste 10-02
8231 JA Lelystad

T (0320) 23 33 27
F (0320) 24 52 90

Bureau Almere
Zoetelaarpassage 27
1315 AV Almere

T (036) 52 97 670
F (036) 52 97 197

Openingstijden ma t/m vr 9.00 – 17.00 uur

www.bureaugelijkebehandeling.nl
info@bureaugelijkebehandeling.nl

KvK 39081532
Bank P9484006

Aan : Brenda

Van : Arja

Onderwerp : onder tekenende offerte

Datum : 14/3/11

- ☐ ter informatie
- ☐ volgens afspraak
- ☐ graag uw reactie
- ☐ graag uw reactie voor.....
- ☐ ter ondertekening
- ☒ ibar archief LRA

Met vriendelijke groet,

Bureau Gelijke Behandeling Flevoland

1 Introductie

Vanuit de nieuw opgerichte Landelijke Branchevereniging voor Anti-discriminatiemeldpunten is er vraag naar een landelijk registratiesysteem voor het centraal administreren van klachten en informatieverzoeken. Doel van dit systeem is om alle aangesloten meldpunten op één en dezelfde wijze registraties uit te laten voeren. Dit komt de kwaliteit van de administratie ten goede en maakt centrale rapportage mogelijk.

Constant IT biedt als oplossing een op maat gemaakt extranet (een besloten website die voor alle aangesloten meldpunten centraal te bereiken is). Op dit extranet kan men alle registratie, administratie en rapportage-taken uitvoeren. Het vervangt de verschillende bestaande software die momenteel door de aangesloten meldpunten in gebruik is.

In deze offerte wordt bovenstaande oplossing nader toegelicht en wordt een kostenspecificatie uiteengezet.

2 Omschrijving van het eindproduct

In dit hoofdstuk wordt de functionaliteit en onderliggende principes van het extranet omschreven.

2.1 Functionaliteiten / afspraken

- Deadline is 1/7/2011.
- Alle betrokken software wordt beschikbaar gesteld aan de LBA. De LBA mag het extranet onbeperkt en onafhankelijk van de ontwikkelaar gebruiken, maar stemt in de code niet te dupliceren voor hergebruik/kopie. De garantie op het systeem vervalt zodra een derde partij wijzigingen aan de code/database uitvoert. Het hostingplatform waar het extranet op draait wordt ingericht en beheerd door Constant IT. Het staat de LBA vrij om de hosting te laten migreren naar een andere partij.
- Site moet afgeschermd zijn voor anonieme bezoekers. Medewerkers van een meldpunt krijgen eigen accounts, gekoppeld aan het meldpunt waar ze voor werken. De admin van de site moet accounts kunnen maken/bewerken/verwijderen.
- Individuele bureaus (districten) hebben uitsluitend toegang tot eigen dossiers. Users moeten alleen klachten kunnen administreren van hun eigen regio. Verder moeten alleen mensen met een 'management'-permissie rapportages (zie laatste bullet) kunnen uitdraaien. De admin van de site moet permissies kunnen toekennen aan users.
- Permissiemodel voor users per district (management, klachtenbehandelaar en voorlichter).
- Speciaal permissiemodel voor onderzoekers (dienen over landelijke anonieme gegevens te beschikken, met mogelijkheid in te zoomen op districtniveau).

- Zoekfunctie op alle mogelijke categorieën per district. (Iemand die is ingelogd in district Groningen dient geen resultaten te krijgen van Rotterdam)
- Automatisch genereren van Straatnaam en Woonplaats, bij het invoeren van de Postcode en het Huisnummer.
- Bewaarduur van dossiers maximaal 5 jaar.
- Naar schatting worden 8000 dossiers per jaar toegevoegd.
- Dossiers dienen automatisch een uniek landelijk- en districtnummer te krijgen.
- Het registreren van klachten en informatieverzoeken geschiedt via "formulieren".
- Een formulier bevat een ongeveer 30 velden. Het is een combinatie van vrije en verplichte invulvelden en selectieopties in categorieën (zie hieronder). Daarnaast moeten er bestanden geupload kunnen worden (bijv. een scan van een brief).
- Voor sommige velden (vrije invulvelden / dropdownmenu's) moeten meerdere keuzes gemaakt kunnen worden.
- Dossiers hebben een status, bijvoorbeeld: open/gesloten/hoor/wederhoor/alleen registratie.
- Een dossier heeft een 'reminderdatum' waarop het dossier duidelijk zichtbaar wordt in het dossieroverzicht van een behandelaar.
- De manager van een district moet taken kunnen toewijzen aan behandelaars. Op de homepage staat een takenlijst met de taken van de ingelogde gebruiker.
- Medewerkers van een district moeten notities kunnen maken voor zichzelf en/of het hele district.
- Wanneer een melding gemaakt wordt waarbij de melder buiten z'n district wordt gediscrimineerd moet het district waar de melder woont een seintje krijgen.
- Ze hebben beide ook velden voor "intakedatum" en "datum afsluiting". Deze velden worden gebruikt om bijv. bij rapportages te kunnen filteren op jaar.
- Contactpersonen moet een losse entiteit in het systeem worden.
- Bij invullen/kiezen van melder/dader/slachtoffer moeten bestaande contacten gekozen kunnen worden. Dit om te voorkomen dat data dubbel ingevoerd moet worden.
- Contactpersonen zijn gekoppeld aan een meldpunt. Het moet niet mogelijk zijn om bestaande contacten van andere meldpunten te zien/gebruiken.
- Aan klachten en informatieverzoeken moeten "stappen" toegevoegd kunnen worden. Dit zijn een soort logboekvermeldingen met een paar velden voor tekst en een file upload. Belangrijk is dat aan in stap ook een tijdregistratie (aantal minuten) wordt opgegeven. In het overzicht van een klacht wordt dan getoond wat de totale tijdsinvestering van een klacht is. In de rapportagefunctie dient een rapport beschikbaar te zijn voor het tonen van de totale tijdsbesteding per medewerker per periode.
- Iedere klachtbehandelaar dient een duidelijk overzicht (tabel) te hebben van openstaande dossiers (klachten en informatieverzoeken)

- Beheer van categorieën. Users met permissie om categorieën te beheren moeten zelf de verschillende selectielijsten kunnen beheren.
- Maken van rapportages door users met "management"-permissie. De rapportages bestaan uit (kruis)tabellen waarbij gekozen kan worden welke categorieën in de assen van de tabel worden uitgezet. Verder dient er geëxporteerd naar Excel/CSV/PDF te kunnen worden.
- Uitgebreid rollen/permissie systeem.

Voor onderzoekers:

- Anonieme rapportage functie. Gebaseerd op de rapportage functie van users met management-permissie, echter dossiers zijn afgeschermd (geen personalia).
- Onderzoekers dienen zowel landelijk, als per district research te kunnen doen.

Voor managers:

Hieronder het overzicht van belangrijke managementinformatie die uit het registratiesysteem moet zijn te halen:

- Afhandelingsduur per klacht; gemiddelde afhandelingsduur
- Overzicht totaal aantal klachten/informatieverzoeken lopend en of afgesloten.
- Overzicht behandelde klachten/informatieverzoeken per werknemer
- Uitgebreide kruistabellen. Categorieën tegen elkaar afzetten.
- Export naar CSV/XLS/PDF.

IT-aspecten / implementatiedetails / beheer

- VPS Hosting en domeinregistratie wordt verzorgd door Constant IT.
- SSL certificaat (encryptie) om beveiliging te waarborgen.
- Dagelijkse back-up op Hosting server.
- Off-site backup.

3 Tijdspad

De beoogde volgorde van taken binnen het project zijn (chronologisch):

Fase: Inventarisatie

- Verzamelen van informatie en ontwerpen van functioneel ontwerp:
 - Welke gegevens worden in het systeem opgeslagen?
 - Welke rollen en permissies zijn er?
 - Wie krijgt toegang tot verschillende onderdelen/functies van het systeem?
- Vastleggen van structuur van extranet (menu's, secties)

Fase: Ontwikkeling

- Ontwikkelen extranet
 - Database
 - PHP-framework uitbouwen
 - Rollen/permissies
 - Rapportages

Fase: Testen

- 1^e testronde
- Aanpassingen n.a.v. 1^e testronde
- 2^e testronde
- Aanpassingen n.a.v. 2^e testronde

Fase: Oplevering

- Oplevering (website toegankelijk maken voor de medewerkers)
- Evaluatie project

De doorlooptijd van het project wordt geschat op **14 weken**. De deadline van het project is vastgesteld op 1 juli 2011. De uiterlijke aanvangdatum van het project is 14 maart.

