

VERWERKERSOVEREENKOMST

PARTIJEN:

1. Politie, (statutair) gevestigd te Den Haag, te dezen vertegenwoordigd door mevrouw P.F. Bosman, directeur Politiedienstencentrum (wnd.), hierna te noemen "**Politie**",
2. 5.1.2.i , hierbij rechtsgeldig vertegenwoordigd door 5.1.2.e , in diens hoedanigheid als 5.1.2.e , hierna te noemen 5.1.2.i ,"

de partijen zijn hierna eveneens gezamenlijk te noemen de "**Partijen**" en elk afzonderlijk een "**Partij**";

OVERWEGEN:

- (A) Politie en 5.1.2.i hebben op 1 januari 2018 de Hoofdovereenkomst met contractnummer 5.1.2.i gesloten voor het verrichten van e-HRM diensten door 5.1.2.i aan Politie. Op grond hiervan Verwerkt 5.1.2.i in opdracht van Politie Persoonsgegevens. Deze Verwerkersovereenkomst maakt als bijlage onlosmakelijk deel uit van de Hoofdovereenkomst;
- (B) Partijen zijn van mening dat Politie kwalificeert als "Verwerkingsverantwoordelijke" in de zin van de Algemene Verordening Gegevensbescherming ("**AVG**") en dat 5.1.2.i kwalificeert als "Verwerker" in de zin van de AVG met betrekking tot deze Persoonsgegevens;
- (C) Politie stelt aan 5.1.2.i Persoonsgegevens ter beschikking om ten behoeve van haar te Verwerken; en
- (D) Politie en 5.1.2.i wensen, mede gezien artikel 28 AVG, de opdracht tot en nadere afspraken omtrent de Verwerking van Persoonsgegevens door 5.1.2.i ten behoeve van Politie vast te leggen in deze Verwerkersovereenkomst;

EN ZIJN ALS VOLGT OVEREENGEKOMEN:

1. Definities

In deze Verwerkersovereenkomst worden de navolgende begrippen gebruikt, waarbij geldt dat definities uit de AVG worden uitgelegd conform hun wettelijke betekenis:

AVG:	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.
Betrokkene:	degene op wie een Persoonsgegeven betrekking heeft, zoals nader aangeduid in Bijlage 1 ;
Datalek:	een inbreuk op de beveiliging, zoals bedoeld in artikel 4 lid 12 AVG, 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;

Hoofdovereenkomst:	de overeenkomst tussen Partijen zoals aangeduid in overweging A.
Persoonsgegevens:	alle informatie over een geïdentificeerde of identificeerbare natuurlijke personen (de "betrokkenen") als bedoeld in art. 4 lid 1 AVG die 5.1.2.1 in opdracht en ten behoeve van Politie Verwerkt in het kader van de Hoofdovereenkomst, zoals nader aangeduid in Bijlage 1 ;
Subverwerker:	een door 5.1.2.1 ingeschakelde verwerker van Persoonsgegevens;
Toepasselijke Regelgeving:	de AVG, UAVG en daarop gebaseerde regelgeving voor zover van toepassing op Politie;
UAVG:	Uitvoeringswet Algemene verordening gegevensbescherming;
Verwerken:	het verrichten van (een) Verwerking(en);
Verwerking:	een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procédés, 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, zoals bedoeld in art. 4 lid 2 AVG;

Verwerkersovereenkomst deze verwerkersovereenkomst.

2. Verwerking

- 2.1 5.1.2.1 zal ten behoeve van Politie Persoonsgegevens Verwerken in overeenstemming met de bepalingen van deze Verwerkersovereenkomst.
- 2.2 5.1.2.1 heeft voor de duur van de Hoofdovereenkomst de opdracht gekregen van de Politie om ter uitvoering van de tussen partijen gesloten Hoofdovereenkomst namens Politie de Persoonsgegevens te Verwerken overeenkomstig Bijlage 1 waarin staat beschreven, per dienst:
 - de categorieën Persoonsgegevens die worden Verwerkt;
 - de categorieën Betrokkenen;
 - de doeleinden van de Verwerking;
 - de locaties waarop 5.1.2.1 de Persoonsgegevens uitsluitend zal Verwerken.
- 2.3 De Verwerking door 5.1.2.1 van Persoonsgegevens zal voldoen aan de Toepasselijke Regelgeving.
- 2.4 5.1.2.1 zal de Persoonsgegevens uitsluitend Verwerken in overeenstemming met de Hoofdovereenkomst en eventuele aanvullende schriftelijke Verwerkingsinstructies die door Politie zijn bekendgemaakt en steeds in overeenstemming met de verplichtingen voortvloeiend uit deze Verwerkersovereenkomst. Het is 5.1.2.1 nadrukkelijk verboden om andere Verwerkingen te verrichten. Politie mag gegeven instructies altijd schriftelijk wijzigen,

aanvullen of intrekken. Artikel 14.7 is van toepassing in geval van een verandering van instructie.