4 Kostenspecificatie

In onderstaande tabellen staat een specificatie van de projectkosten omschreven. De kosten zijn onder te verdelen in initiële kosten en jaarlijkse kosten.

Voor de offerte geldt:

- Alle genoemde prijzen zijn exclusief 19% BTW.
- Betalingsconditie is 50% van initiële ontwikkelkosten vóór aanvang van project, 50% na oplevering project.
- Het project vindt aanvang na ontvangst eerste betaling op rekeningnummer 7572838 t.n.v. Constant IT, Amsterdam.
- De jaarlijkse kosten worden aan het begin van elk kalenderjaar per automatische incasso verrekend.

Initiële ontwikkelkosten:

Omschrijving:	Prijs:
Fase: Inventarisatie • Informatie/materiaal verzamelen • Welke meldpunten zijn aangesloten bij de LBA? • Hoeveel gebruikers zijn er? • Functioneel ontwerp • Technisch ontwerp • Database ontwerp • Research hostingplatform	€ 6.000,-
Fase: Ontwikkeling • Configureren hostingplatform • Inrichten database • Uitbouwen PHP-framework • Inrichten van rollen/permissions • Rapportagefunctie uitbouwen • Grafisch ontwerp toepassen	€ 12.000,-
Fase: Testen • 1^e testfase • Verzamelen aanpassingen/bugs • Wijzigingen doorvoeren, bugs fixen • 2^e testfase • Verzamelen aanpassingen/bugs • Wijzigingen doorvoeren, bugs fixen	€ 3.000,-
Fase: Afronden • Extranet lanceren, toegangsgegevens verstrekken • Projectevaluatie	N.v.t.
Totaal:	€ 21.000,-

Jaarlijkse kosten:

Omschrijving:	Prijs:
Hosting en domeinregistratie - Domeinregistratie - VPS hosting, managed door Constant IT - SSL-certificaat - Extra IP-adres	€ 2.000,-
Technisch onderhoud hostingplatform - Backups hostingplatform - Security updates VPS - Bugfixes	€ 3.000,-
Onderhoud* bestaande functionaliteiten extranet - Herzien/bijschaven bestaande functionaliteiten, n.a.v. feedback - Halfjaarlijkse evaluatie van gebruik.	Ad-hoc **
Support voor gebruikers. - Aanmaken gebruikersaccounts - Hulp bij gebruik (telefonisch/e-mail) - Managementondersteuning (telefonisch/e-mail)	Ad-hoc **
Totaal:	€ 5.000,-

*** Onderhoud:** het aanpassen van reeds bestaande functionaliteiten. Voor het schrijven van nieuwe broncode (nieuwe functionaliteiten) kan op aanvraag een offerte worden gedaan.

**** Ad-hoc:** Wijzigingen in de code en support aan gebruikers zullen op ad-hoc basis worden verrekend. Aan ad-hoc werkzaamheden is geen response-tijd verbonden; dergelijke arbeid wordt op basis van "best-effort" uitgevoerd.

5 Contactinformatie

Contactpersoon *Landelijke Branchevereniging Anti-discriminatiepunten*:

Mevr. A. Kruis

De Veste 10-02

8231 JA Lelystad

Tel. 0320-233327

arja.kruis@bureaugelijkebehandeling.nl

Contactpersoon *Constant IT*:

Dhr. D. Stotijn / Dhr. N. Hoogerdijk

Prinsengracht 530

1017KJ Amsterdam

Tel. 020-6121016

d.stotijn@constant.it / n.hoogerdijk@constant.it

Rekeningnummer Constant IT: 7572838

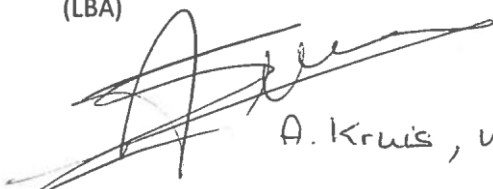
6 Ondertekening

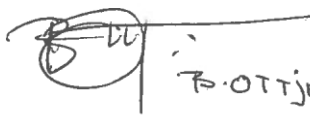
Door ondertekening van deze overeenkomst verklaren de partijen zich akkoord met de inhoud ervan.

Aldus opgemaakt en ondertekend in tweevoud

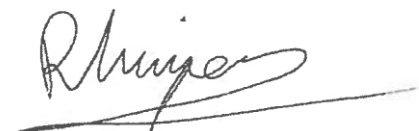
Plaats, datum:

Naam en handtekening tekeningsbevoegde:
(LBA)


A. Kruis, voorz.
LBA


B. OTTJES SECRETARIS LBA

Naam en handtekening tekeningsbevoegde:
(Constant IT)



Beveiligingsinformatie Trends

2.3. Werkplekken

PC's hebben alleen toegang met servers en data via een internetverbinding. De internetverbinding met Trends loopt via een VPN-tunnel. PC's zijn voorzien van antivirussoftware. MS updates en patches worden automatisch geïnstalleerd. Firewall en vergrendeling van de PC wordt standaard ingesteld, maar niet verplicht opgelegd. Gebruikers hebben beperkte rechten op hun PC, rechten voor medewerkers en stagiaires worden middels groepsrechten uitgedeeld. Tevens wordt toegang tot bedrijfsapplicaties via groepsrechten zichtbaar gemaakt. Wachtwoorden moeten (90 dagen) regelmatig vernieuwd worden op basis van complexiteit.

3.3. Virusscanning

1. Zijn de werkplekken voorzien van antivirussoftware? *Ja, McAfee*
2. Wordt deze antivirussoftware automatisch bijgewerkt? *Ja*
3. Wordt deze software centraal beheerd en gemonitord? *Ja, Epo orchestrator*

4.1. Authenticatie

1. Hoe wordt er geauthenticeerd? *Alleen gebruikersnaam en wachtwoord*
2. Wordt er gebruik gemaakt van digitale certificaten? *Ja via Office365 en Windows DC*
3. Zijn dit vertrouwde certificaten of eigen certificaten? *Vertrouwde*
4. Is bekend wanneer deze certificaten verlopen? *Ja*
5. Is bekend welke servers/services er gebruik maken van digitale certificaten?

X. Interview RADAR team onderzoek

Plaats en datum: 's-Hertogenbosch, 14 november 2017

Onderwerp: het nieuwe registratiesysteem ADV-net

Status: Afgerond

Inleiding

Zoals in eerdere contacten besproken, houd ik mij op dit moment bezig met een praktijkgericht juridisch onderzoek. Het juridisch deel is gericht op de nieuwe privacyverordening (de AVG). Het praktijkgericht deel slaat de werkwijze van team Klachtbehandeling, het registratiesysteem en de daarbij komende verwerkingen van persoonsgegevens. Ik heb vernomen dat er in januari 2018 een nieuw registratiesysteem wordt gelanceerd namelijk 'ADV-net'. Voor dit aspect heb ik meer informatie nodig over dit onderwerpen. Dit is dan ook de reden voor dit interview. Door deze informatie te koppelen aan het juridisch deel kan ik uiteindelijk de vraag beantwoorden op welke wijze de verwerking van persoonsgegevens binnen RADAR dient te worden ingericht, zodat deze voldoet aan de AVG.

Wijze van interview

De vragenlijst is vooraf gestuurd naar mevrouw Mink. Zij heeft voor het gesprek de onderstaande vragen beantwoord. Tijdens het interview zijn de antwoorden completer gemaakt en aangevuld door de uitleg van de onderzoeker.

Vragen

Is er met het bouwen van het nieuwe registratiesysteem de nieuwe privacywetgeving in acht genomen? Zo ja, op welke wijze?

Ja. De beveiliging was de hoofdreden om een nieuw systeem te laten bouwen, dat is nu goed geregeld. We hebben verder nagedacht over welke opties we bieden om gegevens van melders/slachtoffers te registreren, zichtbaarheid van gegevens (voor collega's van andere adv's/onderzoekers), bewaartermijn.

Wat wordt er ten opzichte van het oude systeem verbeterd volgens jou gericht op privacy?

De beveiliging is goed geregeld, dat was bij het oude systeem niet meer zo (was verouderd geraakt).

In het oude systeem kon je herkomst en nationaliteit van melder en slachtoffer registreren, daar waren speciale invulvelden voor. In het nieuwe systeem zijn die er niet meer.

In het oude systeem kon je geboortedatum van melder en slachtoffer registreren, dat hebben we nu veranderd in geboortjaar. Geboortjaar en geslacht had ik ook weg willen laten, maar dat vinden anderen (o.a. het bestuur) toch belangrijke gegevens om wel vast te kunnen leggen. Die twee zitten nu wel achter een extra knop. Zodat klachtbehandelaars die met het systeem werken minder geneigd zullen zijn om dit automatisch in te vullen. Tijdens de training en in de handleiding wijzen we erop dat velden niet verplicht zijn om in te vullen en dat elke keer zorgvuldig moet worden afgewogen of (bijzondere) persoonsgegevens nodig zijn om te registreren. Bij rapportage moet die afweging natuurlijk nog zorgvuldiger worden gemaakt. In principe rapporteren we richting externen alleen over de gemeente waar de melder woont.

De gegevens uit het systeem kunnen worden gedownload in Excel, zodat je er analyses op los kunt laten, tabellen kan maken, kan zoeken etc. In Excel kan je alleen de velden zonder privacygevoelige informatie downloaden.

Is er een digitale bewaartermijn geregeld?

We hebben nu afgesproken binnen de LVtD dat de bewaartermijn 5 jaar is. We zijn van plan om in het systeem iets te laten bouwen waardoor na 5 jaar alle velden met privacygevoelige informatie worden gewist. De LVtD wil de andere (niet-privacygevoelige informatie) wel behouden, ook na die 5 jaar.

Wachtwoord: in LBA-net kreeg je een wachtwoord toegewezen, kan je niet meer wijzigen/is nooit gewijzigd. In ADV-net: je kan zelf een wachtwoord kiezen (je moet je registreren met emailadres). Wachtwoord kan je zelf wijzigen. Er is nog geen verplichting om dit na een aantal weken/maanden te doen, dit laten we bouwen indien mogelijk.

Hoe wordt de beveiliging voor het nieuwe systeem gerealiseerd?

Voldoet aan Wbp en OWASP top 10 volgens de overeenkomst die wij met de ontwikkelaar/bouwer hebben afgesloten. Verder wordt de applicatie beveiligd door het platform waar wij gebruik van maken: Betty Blocks. (in de pagina hierna, kan er worden gezien wat OWASP inhoudt.)

Komen in ADV-net ook invulvelden zoals herkomst/geslacht/geboortedatum? En moeten deze ingevuld worden als de klacht niet op ras gericht is?

Zie hiervoor. Er komt een handleiding voor de klachtbehandelaars. De velden voor het invullen blijven bestaan, maar de medewerker moet zelf beslissen of het noodzakelijk is om in te vullen.

Komt er een verwerkingsovereenkomst met ADV-net en bestaat deze al voor LBA-net?

Ja, maar moet nog worden geregeld. NB. De ontwikkelaars/bouwers kunnen niet bij wat wij hebben ingevuld, zij werken in een andere 'omgeving'.

Nee, met de huidige beheerder 'Constant-IT' is geen verwerkingsovereenkomst opgenomen.

Is er een protocol voor de meldplicht datalekken, zo nee is er in de praktijk ooit sprake geweest van een datalek?

Nee, er is geen protocol. Ik weet niet of er ooit een datalek heeft voorgedaan.

Heeft ADV-net een interne functionaris voor de gegevensbescherming?

Nee. Zou dat moeten?

Wordt er door de maker van ADV-net een PIA (risicocheck) uitgevoerd?

Nee niet dat ik weet. RADAR is er wel mee bezig met een extern bedrijf.

OWASP Top-10

De OWASP Top 10 is een overzicht van typen kwetsbaarheden die onder beveiligingsexperts worden gezien als het meest kritisch met betrekking tot webapplicaties. Het is geen kant-en-klare afvinklijst en dekt bovendien niet alle soorten kwetsbaarheden, maar biedt wel een goed zicht op deze complexe materie. De Top 10 vormt daarmee een solide basis voor de door ons aangeboden beveiligingstests.



A1-Injection

Injectiekwetsbaarheden zoals sql-, os commando- of ldap-injectie, ontstaan wanneer niet-geverifieerde data door een hacker wordt verzonden als onderdeel van een commando of query. Deze data kan onbedoelde commando's uitvoeren of ongeautoriseerde toegang tot gegevens verschaffen. [Voorbeeld](#)



A2-Broken Authentication and Session Management

Autorisaties en sessiebeheer worden vaak niet correct geïmplementeerd, waardoor aanvallers wachtwoorden, sleutels of sessietokens kunnen achterhalen om via andere implementatiefouten de identiteit van andere gebruikers aan te nemen.



A3-Cross-Site Scripting (XSS)

We spreken van xss-injectie als een applicatie gegevens zonder filtering en/of encoding naar een web browser zendt. xss-injectie stelt aanvallers in staat om scripts uit te voeren, gebruikerssessies te kapen, websites te beschadigen of de gebruiker naar andere sites te leiden. [Voorbeeld](#)



A4-Insecure Direct Object Reference

Een Insecure Direct Object Reference ontstaat wanneer een ontwikkelaar onbedoeld verwijst naar een intern object zoals een bestand, map of de sleutel van een gegevensbestand. Zonder een toegangscontrole of andere bescherming kunnen hackers deze verwijzingen misbruiken om zichzelf toegang te verschaffen.



A5-Security Misconfiguration

Goede beveiliging vereist een correcte configuratie die wordt afgestemd op de applicatie, frameworks, applicatieserver, webserver, databaseserver en platform. Beveiligingsinstellingen moeten worden gedefinieerd, geïmplementeerd en onderhouden omdat deze standaards vaak onveilig zijn. Daarnaast moet alle software up-to-date zijn.



A6-Sensitive Data Exposure

Veel applicaties beschermen gevoelige gegevens onvoldoende. Denk hierbij aan creditcardnummers, belasting-id's en autorisatiegegevens. Kwaadwillenden kunnen deze stelen of wijzigen voor creditcardfraude, identiteitsdiefstal of andere misdrijven. Gevoelige gegevens moeten extra worden beschermd door middel van versleuteling of andere speciale voorzorgsmaatregelen.



A7-Missing Function Level Access Control

De meeste applicaties controleren autorisaties voordat de gevraagde data zichtbaar wordt in de gebruikersinterface. Applicaties moeten echter bij elke functie die wordt benaderd dezelfde controle uitvoeren op de server. Indien deze niet worden geverifieerd, zijn aanvallers in staat om verzoeken na te bootsen die toegang geven tot functionaliteit waarvoor zij geen autorisatie hebben.



A8-Cross-Site Request Forgery (CRFS)

Een CSRF-aanval dwingt de browser van een aangemeld slachtoffer om een vervalst HTTP-verzoek naar een kwetsbare webapplicatie te verzenden, inclusief sessie-cookie en autorisatie-gerelateerde informatie. Hierdoor kan de hacker de browser dwingen om verzoeken te genereren waarvan de kwetsbare applicatie denkt dat ze legitiem zijn.



A9-Using Components with Known Vulnerabilities

Componenten zoals libraries, frameworks en andere software-modules draaien vaak met volledige autorisatie. Als een kwetsbaar onderdeel wordt geëxploiteerd kan dit tot dataverlies leiden of een overname van de server faciliteren. Componenten met reeds bekende kwetsbaarheden ondermijnen de beveiliging van de applicatie en faciliteren een scala aan mogelijke aanvallen.



A10-Unvalidated Redirects and Forwards

Applicaties leiden gebruikers vaak naar andere pagina's en websites en gebruiken niet-gevalideerde gegevens om de bestemming hiervan te bepalen. Zonder de juiste validatie kunnen aanvallers slachtoffers omleiden naar phishing- of malwaresites of forwards gebruiken voor toegang tot ongeautoriseerde pagina's.

XI. E-mail encryptie

Bron: <https://support.office.com/nl-nl/article/E-mailberichten-versleutelen-373339cb-bf1a-4509-b296-802a39d801dc>

E-mailberichten versleutelen

Als u de privacy van een e-mailbericht wilt beschermen, versleutel het dan. Als u een e-mailbericht in Outlook versleutelt, wordt de leesbare, platte tekst omgezet in code. Alleen de geadresseerde die beschikt over de persoonlijke sleutel die hoort bij de openbare sleutel waarmee het bericht is versleuteld, kan het bericht ontcijferen, zodat diegene het kan lezen. Een geadresseerde die niet over de bijbehorende privésleutel beschikt, ziet echter slechts ontcijferbare tekst.