- 2.5 Indien ^{5.1.2.i} van mening is dat een Verwerkingsinstructie van Politie een inbreuk oplevert op de Toepasselijke Regelgeving, dan stelt zij Politie hiervan onmiddellijk in kennis.
- 2.6 ^{5.1.2.i} zal erop toezien dat overdrachten van Persoonsgegevens naar (of toegang door ^{5.1.2.i} vanuit) een land of een organisatie buiten de EER of, een land betreft zoals beschreven in artikel 45 van de AVG ofwel dat passende waarborgen worden geboden zoals beschreven in artikel 46 van de AVG, en dat dergelijke overdrachten en veiligheidsmechanismen worden gedocumenteerd overeenkomstig artikel 30 lid 2 van de AVG.
- 2.7 Als ^{5.1.2.i} op grond van een op ^{5.1.2.i} van toepassing zijnde dwingendrechtelijke bepaling van het recht de Europese Unie of een lidstaat van de Europese Unie verplicht is om de Persoonsgegevens te verwerken in afwijking van de instructies van Politie, dan zal ^{5.1.2.i} Politie hierover voorafgaand informeren, behalve indien en voor zolang dit niet is toegestaan op grond van de genoemde dwingendrechtelijke bepaling.
- 2.8 De in artikel 2.2 gegeven opdracht eindigt zodra de verplichtingen uit de Hoofdovereenkomst en deze Verwerkersovereenkomst zijn vervuld, of zoveel eerder als Politie de opdracht schriftelijk beëindigt, onverminderd de verplichtingen die ^{5.1.2.i} nog heeft tot afronding zoals voortvloeiend uit deze Verwerkersovereenkomst. Politie is voor het naleven van de conform artikel 2.4 gewijzigde instructies door ^{5.1.2.i} geen extra vergoeding verschuldigd voor zover wijziging van instructies nodig is om te zorgen dat Politie aan de Toepasselijke Regelgeving kan (blijven) voldoen, tenzij het voldoen aan de Toepasselijke Regelgeving op dat specifieke punt de verantwoordelijkheid van de Politie als Verwerkingsverantwoordelijke is. In andere gevallen zullen Partijen in gezamenlijk overleg de verschuldigdheid en hoogte van een eventuele aanvullende vergoeding bepalen.
- 2.9 Behoudens het in artikel 2.7 bepaalde, wordt de vergoeding voor de door ^{5.1.2.i} te verlenen diensten op basis van deze Verwerkersovereenkomst geacht te zijn inbegrepen in afspraken zoals deze door partijen zijn gemaakt in de Hoofdovereenkomst.
- 3. Register en Medewerking** ^{5.1.2.i}
- 3.1 ^{5.1.2.i} houdt een register bij van alle categorieën van Verwerkingen die zij ten behoeve van Politie verricht als bedoeld in art. 30 lid 2 AVG.
- 3.2 Rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie zal ^{5.1.2.i} Politie bijstand verlenen bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 31 tot en met 36 van de AVG.
- 3.3 Op het eerste verzoek van Politie zal ^{5.1.2.i} medewerking verlenen aan toezichthoudende autoriteiten bij de vervulling van hun taken. ^{5.1.2.i} zal Politie onverwijld op de hoogte stellen vanaf het eerste moment van zowel formeel als informeel contact met een toezichthouder voor zover dit verband houdt met de dienstverlening van ^{5.1.2.i} aan Politie en zal Politie op de hoogte houden van de gebeurtenissen hieromtrent.
- 4. Subverwerkers**
- 4.1 ^{5.1.2.i} is niet bevoegd om de Persoonsgegevens op enige wijze door Subverwerkers te laten Verwerken, anders dan als toegestaan ingevolge deze Verwerkersovereenkomst.

42 Politie is akkoord met het inschakelen van de Subverwerkers die op het moment van tekenen van deze Verwerkersovereenkomst zijn vermeld in **Bijlage 2** voor de daargenoemde diensten. In **Bijlage 2** wordt een onderscheid gemaakt tussen de Subverwerkers waarvoor Politie een algemene toestemming geeft en de Subverwerkers waarvoor Politie een specifieke toestemming geeft. Algemene toestemming is vereist voor Subverwerkers die 5.1.2.i inschakelt in het kader van producten en diensten die 5.1.2.i op de markt brengt. Specifieke toestemming is vereist voor Subverwerkers die 5.1.2.i inschakelt in het kader van producten en diensten van derden die via 5.1.2.i worden aangeboden, welke producten en diensten in beheer zijn van derden en welke niet door of in opdracht van 5.1.2.i zijn ontwikkeld.