Wat gebeurt er als de geadresseerde niet over de bijbehorende privésleutel beschikt? Dan ziet de geadresseerde dit bericht:

'Dit item kan niet in het leesvenster worden weergegeven. Open het item om de inhoud ervan te lezen.'

Als de geadresseerde vervolgens het item wil openen, verschijnt er een dialoogvenster met het volgende bericht:

'Het item kan niet worden geopend. Dit kan een tijdelijk probleem zijn, maar als dit bericht opnieuw verschijnt, start Outlook dan opnieuw. De naam van uw digitale id kan niet worden gevonden.'

Wat u nog meer moet weten over versleutelde berichten.

Voor het verzenden en weergeven van versleutelde e-mailberichten moeten de afzender en de geadresseerde hun digitale id of openbare sleutelcertificaat uitwisselen. Dit betekent dat u en de geadresseerde elkaar een digitaal ondertekend bericht moeten sturen, zodat u het certificaat van de ander kunt toevoegen aan uw contactpersonen. U kunt geen e-mailberichten versleutelen zonder een digitale id.

Als u een versleuteld bericht verstuurt aan een geadresseerde met een e-mailconfiguratie die geen versleuteling ondersteunt, krijgt u daarvan een melding en krijgt u de optie het bericht in een niet-versleutelde indeling te versturen. Bijlagen die met versleutelde berichten worden meegestuurd, worden eveneens versleuteld.

Eén bericht versleutelen

1. Klik in een bericht dat u opstelt op **Bestand > Eigenschappen**.
2. Klik op **Beveiligingsinstellingen** en schakel het selectievakje **Berichttekst en bijlagen versleutelen** in.
3. Stel uw bericht op en klik op **Verzenden**.

Alle uitgaande berichten versleutelen

Wanneer u ervoor kiest standaard alle uitgaande berichten te versleutelen, kunt u berichten opstellen en verzenden op dezelfde manier als alle andere berichten. Alle potentiële ontvangers moeten dan echter over uw digitale id beschikken om het bericht te kunnen decoderen of weergeven.

1. Kies op het tabblad **Bestand** achtereenvolgens **Opties > Vertrouwenscentrum > Instellingen voor het Vertrouwenscentrum**.
2. Schakel op het tabblad **E-mailbeveiliging** onder **Versleutelde e-mail** het selectievakje **Alle inhoud en bijlagen voor uitgaande berichten versleutelen** in.
3. Klik op **Instellingen** als u nog meer opties wilt wijzigen, bijvoorbeeld als u een specifiek certificaat wilt gebruiken.

XII. Stappenplan bewustwording privacy voor klachtbehandelaars

Stap 1:

Voordat er wordt over gegaan moet de klachtbehandelaar zeker weten dat de cliënt op de hoogte is van de volgende informatie:

- ✓ Dat er persoonsgegevens worden opgeslagen;
- ✓ Identiteit van RADAR;
- ✓ Manier waarop de gegevens verkregen zijn;
- ✓ Dat er verwerking plaatsvindt voor het verlenen van bijstand en het registreren van de klachten;
- ✓ De wijze van dossiervorming;
- ✓ Wanneer een cliënt anoniem wil blijven, welke gevolgen dit heeft;
- ✓ Dat de cliënt een klacht kan indienen bij de Autoriteit Persoonsgegevens;
- ✓ Welke rechten een cliënt heeft en hoe zij/zij deze moet uitoefenen;
- ✓ Wie de ontvangers zijn van de gegevens;
- ✓ Dat RADAR gegevens mag verwerken doordat zij moeten voldoen aan een wettelijke verplichting;
- ✓ Contactgegevens RADAR en FG;
- ✓ Bewaartermijn persoonsgegevens;
- ✓ Risico's en regels van de verwerking;
- ✓ Toestemming geven is een verplichting voor het verwerken van bijzondere persoonsgegevens*;
- ✓ Op welke manier betrokkene zijn/haar toestemming kan intrekken;
- ✓ Toestemming mag geen vereiste zijn om bijstand te verlenen.

Stap 1 voldaan? Ga naar **stap 2**

Stap 1 niet voldaan? Breng de cliënt op de hoogte van bovenstaande informatie. Verwijs de cliënt naar de website.

Stap 2:

Is de toestemming voor verwerking van eventuele (bijzondere)persoonsgegevens* in goede orde ontvangen?

*Zo ja, ga naar **stap 3***

Zo nee, zorg dat de toestemming wordt gegeven voordat je begint aan de verwerking van (bijzondere) persoonsgegevens.*

Stap 3:

Is de verwerking van de persoonsgegevens nodig voor het verlenen van bijstand en/of registratie van de klacht? Neem de volgende punten mee bij de beslissing:

- ✓ Vul alleen de gegevens in die relevant zijn;
- ✓ Verwerk niet meer gegevens dan nodig is.
(Indien het een klacht betreft op geslacht, is het overbodig om de herkomst in te vullen.)

*Stap 3 voldaan? Ga naar **Stap 4***

Stap 3 niet voldaan? Verwijder irrelevante gegevens uit het dossier.

Stap 4:

Heeft de cliënt toestemming gegeven om persoonsgegevens door te sturen naar derden?

Ja, deze is gelijk gegeven met de toestemming voor de gegevensverwerking. Ga naar Stap 5

Nee? Zorg dat deze toestemming verkregen wordt. Dit kan door een toestemmingsformulier over de mail te verzenden.

Stap 5:

Worden er dossiers geprint?

Ja, zorg dat deze op een veilige manier bewaard worden.

Nee → de privacy van de cliënt is gewaarborgd.

***Bijzondere persoonsgegevens zijn gegevens omtrent godsdienst, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond of een strafrechtelijk verleden.**

XIII. Model verwerkersovereenkomst

Bron: www.privacycompany.eu

Verwerkersovereenkomst [NAAM BEDRIJF]

Datum: [invoeren datum] Contractspartijen:

STATUTAIRE NAAM

gevestigd te [PLAAT]



1. Verantwoordelijke te weten
[], statutair

S),

vertegenwoordigd door [NAAM EN/OF
NAAM BESTUURDER]

hierna te noemen: "Ik",

en



2. Verwerker te weten [STATUTAIRE
NAAM], statutair gevestigd te [PLAATS],

vertegenwoordigd door [NAAM EN/OF
NAAM BESTUURDER]

hierna te noemen: "Jij", gezamenlijk

aan te duiden als: "Wij";

Overwegende dat:

Wij hebben op [DATUM] een O [vereenkomst met
betrekking tot [OMSCHRIJVING] gesloten. Ter
uitvoering van onze Overeenkomst
worden Persoonsgegevens verwerkt.

Ik hecht grote waarde aan het beschermen van deze
Persoonsgegevens, daarom ben Ik verantwoordelijk
voor de gegevens die Jij gaat verwerken en leggen Wij
in deze Verwerkersovereenkomst en de daarbij
behorende bijlagen:

1. Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen
2. Overzicht met beveiligingsmaatregelen
3. Proces rondom het melden van Datalekken en de te verstrekken informatie

vast wat Jij wel en niet mag doen met de
Persoonsgegevens.



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

- 1.1 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 identifier zoals een
naam, een identificatienummer, locatiegegevens,
een online identifier of van een of meer
elementen die kenmerkend zijn voor de fysieke,
fysiologische, genetische, psychische,
economische, culturele of sociale identiteit van
die natuurlijke persoon
- 1.2 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;
- 1.3 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
verwerkingsverantwoordelijke is of volgens welke
criteria deze wordt aangewezen;

- 1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- 1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegevens betrekking hebben;
- 1.6 Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen;
- 1.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;
- 1.8 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");
- 1.9 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;



2. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Wij deze ondertekenen.
- 2.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
- 2.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.
- 2.4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor jou, zoals het melden van Datalekken, waarbij de Persoonsgegevens van mij betrokken zijn, en de plicht tot geheimhouding blijven voortduren.



3. Verwerken Persoonsgegevens

3.1 Jij zult alleen Persoonsgegevens verwerken in mijn opdracht en hebt geen zeggenschap over de Persoonsgegevens.

Jij volgt mijn instructies hierover op en je mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Ik jou daar van te voren toestemming of opdracht voor geef.