4.3 In het geval van een beoogde verandering inzake de toevoeging of vervanging van Subverwerkers waarvoor Politie een algemene toestemming geeft, licht 5.1.2.i Politie hierover vooraf in, waarbij Politie de mogelijkheid wordt geboden om tegen deze verandering bezwaar te maken. Een eventueel bezwaar van Politie wordt verwacht binnen 4 weken nadat Politie hierover is geïnformeerd door 5.1.2.i. Het is Politie toegestaan bezwaar te maken op redelijke gronden, waarbij de volgende omstandigheden in ieder geval, doch niet limitatief, geacht worden redelijke gronden te zijn:

- a. de beoogde andere Subverwerker zal Persoonsgegevens buiten de Europese Economische Ruimte Verwerken, is niet gebonden aan bindende bedrijfsvoorschriften voor Verwerkers, niet gecertificeerd op basis van de EU-US Privacy Shield, en is niet bereid akkoord te gaan met standaardbepalingen inzake gegevensbescherming die conform artikel 46 AVG zijn vastgesteld;
- b. Politie aannemelijk kan maken dat het onwaarschijnlijk is dat de beoogde andere Subverwerker zal kunnen voldoen aan de verplichtingen voortvloeiend uit deze Verwerkersovereenkomst;
- c. Politie aannemelijk kan maken dat het aannemelijk is dat het inschakelen of de vervanging van de beoogde andere Subverwerker een onredelijk risico inhoudt voor de bescherming van Persoonsgegevens; of
- d. Een ander zwaarwegende belang van Politie dat zich tegen de inschakeling van de Subverwerker verzet.

In het geval Politie tijdig en op redelijke gronden bezwaar maakt tegen het inschakelen of de vervanging van de beoogde Subverwerker, dan is het 5.1.2.i toegestaan om binnen een redelijke termijn een alternatief te bieden om de relevante dienst voort te zetten. Indien dat alternatief redelijkerwijs niet acceptabel is voor Politie, of indien 5.1.2.i geen alternatief biedt, dan is het haar toegestaan om die relevante dienst op te zeggen, die niet zonder het inschakelen of de vervanging van de beoogde andere Subverwerker kan worden verleend.

4.4 In het geval van een beoogde verandering inzake de toevoeging of vervanging van Subverwerkers waarvoor Politie een specifieke toestemming geeft, licht 5.1.2.i Politie hierover vooraf in, waarna 5.1.2.i met Politie in overleg treedt om goedkeuring te krijgen voor deze verandering.

4.5 5.1.2.i is verantwoordelijk en aansprakelijk voor door haar ingeschakelde Subverwerkers in de nakoming van diens verplichtingen ten aanzien van de Verwerking van Persoonsgegevens. 5.1.2.i dient in ieder geval die voorwaarden te verbinden aan deze inschakelingen die equivalent zijn aan de voorwaarden onder deze Verwerkersovereenkomst. Op eerste verzoek van Politie verstrekt 5.1.2.i aan Politie details over de met deze Subverwerker(s) gesloten

Subverwerkersovereenkomst(en).

- 4.6 ^{5.1.2.i} zal voor iedere Subverwerker jaarlijks een review uitvoeren op de gesloten Subverwerkersovereenkomst, werkzaamheden en assurance (rapportages). Een kopie van de betreffende reviews stelt ^{5.1.2.i} op verzoek ter beschikking aan Politie.

5. Verzoeken van betrokkenen of instanties

- 5.1 Op verzoek van Politie zal ^{5.1.2.i} Politie steeds onmiddellijk toegang verlenen tot de Persoonsgegevens. Ook zal ^{5.1.2.i} binnen twee (2) weken na verzoek van Politie (i) een kopie aan Politie verstrekken van alle Persoonsgegevens dan wel Persoonsgegevens betreffende een bepaalde persoon die in zijn bezit of beheer zijn alsmede een kopie van alle documenten waarin deze Persoonsgegevens zijn opgenomen en een overzicht van alle systemen waarin deze Persoonsgegevens zijn opgenomen en alle overige Verwerkingen van deze Persoonsgegevens die door ^{5.1.2.i} worden uitgevoerd in zodanig format als Politie redelijkerwijs verzoekt, (ii) bepaalde Persoonsgegevens verwijderen, blokkeren of corrigeren conform aanwijzingen van Politie, of (iii) vastleggen dat aan bepaalde verzoeken tot verwijdering, blokkering of correctie geen gevolg wordt gegeven en de redenen hiervan.
- 5.2 Indien ^{5.1.2.i} zelf verzoeken (zoals verzoeken om inzage, rectificatie, gegevenswissing of beperking van de Verwerking van Persoonsgegevens) ontvangt van Betrokkenen, zal ^{5.1.2.i} deze onverwijld aan Politie doorsturen. ^{5.1.2.i} zal niet zonder tussenkomst van Politie gehoor geven aan een AVG verzoek van een betrokkene. ^{5.1.2.i} zal binnen twee (2) weken na ontvangst van het verzoek om inzage van Persoonsgegevens een kopie aan Politie verstrekken van alle Persoonsgegevens betreffende deze Betrokkene die in zijn bezit of beheer zijn alsmede een kopie van alle documenten en een overzicht van alle systemen waarin deze Persoonsgegevens zijn opgenomen en alle overige Verwerkingen van deze Persoonsgegevens die door ^{5.1.2.i} worden uitgevoerd.
- 5.3 ^{5.1.2.i} zal de in de artikelen 5.1 en 5.2 bedoelde handelingen verrichten binnen de in deze artikelen aangegeven termijn dan wel enige andere termijn die Politie in afwijking hiervan in redelijkheid heeft vastgesteld.
- 5.4 ^{5.1.2.i} stelt Politie onverwijld in kennis indien een daartoe bevoegde instantie een juridische bindend verzoek om verstrekking van de Persoonsgegevens heeft gedaan, tenzij het ^{5.1.2.i} omwille van gewichtige redenen van algemeen belang niet is toegestaan Politie hiervan in kennis te stellen, zoals in het geval van een strafrechtelijk gebod om de vertrouwelijkheid van een rechtshandavingsonderzoek te bewaren.
- ## 6. Geheimhouding, beveiliging en auditrecht
- 6.1 ^{5.1.2.i} zal conform artikel 32 AVG passende technische en organisatorische maatregelen nemen teneinde de Persoonsgegevens te beschermen tegen vernietiging, verlies of onrechtmatige verstrekking of andere onrechtmatige Verwerking, waaronder onnodige verzameling en verdere Verwerking van Persoonsgegevens. De beveiligingsmaatregelen die door ^{5.1.2.i} op het moment van aangaan worden getroffen zijn omschreven op www.^{5.1.2.i}.nl/ ^{5.1.2.i} **Bijlage 3** bevat een momentopname van de voornoemde website, de huidige ^{5.1.2.i} in control'-statement en de huidige 'Statement of Applicability ISO27001'. Partijen zijn zich ervan bewust dat dit aan verandering onderhevig is en dat de Politie altijd de meest recente versies kan inzien en/of opvragen.
- 6.2 ^{5.1.2.i} zal ervoor zorgen dat alleen de door haar gemachtigde personen die nodig zijn om de Persoonsgegevens te Verwerken, toegang zullen hebben tot de Persoonsgegevens. ^{5.1.2.i} zal deze medewerkers adequaat instrueren en ervoor zorgen dat zij zich contractueel hebben