- 3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Jij precies zal verwerken en voor welke verwerkingsdoeleinden.
- 3.3 Jij houdt je aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.
- 3.4 Jij mag zonder mijn voorafgaande schriftelijke toestemming geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
- 3.5 Wanneer Jij met mijn toestemming andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.
- 3.6 Wanneer Ik een verzoek krijg van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werk je daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.



4. Beveiligen van Persoonsgegevens

- 4.1 Jij zorgt ervoor dat je de Persoonsgegevens voldoende beveiligt. Om verlies en onrechtmatige verwerkingen te voorkomen neem Jij passende technische en organisatorische maatregelen.
- 4.2 Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover neem je op in Bijlage 2.
- 4.3 Ter controle zal Jij aan mij ieder jaar een rapportage sturen waarin de genomen maatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor zul Jij aan mij geen kosten in rekening brengen.
- 4.4 Ik mag een inspectie of audit in jouw organisatie laten uitvoeren om te bepalen of het verwerken van de

Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zul Jij je medewerking verlenen, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

- 4.5 De kosten voor de uitvoering van deze audit zullen voor jouw rekening komen wanneer blijkt dat Jij je niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.
- 4.6 De controle op de algehele verwerking van Persoonsgegevens door jou kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. Jij zal hierbij aan Mij een rapport verstrekken waarin Jij aantoont dat je voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de jouw organisatie.
- 4.7 Wanneer een van ons vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Wij in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van degene die de kosten maakt.



5. Exporteren Persoonsgegevens 5.1

Jij mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande toestemming te hebben verkregen van mij.

6. Geheimhouding

- 6.1 Jij zult de aan jou verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.
- 6.2 Jij zult ervoor zorgen dat ook jouw personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.



7. Datalekken

- 7.1 In geval van een ontdekking van een mogelijk Datalek zul Jij mij hierover informeren binnen 24 uur via [e-mailadres en telefoonnummer] en mij de informatie verstrekken die is aangegeven in Bijlage 3, zodat Ik indien nodig een melding bij de Toezichthouder kan doen.
- 7.2 Na de melding van een Datalek aan mij, zul je mij op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die Jij hebt getroffen om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.
- 7.3 Het niet toegestaan dat Jij een melding van een Datalek doet aan de Toezichthouder en ook mag Jij de Betrokkenen niet informeren over het Datalek. Dit is mijn verantwoordelijkheid.
- 7.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.



8. Aansprakelijkheid

- 8.1 Als Jij jouw verplichtingen uit deze Verwerkersovereenkomst niet nakomt, stel Ik jou daarvoor aansprakelijk.
- 8.2 Jij bent aansprakelijk voor alle schade en nadeel geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door jouw werkzaamheden.
- 8.3 Indien Jij de verplichtingen in deze Verwerkersovereenkomst overtreedt, ben Jij aan mij een direct opeisbare boete verschuldigd van [BEDRAG] voor iedere overtreding en [BEDRAG] voor iedere dag dat je de overtreding begaat. Daarnaast behoud Ik het recht om schadevergoeding te vorderen.
- 8.4 Jij bent aansprakelijk voor de aan mij opgelegde bestuurlijke boete door de Toezichthouder als de geleden schade het gevolg is van jouw onrechtmatig of nalatig handelen.

- 8.5 Ik ben niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar Jij de samenwerking mee bent aangegaan of waarvan Jij Persoonsgegevens verwerkt, als dit het gevolg is van jouw onrechtmatig of nalatig handelen.



9. **Teruggave Persoonsgegevens en bewaartermijn** 9.1 Na het beëindigen van deze

Verwerkersovereenkomst geef Jij de Persoonsgegevens terug. Eventuele achtergebleven Persoonsgegevens zul je op een zorgvuldige en veilige manier vernietigen.

- 9.2 De Persoonsgegevens die Jij verwerkt volgens deze Verwerkersovereenkomst zul je vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van mij.



10. **Slotbepalingen**

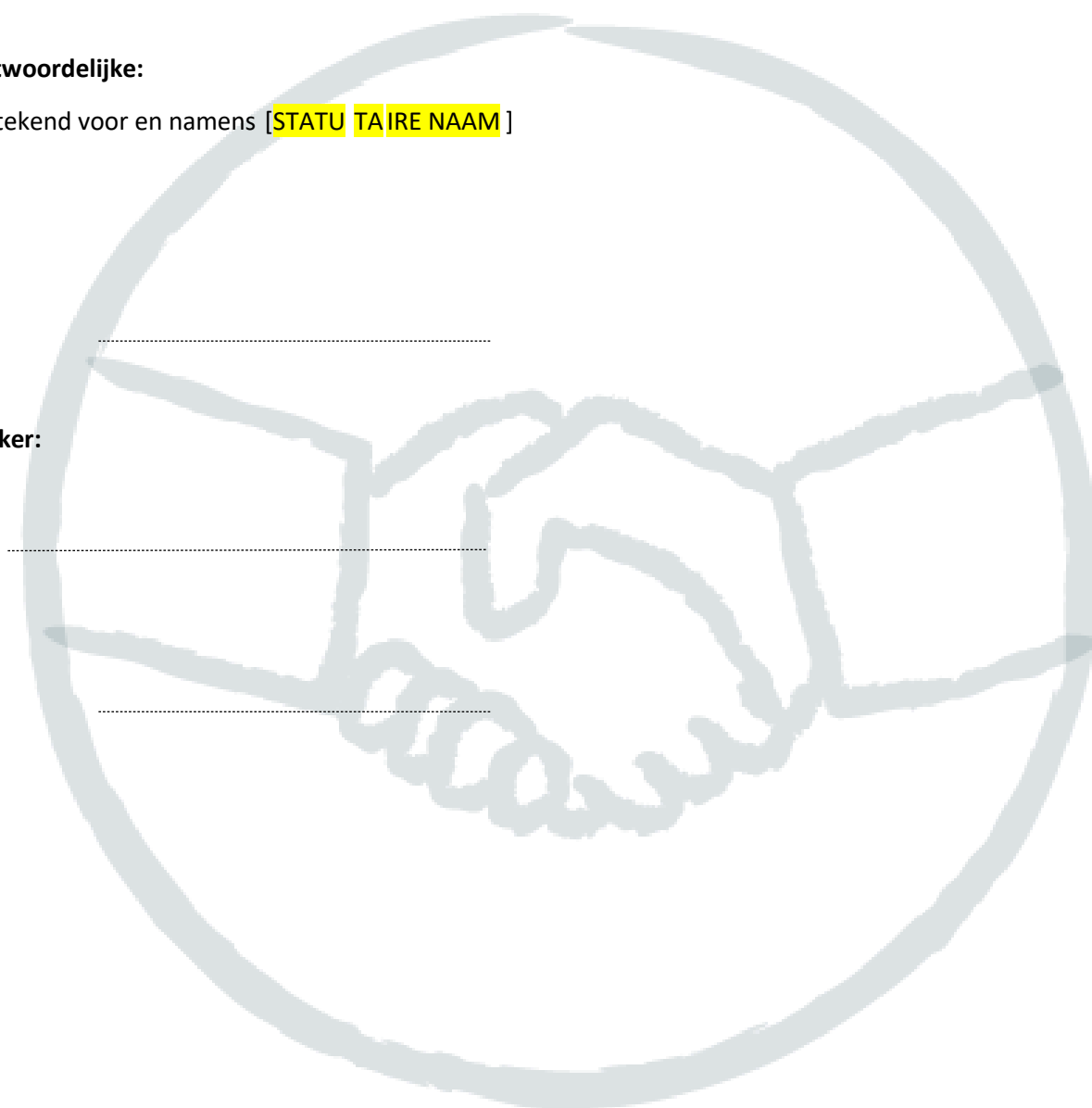
- 10.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.
- 10.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.
- 10.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Wij dit samen schriftelijk afspreken.

Aldus door ons overeengekomen en ondertekend:

Verantwoordelijke:

Ondertekend voor en namens [STATU TAIRE NAAM]

Bewerker:



Naam:

Functie:

Datum en plaats:

Handtekening:

Ondertekend voor en namens [STATUTAIRE NAAM]

Naam:

Functie:

Datum en plaats:

Handtekening:



Bijlage 1: Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen



Het onderstaande schema zal ingevuld moeten worden elke keer dat een Verwerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de persoonsgegevens worden verwerkt.

Beschrijving verwerkingsactiviteiten door Verwerker:	
Verwerkingsdoelen:	
Verwerkingsverantwoordelijke:	
Verwerker:	
Sub verwerkers:	
Verwerkte Persoonsgegevens:	
Locatie verwerkingen:	
Bewaartermijn:	



Bijlage 2: Overzicht met beveiligingsmaatregelen

Hier moet een overzicht van de beveiligingsnormen opgenomen worden die de Verwerkingsverantwoordelijke aan de Verwerker oplegt.

Om vast te stellen wat passende beveiligingsmaatregelen zijn moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- * Het soort persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. *Gaat het bijvoorbeeld om een naam of een emailadres, wat minder gevoelige persoonsgegevens zijn, of gaat het om het verwerken van een BSN.*
- * De hoeveelheid betrokkenen van wie gegevens worden verwerkt. *Hoe meer betrokkenen er zijn hoe meer eisen er worden gesteld aan de beveiliging van de gegevens.*
- * Het doel waarvoor gegevens worden verwerkt.
- * De duur en de wijze waarop gegevens bewaard moeten worden. Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.



Technische beveiligingsmaatregelen

- ☐ Up to date virusscan
- ☐ Beveiligde USB-sticks
- ☐ Accurate beveiliging medewerkerstelefoon
- ☐ Bitlocker toegangsmechanisme
- ☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)
- ☐ Versleutelde email
- ☐ Geen onbeveiligde externe harde schijven
- ☐ Geen onbeveiligde back ups maken
- ☐ Geen documenten op privé laptop op slaan



Organisatorische beveiligingsmaatregelen

- ☐ Clean desk policy
- ☐ Laptop niet onbemand achterlaten
- ☐ Laptop nooit achterlaten in de auto
- ☐ Privacy screens medewerkers
- ☐ Oude documenten op juiste manier vernietigen
- ☐ Zorgvuldig gebruik van USB-sticks



Bijlage 3: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met logingegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?

Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits)fraude mee kan worden gepleegd, zoals een Burgerservicenummer.
- Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen? - Worden de persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de [invoeren naam contactpersoon of afdeling].

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de [invoeren naam contactpersoon of afdeling]:

TEL: [invoeren telefoonnummer]

Of

E-MAIL: [invoeren e-mailadres].

Geef in je e-mail beantwoording op de onderstaande vragen.

Wij willen graag dat je de onderstaande vragen voor ons beantwoord. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De [invoeren naam contactpersoon of afdeling] kan je helpen met de beantwoording hiervan. Gaarne de 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 een 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?

Heb je 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.

XIV. Privacy statement

PRIVACY- EN COOKIEVERKLARING RADAR (concept)

RADAR is zich er van bewust dat een passende verwerking van persoonsgegevens een onmisbaar aspect is van het privacyrecht. Om dit recht te waarborgen, kunt u in deze verklaring nagaan wat er met uw gegevens gebeurt. De handelswijze van RADAR is vanzelfsprekend alvast in overeenstemming met de Algemene Verordening Gegevensbescherming, die in mei 2018 van kracht wordt.

Dit privacy statement is als volgt opgebouwd:

1. Doeleinden van gegevensverwerking (algemeen);
2. Marketingactiviteiten;
3. Beveiligingsniveau;
4. Rechten van betrokkenen;
5. Contactgegevens;.

1. Doeleinden van de gegevensverwerking (algemeen)

RADAR antidiscriminatiebureau is in het leven geroepen door de Wet Gemeentelijke Antidiscriminatievoorzieningen. In artikel 1 sub a van deze wet wordt genoemd dat een antidiscriminatievoorziening de taak heeft om burgers onafhankelijk bijstand te verlenen bij de afwikkeling van hun klachten gericht op discriminatie. In sub b wordt als kerntaak genoemd dat de klachten onder onderdeel a geregistreerd dienen te worden. De registratie en gegevensverwerking volgt door deze bepaling uit een wettelijke verplichting. Uit deze wettelijke bepaling blijkt dat het noodzakelijk is dat zij persoonsgegevens verwerken om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.

Voor de behandeling van klachten is het noodzakelijk om in ieder geval de postcode van de cliënt te hebben. Het blijft mogelijk om een anonieme melding te doen, maar indien er een klacht wordt ingediend is het hebben van een aantal persoonsgegevens cruciaal. Wanneer betrokkene ervoor kiest om tot bemiddeling over te gaan, kan het zijn dat er gegevens worden uitgewisseld met deze desbetreffende persoon of instantie. Wenst betrokkene geen bemiddeling dan worden er geen gegevens verstrekt aan derden.

2. Marketingactiviteiten

Welke informatie RADAR van u verzamelt, hangt af van hetgeen u doet wanneer u onze website bezoekt. Via de site worden geen persoonsgegevens verzameld, tenzij u ervoor kiest deze informatie te verschaffen via een informatieverzoek of klachtenformulier. Bij uw bezoek aan de website worden per opgevraagde pagina standaardgegevens verzameld en opgeslagen zoals de datum en tijd waarop de pagina is opgevraagd, het IP-adres en de browser. Deze gegevens worden uitsluitend gebruikt om de website te kunnen verbeteren en de dienstverlening te optimaliseren. Indien u per e-mail of via webformulieren persoonsgegevens aan RADAR verstrekt, worden deze verzameld en gebruikt voor het doel waarvoor u ze achterlaat en eventueel voor interne kwaliteitsonderzoeken om de dienstverlening te kunnen meten. Geanonimiseerd worden de gegevens gebruikt voor analyse, rapportage en onderzoek.

3. Beveiligingsniveau

RADAR beschermt de aan haar toevertrouwde gegevens met behulp van technische en organisatorische veiligheidsmaatregelen om het risico van verlies, misbruik, onbevoegde toegang, openbaarmaking en wijziging zo klein mogelijk te maken. Hierbij kunt u denken aan firewalls, versleuteling van gegevens en fysieke en administratieve toegangscontroles tot aan de data en servers.

4. Rechten van betrokkenen

Om de betrokkene te beschermen heeft de wet aan de betrokkene een aantal rechten toegekend. Deze rechten betreffen de zeggenschap van de betrokkene over zijn/haar persoonsgegevens. De Algemene Verordening Gegevensbescherming kent verschillende rechten toe aan personen van wie persoonsgegevens worden verwerkt. Deze rechten bieden meer middelen om de verwerking van hun persoonsgegevens te controleren en te beïnvloeden. Onderstaand worden de rechten van betrokkene opgesomd.

Recht op informatie

RADAR moet de betrokkenen op de hoogte houden van het feit dat er verwerking plaatsvindt van zijn persoonsgegevens. Daarnaast moet het, tijdens het verzamelen van de persoonsgegevens en vóór de verwerking, voor de betrokkene duidelijk zijn wat de doeleinden van de verwerking zijn. Mocht het doel van de verwerking veranderen, dan moet de betrokkene daarover geïnformeerd worden.

Recht van inzage

De verwerkingsverantwoordelijke moet de betrokkene de mogelijkheid geven om zijn of haar gegevens in te zien. RADAR zal bij een inwilliging van het inzagerecht, de betrokkene moeten informeren over de informatieverplichtingen.

Recht op rectificatie

Indien er onjuiste persoonsgegevens worden verwerkt heeft de betrokkene recht op rectificatie. Rectificatie houdt in dat er een aanvullende verklaring op basis van onvolledige gegevens kan worden ingediend.

Recht op gegevenswissing/ vergetelheid

De verwerkingsverantwoordelijke (RADAR) is verplicht persoonsgegevens van de betrokkene zonder onredelijke vertraging te wissen. Dit moet gebeuren als de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt. RADAR dient ook de gegevens te wissen als de betrokkene onverhoopt zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat. De gegevens moeten ook gewist worden als betrokkene bezwaar maakt tegen de verwerking of als de persoonsgegevens onrechtmatig verwerkt zijn.

Recht op beperking van de verwerking

Het recht op beperking van de verwerking houdt in dat er (tijdelijk) niet verwerkt of gewijzigd mag worden. Mocht er een beperking zijn, dan moet RADAR dit duidelijk in een bestand hebben aangegeven. Tevens moet de betrokkene op de hoogte worden gebracht van de beperking en ook als deze weer wordt opgeheven.

Recht op overdraagbaarheid / dataportabiliteit

Betrokkene hebben het recht om haar of zijn persoonsgegevens op te vragen die aan RADAR verstrekt zijn. Hierdoor ontstaat er voor betrokkene nog meer zeggenschap over zijn eigen persoonsgegevens. Een betrokkene heeft het recht om de gegevens van de verwerkingsverantwoordelijke te verkrijgen in gestructureerde, gangbare en machineleesbare vorm.