verbonden om vertrouwelijkheid in acht nemen en bekend zijn met de verantwoordelijkheden en verplichtingen uit hoofde van de Toepasselijke Regelgeving.

- 6.3 ^{5.1.2.i} beheerst haar processen door middel van een stelsel van beheersmaatregelen op de invoer, het Verwerkingsproces en de uitvoer. Daarnaast worden ook de IT processen met een stelsel van beheersmaatregelen beheerst. Deze maatregelen zijn vastgelegd in een beheersraamwerk. De beheersmaatregelen worden jaarlijks getoetst door een onafhankelijke auditor en vastgelegd in een ISAE3402 type II mededeling. Op verzoek van Politie zal ^{5.1.2.i} de conclusies van deze toetsing ter beschikking stellen. Daarnaast zijn de informatiebeveiligingsmanagementsystemen conform ISO27001 gecertificeerd.
- 6.4 ^{5.1.2.i} behoudt zich het recht voor de ISO 27001 certificering en de ISAE 3402 type II mededelingen te vervangen door een andere adequate en algemeen geaccepteerde verklaring en/of normenkader gebaseerd op nationale of internationale standaarden. Indien ^{5.1.2.i} dit voornemen heeft zal zij dit tijdig kenbaar maken aan de Politie en kunnen Partijen in gesprek gaan over eventuele vraagstukken/bezwaren.
- 6.5 ^{5.1.2.i} treft de maatregelen bedoeld in artikel 6.1 voordat met de Verwerking wordt aangevangen en zorgt dat gedurende de gehele looptijd van de Verwerkersovereenkomst een adequaat beveiligingsniveau is gegarandeerd, indien nodig door aanpassingen op de beveiligingsmaatregelen waarbij rekening dient te worden gehouden met de stand van de techniek, de uitvoeringskosten, alsook de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.
- 6.6 ^{5.1.2.i} stelt aan Politie desgevraagd alle informatie ter beschikking die Politie nodig acht om nakoming van de verplichtingen van ^{5.1.2.i} op grond van deze Verwerkersovereenkomst aan te tonen. Om aan deze verplichting te kunnen voldoen, zal ^{5.1.2.i} alle ter zake relevante informatie documenteren en deugdelijk archiveren.
- 6.7 Politie heeft het recht om audits uit te voeren onder de voorwaarden zoals gesteld in dit artikel. Indien Politie een verzoek tot het verrichten van een audit doet conform de voorwaarden van dit artikel, zal ^{5.1.2.i} die locaties voor een audit ter beschikking stellen waar Persoonsgegevens worden Verwerkt ten behoeve van Politie. ^{5.1.2.i} biedt alle medewerking en informatie die Politie redelijkerwijs nodig heeft voor de audit. Een dergelijke audit zal worden uitgevoerd door een onafhankelijke derde partij, welke partij door Politie wordt geselecteerd. Indien ^{5.1.2.i} aannemelijk kan maken dat het voor ^{5.1.2.i} onredelijk is dat de audit uit wordt gevoerd door de geselecteerde partij, treden Partijen hierover in overleg. Deze partij zal ten minste gekwalificeerd zijn als (IT-)auditor en ten minste geaccrediteerd zijn als Register Controller, Register Accountant of Register EDP-auditor. In afwijking van het voorgaande heeft Politie het recht om haar eigen auditdienst V&I of een in cybersecurity gespecialiseerde derde partij van goede reputatie in te schakelen in geval van een ernstig en urgent beveiligingsprobleem dat specifiek betrekking heeft op de Politie. De (interne en externe) kosten van een audit zijn voor rekening van Politie, tenzij uit de audit blijkt dat ^{5.1.2.i} wezenlijk tekortkomt of tekort is gekomen in de nakoming van haar verplichtingen opgenomen in deze Verwerkersovereenkomst. Vóór de aanvang van een audit zullen Partijen met elkaar overeenkomen wat de scope, planning en de duur van de audit zal zijn, en eveneens bepalen welke tarieven gelden voor de geboden ondersteuning van Verwerker (en haar Subverwerkers). De tarieven worden in redelijkheid vastgesteld en op voorhand besproken. ^{5.1.2.i} zal aan haar medewerking geen andere voorwaarden stellen dan ondertekening van een gangbare en niet onnodig bezwarende geheimhoudingsverklaring door de derde partij. Indien ^{5.1.2.i} een intern of extern recent (niet ouder dan een jaar) auditrapport kan overleggen dat