Recht van verzet/bezwaar

Betrokkenen hebben het recht om aan RADAR te vragen om hun persoonsgegevens niet meer te gebruiken. In de meeste gevallen is dit van toepassing op organisaties die de persoonsgegevens gebruiken voor marketingdoeleinden. Indien de betrokkene bezwaar maakt dient de RADAR de verwerking te staken.

5. Contactgegevens

De kantoren van **Antidiscriminatiebureau RADAR** zijn telefonisch bereikbaar van maandag t/m vrijdag van 9.00 uur tot 17.00 uur. 's Avonds en in het weekend is er een antwoordapparaat waarop u een bericht kunt inspreken. Ook kunt u altijd [per e-mail](#) contact met ons opnemen.

Op afspraak is het ook mogelijk een medewerker persoonlijk te spreken op een van onze vestigingen of op een locatie in uw woonplaats als daar afspraken over zijn gemaakt met de betreffende gemeente.

Met consumentenvragen n.a.v het programma **Radar (AVROTROS)** kunt u terecht op radar.avrotros.nl



Rotterdam-Rijnmond en Zuid-Holland-Zuid

Bezoekadres
Grotekerkplein 5,
3011 GC
Rotterdam

Telefoon
Rotterdam 010 411 39 11
Dordrecht 078 639 04 29

E-mail
info-rotterdam@radar.nl
info-dordrecht@radar.nl



Midden- en West-Brabant

Bezoekadres
Spoorlaan 432
5038 CX
Tilburg

Telefoon
Tilburg: 013 820 02 12
Breda: 076 530 91 37

E-mail
info-tilburg@radar.nl
info-breda@radar.nl



Brabant-Noord

Bezoekadres
Emmaplein 19d
5211 VZ
's-Hertogenbosch

Telefoon
073 744 01 18

E-mail
info-denbosch@radar.nl

E-mail algemeen info@radar.nl

Postadres voor alle locaties Postbus 1812 3000 BV Rotterdam

U kunt uw vragen en verzoeken rond de verwerking van persoonsgegevens richten tot:

***contactgegevens van de functionaris voor de gegevensbescherming toevoegen.**

XV. Privacy-gegevensbeschermingsbeleid RADAR

Privacy-gegevensbeschermingsbeleid RADAR, december 2017

Doeleinden gegevensverwerking

RADAR mag op grond van de Algemene Verordening Gegevensbescherming gegevens alleen verzamelen met het uitdrukkelijke doel klachtbehandeling, registratie en monitoring. Eén van de eisen die de AP stelt bij het inrichten van de gegevensverwerking is dat steeds nagegaan moet worden of het gebruik van persoonsgegevens noodzakelijk is voor het doel waarvoor de toestemming is verleend. Dit betekent dat er met minder gegevens hetzelfde doel bereikt kan worden en of niet langs een andere weg hetzelfde resultaat bereikt kan worden, bijvoorbeeld door met behulp van technische hulpmiddelen te bewerkstelligen dat we geen of zo min mogelijk persoonsgegevens gebruiken.

RADAR antidiscriminatiebureau is in het leven geroepen door de Wet Gemeentelijke Antidiscriminatievoorzieningen. In artikel 1 sub a van deze wet wordt genoemd dat een antidiscriminatievoorziening de taak heeft om burgers onafhankelijk bijstand te verlenen bij de afwikkeling van hun klachten gericht op discriminatie. In sub b wordt als kerntaak genoemd dat de klachten onder onderdeel a geregistreerd dienen te worden. De registratie en gegevensverwerking volgt door deze bepaling uit een wettelijke verplichting. Uit deze wettelijke bepaling blijkt dat het noodzakelijk is dat zij persoonsgegevens verwerken om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.

Categorieën van persoonsgegevensverwerking

Om de klacht te registreren, verzamelt de klachtbehandelaar een aantal persoonsgegevens. In de onderstaand tabel, wordt genoemd welke persoonsgegevens, bijzondere persoonsgegevens en welke discriminatiegronden worden verwerkt.

Algemene persoonsgegevens	Bijzondere persoonsgegevens (verplicht in te vullen *)	Keuze discriminatiegronden (optioneel, op grond van klacht)
Naam, achternaam en woonplaats	Nationaliteit	Arbeidscontract
Adres	Herkomst *	Arbeidsduur
Geslacht		Burgerlijke staat
E-mailadres		Geslacht
Telefoonnummer		Godsdienst
Geboortedatum		Handicap
		Leeftijd
		Levensovertuiging
		Nationaliteit
		Niet-wettelijke gronden
		Politieke gezindheid
		Ras
		Seksuele geaardheid

Beginnelsen verwerking van persoonsgegevens * aanvullen hoe RADAR aan deze beginselen gaat voldoen.

Beginnelsen van rechtmatigheid, behoorlijkheid en transparantie:

RADAR biedt op de website een privacystatement aan. Hierin staat genoemd welke rechten betrokkenen hebben. Er wordt duidelijk gemaakt welke informatie wordt verwerkt en waarvoor.

Dit beginsel legt RADAR de plicht om op de gegevens rechtmatig, behoorlijk en transparant te verwerken. Met rechtmatig wordt bedoeld op de rechtmatigheid en aanwezigheid van een gerechtvaardigde grondslag. Met behoorlijk en transparant wordt bedoeld dat er op een vertrouwelijke manier met de gegevens wordt omgegaan. De transparantie ziet er op dat het voor betrokkene duidelijk moet zijn welke gegevens van hem worden verwerkt en met welke reden.

Beginsel van doelbinding:

RADAR geeft aan waarvoor hij persoonsgegevens verzamelt. De doeleinden dienen gerechtvaardigd te zijn. Er mogen geen gegevens worden verwerkt die niet noodzakelijk zijn om het doel te bereiken. De verwerkingsverantwoordelijke dient zelf te beoordelen of het hergebruik van persoonsgegevens voor andere doeleinden, al dan niet verenigbaar is. Er zal rekening moeten worden gehouden met of er eventueel een verband bestaat tussen de doeleinden waarvoor de gegevens werden verkregen en de doeleinden van de voorgenomen verdere verwerking.

Beginsel van minimale gegevensverwerking:

De registratiesystemen zijn zo ingericht dat er geen onnodige persoonsgegevens worden verwerkt.

RADAR moet rekening houden met het principe van 'minimale gegevensverwerking'. Het beginsel van dataminimalisatie brengt met zich mee dat niet meer persoonsgegevens verwerkt mogen worden dan strikt noodzakelijk is voor het doel. Dit houdt in dat slechts de persoonsgegevens verzamelt mogen worden die nodig zijn om de taakvervulling goed te kunnen uitvoeren.

Beginsel van juistheid:

De persoonsgegevens dienen juist en actueel te zijn. Blijkt het dat gegevens onjuist of achterhaald zijn, dan moeten zij worden gewist. RADAR dient zelfstandig en actief zorg te dragen voor de juistheid van de persoonsgegevens die hij onder zich heeft.

Beginsel van opslagbeperking:

RADAR hanteert een bewaartermijn van vijf jaar.

De persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is. Er dient gezorgd te worden voor een passende beveiliging voor de persoonsgegevens en de persoonsgegevens moeten juist, actueel, toereikend en ter zake dienend zijn. De AVG noemt geen termijnen voor het bewaren van de persoonsgegevens. Diverse wetgeving verplichten de verwerkingsverantwoordelijke om bepaalde gegevens te bewaren gedurende een bepaalde periode.

Beginsel van integriteit en vertrouwelijkheid:

RADAR heeft alle medewerkers, stagiaires en vrijwilligers een geheimhoudingsovereenkomst laten tekenen.

Om de integriteit en vertrouwelijkheid te waarborgen, dient de verwerkingsverantwoordelijke technische en organisatorische beveiligingsmaatregelen te treffen. Dit om ongeoorloofde toegang en het ongeoorloofde gebruik van persoonsgegevens te voorkomen.

De beginselen van proportionaliteit en subsidiariteit:

Het evenredigheids- of proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. De grens ligt daar waar het middel niet in verhouding staat tot het doel, want dan is het optreden buiten proportie. Het subsidiariteitsbeginsel wordt beschouwd als een factor die een rol speelt in het kader van de evenredigheidstoets.