toeziet op dezelfde locaties als waarvoor Politie een audit verzoekt, is het 5.1.2.i toegestaan om eerst dit auditrapport te overleggen aan Politie. Indien Politie meent dat de omvang van de audit, auditopdracht, de gebruikte methode(s) of wijze van rapportage onvoldoende is voor Politie om de nakoming van deze Verwerkersovereenkomst te kunnen vaststellen dan is het Politie toegestaan om alsnog zelf een audit te laten voeren. Het is 5.1.2.i toegestaan, na in hiertoe toestemming te hebben gevraagd en gekregen van Politie, deze audit-rapportage te gebruiken voor haar andere klanten. Het recht om een audit te doen verrichten bij 5.1.2.i blijft bestaan tot twaalf maanden na ontvangst van de in artikel 13.1 genoemde schriftelijke verklaring.

7. Inbreuk in verband met persoonsgegevens (datalek)

- 7.1 Indien er sprake is van een Datalek waarbij de Persoonsgegevens die 5.1.2.i of de door haar ingeschakelde Subverwerkers Verwerken zijn betrokken, dan stelt 5.1.2.i Politie zonder vertraging, en in ieder geval binnen 36 uur, na kennisgeving daarvan op de hoogte. 5.1.2.i voorziet Politie daarbij van alle, redelijkerwijs benodigde informatie, waaronder in ieder geval begrepen de informatie als bedoeld in artikel 33 lid 3 AVG, om Politie in staat te stellen zulks - indien vereist op grond van artikel 33 en 34 AVG - tijdig, juist en volledig te melden aan de Autoriteit Persoonsgegevens en de relevante Betrokkenen.
- 7.2 Bij het aanleveren van de informatie zoals bedoeld in artikel 7.1 levert 5.1.2.i de informatie aan zoals deze door de Autoriteit Persoonsgegevens wordt opgevraagd middels de door haar vastgestelde standaardformulieren. Daarnaast is de functionaris gegevensbescherming van 5.1.2.i beschikbaar voor eventuele vervolgvragen van Politie.
- 7.3 5.1.2.i documenteert alle Datalekken, inclusief de feiten omtrent een Datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. 5.1.2.i houdt documentatie beschikbaar voor Politie voor zover dit betrekking heeft op Politie.
- 7.4 Indien zich na de melding aan Politie, als bedoeld in artikel 7.1, eventuele nieuwe, relevante ontwikkelingen voordoen, dan stelt 5.1.2.i Politie daarvan onverwijld op de hoogte.
- 7.5 5.1.2.i zal alle redelijkerwijs te nemen maatregelen treffen die nodig zijn om nadelige gevolgen te beperken of te voorkomen. Deze maatregelen worden in beginsel pas getroffen na overleg met Politie, tenzij door de aard van het Datalek dergelijk overleg niet kan worden afgewacht, in welk geval 5.1.2.i Politie onverwijld op de hoogte stelt van de getroffen maatregelen.
- 7.6 5.1.2.i verleent bijstand aan Politie bij het verrichten van meldingen aan toezichthoudende autoriteit(en) en betrokkenen in verband met een Datalek waarbij 5.1.2.i betrokken is.
- 7.7 Indien Persoonsgegevens door een Datalek beschadigd of anderszins onbruikbaar zijn geworden, dan zal de 5.1.2.i zich inspannen om die onverwijld en kosteloos te herstellen op basis van de gehanteerde backup en/of disaster recovery-procedures.

8. Aansprakelijkheid

- 8.1 5.1.2.i is jegens Politie als gevolg van of verband houdende met deze Verwerkersovereenkomst of uit enige andere hoofde aansprakelijk voor zover en tot zover partijen dit zijn overeengekomen in de Hoofdovereenkomst. De in de Hoofdovereenkomst overeengekomen beperking van de aansprakelijkheid is onverminderd van kracht op de verplichtingen zoals opgenomen in deze Verwerkersovereenkomst, met dien verstande dat eenzelfde gebeurtenis nooit tot meerdere schadevorderingen kan leiden.
- 8.2 Onverminderd artikel 8.1 kan 5.1.2.i geen beroep doen op de aansprakelijkheidsbeperking en

uitsluiting van aansprakelijkheid opgenomen in de Hoofdovereenkomst in geval van schade waarvoor 5.1.2.i conform artikel 82 AVG aansprakelijk is. 5.1.2.i vrijwaart Politie ter zake van alle kosten, schade, aanspraken, claims en handhaving jegens Politie voor zover er sprake is van een tekortkoming die of handelen dat toerekenbaar is aan 5.1.2.i. In geval van aanspraken of claims van derden zal Politie onverwijld melding doen aan 5.1.2.i de verdediging, schikkingsonderhandelingen en de processtrategie laten bepalen door 5.1.2.i en in dat kader alle redelijke instructies van 5.1.2.i opvolgen, waaronder – zo nodig – het verstrekken van een procesvolmacht. In het geval van handhaving jegens Politie zal Politie 5.1.2.i hierover zo spoedig mogelijk informeren en 5.1.2.i de gelegenheid stellen haar visie te geven.

9. Overmacht

- 9.1 Indien 5.1.2.i als gevolg van overmacht haar verplichtingen uit hoofde van deze Verwerkersovereenkomst geheel of gedeeltelijk niet kan of kon nakomen, dient 5.1.2.i Politie hiervan onverwijld melding te doen.

10. Looptijd

- 10.1 Deze Verwerkersovereenkomst treedt in werking op de datum van ondertekening door beide Partijen en loopt qua duur gelijk aan de Hoofdovereenkomst.

11. Aanvullingen en wijzigen van deze Verwerkersovereenkomst

- 11.1 Aanvullingen van en wijzigingen in deze Verwerkersovereenkomst en de daarbij behorende bijlagen zijn slechts geldig indien deze schriftelijk zijn opgemaakt en door beide partijen zijn ondertekend. Dit houdt - ter verduidelijking - tevens in dat handgeschreven wijzigingen op deze Verwerkersovereenkomst niet akkoord zijn, tenzij door beide partijen geparafeerd.

12. Overdraagbaarheid

- 12.1 Partijen zijn niet gerechtigd zonder voorafgaande schriftelijke toestemming van de andere Partij de rechten en/of plichten voortvloeiende uit deze Verwerkersovereenkomst aan een derde over te dragen.

13. Teruggave / Vernietiging Persoonsgegevens

- 13.1 Na afloop of tussentijdse beëindiging van de Verwerkersovereenkomst zal 5.1.2.i alle Persoonsgegevens zo spoedig mogelijk, in ieder geval binnen vier (4) weken, terug overdragen aan Politie en/of op verzoek van Politie alle achterblijvende Persoonsgegevens vernietigen, wissen of verwijderen, inclusief alle (kopieën van) elektronisch vastgelegde Persoonsgegevens uit/van alle documenten, computerdisks en andere gegevensdragers waarop of waarin deze Persoonsgegevens zich bevinden, met inbegrip van alle (archief)kopieën daarvan met uitzondering van de centrale off-site back-up tape. 5.1.2.i zal schriftelijk bevestigen aan Politie dat alle Persoonsgegevens terug aan haar zijn overgedragen dan wel zijn vernietigd of verwijderd. De centrale off-site back-up tape is een secundaire back-up die door 5.1.2.i alleen in geval van ernstige calamiteiten wordt gebruikt. De data op deze back-up is met behulp van hardware versleuteling offline en fysiek opgeslagen in een beveiligde omgeving en kan alleen door 5.1.2.i met behulp van unieke hardware gebruikt worden. Na afloop of tussentijdse beëindiging van de Verwerkersovereenkomst worden de Persoonsgegevens overeenkomstig best practice procedureel uitgesloten van gebruik door ze te kenmerken als 'niet meer beschikbaar voor restoredoeleinden'.
- 13.2 Indien op 5.1.2.i de wettelijke plicht rust om te blijven Verwerken, dan zal zij aan het verzoek van Politie voldoen voor zover zulks is toegestaan op grond van toepasselijke wet- en regelgeving. Zodra naleving van de verplichting uit artikel 13.1 niet langer wordt verhinderd

door de betreffende regelgeving, zal 5.1.2.i alsnog overgaan tot over hetgeen dat daar is bepaald.