Het doel waarvoor de persoonsgegevens worden gebruikt, dient in redelijkheid niet op een andere, minder nadelige wijze te kunnen worden verwerkt.

Rechten betrokkenen

In het **protocol klachtbehandeling**, toegankelijk via onze website <https://radar.nl/read/protocol-klachtbehandeling-2014?sublist=507> is hierover het volgende opgenomen:

4.4.8 Registratie en privacybescherming

De cliënt wordt geïnformeerd over de wijze van dossiervorming en hoe met deze gegevens wordt omgegaan. De persoonsgegevens blijven vertrouwelijk. De cliënt wordt verteld dat deze nooit zonder zijn of haar persoonlijke toestemming beschikbaar worden gesteld aan derden. De cliënt heeft na afspraak recht op inzage in het eigen dossier. RADAR is gebonden aan de Wet Bescherming Persoonsgegevens.

Recht op informatie

RADAR moet de betrokkenen op de hoogte houden van het feit dat er verwerking plaatsvindt van zijn persoonsgegevens. Daarnaast moet het, tijdens het verzamelen van de persoonsgegevens en vóór de verwerking, voor de betrokkene duidelijk zijn wat de doeleinden van de verwerking zijn. Mocht het doel van de verwerking veranderen, dan moet de betrokkene daarover geïnformeerd worden.

Recht van inzage

De verwerkingsverantwoordelijke moet de betrokkene de mogelijkheid geven om zijn of haar gegevens in te zien. RADAR zal bij een inwilliging van het inzagerecht, de betrokkene moeten informeren over de informatieverplichtingen.

Recht op rectificatie

Indien er onjuiste persoonsgegevens worden verwerkt heeft de betrokkene recht op rectificatie. Rectificatie houdt in dat er een aanvullende verklaring op basis van onvolledige gegevens kan worden ingediend.

Recht op gegevenswissing/ vergetelheid

De verwerkingsverantwoordelijke (RADAR) is verplicht persoonsgegevens van de betrokkene zonder onredelijke vertraging te wissen. Dit moet gebeuren als de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt. RADAR dient ook de gegevens te wissen als de betrokkene onverhoopt zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat. De gegevens moeten ook gewist worden als betrokkene bezwaar maakt tegen de verwerking of als de persoonsgegevens onrechtmatig verwerkt zijn.

Recht op beperking van de verwerking

Het recht op beperking van de verwerking houdt in dat er (tijdelijk) niet verwerkt of gewijzigd mag worden. Mocht er een beperking zijn, dan moet RADAR dit duidelijk in een bestand hebben aangegeven. Tevens moet de betrokkene op de hoogte worden gebracht van de beperking en ook als deze weer wordt opgeheven.

Recht op overdraagbaarheid / dataportabiliteit

Betrokkene hebben het recht om haar of zijn persoonsgegevens op te vragen die aan RADAR verstrekt zijn. Hierdoor ontstaat er voor betrokkene nog meer zeggenschap over zijn eigen persoonsgegevens. Een betrokkene heeft het recht om de gegevens van de verwerkingsverantwoordelijke te verkrijgen in gestructureerde, gangbare en machineleesbare vorm .

Recht van verzet/bezwaar

Betrokkenen hebben het recht om aan RADAR te vragen om hun persoonsgegevens niet meer te gebruiken. In de meeste gevallen is dit van toepassing op organisaties die de persoonsgegevens gebruiken voor marketingdoeleinden. Indien de betrokkene bezwaar maakt dient de RADAR de verwerking te staken.

Persoonsgegevensbeveiliging

De medewerker draagt er zorg voor dat privacy-gevoelige gegevens vertrouwelijk worden behandeld en op zodanige wijze worden geadministreerd en gearhiveerd dat de vertrouwelijkheid optimaal is gewaarborgd. Dat houdt concreet in dat dossiers buiten kantoor tijden worden bewaard in een afgesloten kluis. Toch kunnen er zich omstandigheden voor doen dat dossiers mee worden genomen buiten het kantoor en buiten werktijd. In principe wordt een kopie met de noodzakelijke gegevens meegenomen. Met dossiers en dossiergegevens moet buiten kantoor uiterst zorgvuldig worden omgegaan. Dat wil zeggen niet uit het oog verliezen en thuis op een veilige plek opbergen. Als het niet anders mogelijk is dan dat dossiers meegenomen worden naar buiten, dient zich altijd een kopie van de eerste pagina (met contactgegevens) op kantoor in de kluis te bevinden. Deze privacybepaling geldt ook ten aanzien van wachtwoorden voor het computerprogramma's, telebankieren en dergelijke vertrouwelijke gegevens. Deze wachtwoorden worden niet doorgegeven en er wordt zorgvuldig mee om gegaan. Op basis van de privacywetgeving zijn de databestanden waar de klachtbehandelaars mee werken alleen voor hen toegankelijk. De klachtbehandelaars werken ermee en voor hen is er een doel om toegang te hebben tot deze gegevens. Ook de monitormedewerkers hebben toegang tot de klachtgegevens omdat zij de informatie hieruit controleren en verwerken. Verder is het zo georganiseerd dat medewerkers alleen toegang hebben tot de klachten en meldingen van de vestiging waar zij werken.

***aanvullen met informatie over de beveiliging van outlook en het registratiesysteem**

Bewaartermijn

RADAR hanteert voor het bewaren van persoonsgegevens, de bewaartermijn genoemd in de Archiefwet. RADAR heeft gekozen om de papierendossiers te bewaren voor een periode van vijf jaar. **In de offerte van Constant-IT is opgenomen dat digitale dossiers een bewaarduur van een periode van maximaal vijf jaar heeft.**

***bewaartermijn met Enigmatry toevoegen**



XVI. Toestemmingsformulier

Toestemming is doorgaans niet vereist voor de verwerking van persoonsgegevens bij RADAR. Er zal dus niet altijd gebruik hoeven te worden gemaakt van toestemming als grondslag voor de verwerking van persoonsgegevens. Het vragen van toestemming als grondslag voor gegevensverwerking is wél nodig als bijzondere persoonsgegevens worden verwerkt ten behoeve van het verlenen van bijstand. Wanneer klachten gericht zijn op: ras, nationaliteit, godsdienst, handicap, gezondheid of seksuele voorkeur, dient er toestemming te worden verleend voor het registreren van deze persoonsgegevens. Daarnaast is er toestemming nodig om te bemiddelen tussen partijen. Wanneer u ervoor kiest om de klacht te laten bemiddelen, worden er persoonsgegevens uitgewisseld met de wederpartij. Wanneer u niet tot bemiddeling wil overgaan dient u een kruis te zetten in onderstaande tekst.

**vóór gelijke behandeling
tegen discriminatie**

Met dit formulier geef iktoestemming **om gegevens over mij te verwerken.** Het gaat om gegevens over mij die door RADAR worden geregistreerd.

Met dit formulier geef iktoestemming **om gegevens van mij te delen met de wederpartij.** Het gaat om gegevens over mij die door RADAR worden geregistreerd.

Hieronder zie ik voor welke gegevensverwerkingen ik toestemming geef.

Ik geef toestemming onder deze voorwaarden:

- Mijn toestemming geldt alleen voor de hieronder beschreven redenen, gegevens en personen / instellingen. Voor nieuwe gegevensverwerkingen vraagt RADAR mij opnieuw om toestemming;
- RADAR informeert mij over de gegevens die over mij worden uitgewisseld en de gegevens die over mij worden geregistreerd. Dat betekent bijvoorbeeld dat het RADAR mij uitlegt om welke specifieke gegevens het gaat en waarom deze gegevens noodzakelijk zijn om mij te kunnen helpen;
- Als gegevens niet (meer) noodzakelijk zijn zal RADAR deze niet registreren dan wel verwijderen;
- Ik kan ervoor kiezen om geen toestemming te geven of om alleen voor bepaalde delen toestemming te geven. RADAR legt uit wat de gevolgen voor mijn hulpverlening zijn als ik (voor bepaalde) gegevens of personen geen toestemming geeft;
- Ik mag mijn toestemming op elk moment intrekken. In sommige gevallen zal het intrekken van toestemming gevolgen hebben voor mijn hulpverlening. RADAR zal mij hier van geval tot geval over informeren.
- Indien ik ervoor kies om over te gaan tot bemiddeling, geef ik toestemming om contact op te nemen met de wederpartij. Mijn persoonsgegevens mogen worden uitgewisseld om te bemiddelen.

Datum

Handtekening

.....