14. Slotbepalingen

- 14.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Geschillen zullen ter beslechting worden voorgelegd aan de bevoegde rechter 5.1.2.i.
- 14.2 De nietigheid van enige bepaling van deze Verwerkersovereenkomst tast de geldigheid van de overige bepalingen niet aan.
-
- 14.3 Voorwaarden van deze Verwerkersovereenkomst die naar hun aard bedoeld zijn om voort te duren, blijven van kracht na beëindiging ervan.
- 14.4 In geval van strijdigheid tussen bepalingen van de Verwerkersovereenkomst en de Hoofdovereenkomst, prevaleert de bepaling van de Verwerkersovereenkomst, tenzij expliciet anders overeengekomen.
- 14.5 In geval van strijdigheid tussen bepalingen van de Verwerkersovereenkomst en de Bijlagen bij deze Verwerkersovereenkomst, prevaleert de bepaling van de Verwerkersovereenkomst, tenzij expliciet anders overeengekomen.
- 14.6 In geval 5.1.2.i een informatie- of notificatieplicht heeft jegens Politie op basis van deze Verwerkersovereenkomst zal de communicatie schriftelijk plaatsvinden tussen Raet en de desbetreffende accountmanager van Politie.
- 14.7 Een verandering van een bijlage bij deze overeenkomst is alleen mogelijk met wederzijdse schriftelijke instemming van partijen. Partijen zijn gezamenlijk verantwoordelijk voor het actueel houden van de bijlagen bij deze Verwerkersovereenkomst. Partijen zullen dit binnen de bestaande governance op de agenda zetten van het maandelijks Service Lijn Overleg ("SLO") dat wordt gehouden met de accountteams van beide Partijen.

[TEKENPAGINA VOLGT]

ALDUS OVEREENGEKOMEN EN GETEKEND:

De korpschef van Politie

5.1.2.i

5.1.2.e

5.1.2.e

Functie: Directeur Politiedienstencentrum (wnd.)
Datum:

5.1.2.e

Datum: 23-04-2020

Bijlagen:

1. Overzicht van Verwerkingen
2. Goedgekeurde Subverwerkers
3. Beveiligingsmaatregelen en toegang

Bijlage 1 – Overzicht van Verwerkingen

1.1 Beaufort (HR Core)

1.1.1 Overzicht Verwerking

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	- NP medewerkers - Externe medewerkers - Ketenpartners	Persoons- en arbeidsrelatie.	- Onderhouden statussen - Onderhoudt historie
(2)	Idem	Personeelsgegevens, adresgegevens en BSN.	- Identificatie - Rapportages - Uitvoeren CAO - Correspondentie - Calamiteiten
(3)	Idem	Aanstelling / dienstverband	- Aanstellings- en contractgegevens
(4)	NP medewerkers	Verzuim	- Uitvoering regelgeving
(5)	Idem	Werktijd	- Management informatie - Planning
(6)	Idem	Salarisgegevens	- Uitvoering salarisberekening en -afrekening - Uitbetaling salaris per CAO-soort en functiegroep - Loonbeslagen
(7)	Idem	Bankrelaties	- Overmaking betalingen naar medewerker d.m.v. opgegeven betalingswijze
(8)	Idem	Externe overschrijvingen	- betaalbaar stellen/overschrijven naar derde organisaties
(9)	Idem	Loonheffing	- randvoorwaarden uitvoering fiscale regelgeving
(10)	Idem	Sociale verzekeringen	- Registratie van SV-gegevens t.b.v. uitvoering - Bruto/netto salarisverwerking.

Algemeen doeleinde van de verwerkingen: uitvoeren van de personeels- en salarisadministratie.

1.1.2 Locaties

In het kader van HR Core worden de Persoonsgegevens op de volgende locaties Verwerkt:

- (1) Politielocatie: 5.1.2.1 levert de software die door de politie lokaal wordt geïnstalleerd en gebruikt.

1.2 Gemal (payroll)

1.2.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: uitvoeren van de Salarisadministratie.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	NP medewerkers	Salarisgegevens	- Uitvoering salarisberekening en -afrekening - Uitbetalen salaris per CAO-soort en functie - Loonbeslagen - Verzorgen van afdrachten - Genereren van loonstroken en jaaropgaven

1.2.2 Locaties

In het kader van Gemal (payroll) worden de Persoonsgegevens op de volgende locaties Verwerkt:

5.1.2.h

1.3 YouForce Opleidingsmanagement

1.3.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: voor de persoonlijke ontwikkeling van medewerkers en tevens management informatie voor leidinggevende.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	(Interne) medewerkers NP	- Personeelsnummer - Eenheidscode - OE code en afdelingsnaam - Voor- en achternaam - Functie - E-mailadres (werk) - Arbeidsrelatie (vast dienst of tijdelijk)	Om de aanvraag te kunnen koppelen aan de persoon die het betreft. Het functieprofiel wordt gekoppeld aan het aanbod van onderwijs Om de gevolgde opleidingen per medewerker te kunnen vasthouden (wie heeft welke trainingen gevolgd (skills). En om het resultaat van de gevolgde opleiding te kunnen beschouwen.
(2)	Trainer (in dienst van NP)	- Naam of	Wie de training heeft

		inloggegevens	verzorgd/ het examen heeft afgenomen
--	--	---------------	--------------------------------------

1.3.2 Locaties

In het kader van YouForce (e-HRM) worden de Persoonsgegevens op de volgende locaties Verwerkt:

5.1.2.h

1.4 YouForce Performance Management

1.4.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: deze tool dient als digitale ondersteuning van de Resultaat- en Ontwikkelcyclus (R&O cyclus) bestaande uit resultaatgesprek, voortgangsgesprek, functioneringsgesprek (evaluatie) en ontwikkelgesprek over ontwikkelplan.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	Medewerkers NP	- Voor- en achternaam - Personeelsnummer - Datum indiensttreding - Functie - Eenheid - Afdeling - Team - Geboortedatum - Competenties - Kennis - Vaardigheden - Beoordeling (per target) - Portfolio	Ondersteuning van de Resultaat- en Ontwikkelcyclus (R&O cyclus). Deze cyclus bestaat uit regelmatige gesprekken tussen medewerker en leidinggevende of medewerker met organisatorische coördinatie.
(2)	(Plaatsvervangend) leidinggevenden	- Voor- en achternaam	Wie de afspraken met de medewerker heeft gemaakt

1.4.2 Locaties

In het kader van YouForce Performance Management worden de Persoonsgegevens op de volgende locaties Verwerkt:

5.1.2.h

1.5 YouForce Performance Selfservice

1.5.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: deze tool dient als digitale ondersteuning (workflow) voor de processen t.b.v. de Personeels- en Salarisadministratie en sluiten aan op de bronregistratie Beaufort.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	Medewerkers NP	Proces-gestuurd gekoppeld aan alle te muteren velden in Beaufort (zie 1.1.1)	ondersteuning voor de processen voor de Personeels- en Salarisadministratie
(2)	(Plaatsvervangend) leidinggevenden	De processen waarbij de leidinggevende de initiator is of degene die akkoord moet geven	Initiëren of accorderen van processen ter voorbereiding op de definitieve verwerking (in Beaufort)
(3)	HR Administratie	Laatste (controle) stap binnen de ingerichte processen (zie hiervoor)	Controle op juistheid en volledigheid

1.5.2 Locaties

In het kader van YouForce Selfservice worden de Persoonsgegevens op de volgende locaties Verwerkt:

5.1.2.h

1.6 YouForce Werving en Selectie

1.6.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: deze tool dient als digitale ondersteuning voor het werving en selectieproces van nieuwe medewerkers.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	Solicitant	Voornaam Achternaam Geslacht Geboortedatum Emailadres Telefoon Mobiele telefoon Adres Postcode Woonplaats Kandidaat-id Persoonsgegevens in CV (document)	Het selecteren van de beste kandidaten voor de opengestelde functies in lijn met de aanstellingseisen en de competentieprofielen behorend bij het LFNP
(2)	Medewerker	Voornaam Achternaam E mailadres Mobiele telefoonnummer Initialen	Het selecteren van de beste kandidaten voor de opengestelde

		SSO-ID You Force	functies in lijn met de aanstellingseisen en de competentieprofielen behorend bij het LFNP
--	--	------------------	--

1.6.2 Locaties

In het kader van YouForce Werving en Selectie (Easycruit) worden de Persoonsgegevens op de volgende locaties Verwerkt:

(1) Datacentrum 5.1.2.i

1.7 YouForce Personeel- en Salarisdossier Online (PDOL en SDOL)

1.7.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: deze tool verzorgt de digitale opslag van de gedurende het Youforce processen gegenereerde documenten, historische documenten en andere relevante documenten en levert informatie rondom verjaring/vernietiging.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	Medewerkers NP en (Plaatsvervangend) leidinggevenden	- Persoonlijk - Aanstelling - Loopbaan - Opleiding en cursussen - Inzetbaarheid - Dienstongevallen - Salaris - Verlof - Einde dienstverband	Wettelijke grondslag
(2)			

1.7.2 Locaties

In het kader van YouForce PDOL en SDOL worden de Persoonsgegevens op de volgende locaties Verwerkt:

5.1.2.h

1.8 YouForce User Management

1.8.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: deze tool dient als digitale ondersteuning bij het autorisatiebeheer.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	Selfservice TalentSuite PDOL	- Naam - Pers. nr - OE - functie	Autorisatie aanpalende applicaties
(2)			

1.8.2 Locaties

In het kader van YouForce User Management worden de Persoonsgegevens op de volgende locaties Verwerkt:

5.1.2.h



1.9 YouForce Flex Benefit

1.9.1 Overzicht Verwerkingen

Algemeen doeleinde van de verwerkingen: deze tool dient als digitale ondersteuning voor de inzet van de flexibele arbeidsvoorwaarden.

	Betrokkenen (per categorie)	Persoonsgegevens (per categorie)	Doeleinde van Verwerking
(1)	Medewerkers NP	- Naam - Pers. nr - OE - Functie - Salaris	Keuze inzet flexibele arbeidsvoorwaarden
(2)			

1.9.2 Locaties

In het kader van YouForce User Management worden de Persoonsgegevens op de volgende locaties Verwerkt:

5.1.2.h



Bijlage 2 – Goedgekeurde Subverwerkers

In deze bijlage wordt een onderscheid gemaakt tussen de Subverwerkers voor diensten met een algemene toestemming en de Subverwerkers waarvoor ^{5.1.2.i} een specifieke toestemming heeft gegeven.

2.1 Algemene toestemming

Politie stemt ermee in dat ^{5.1.2.i} – met in acht name van hetgeen opgemerkt in artikel 4 van deze Verwerkersovereenkomst – de volgende partijen als Subverwerker inschakelt, waarvoor Politie een algemene toestemming geeft:

5.1.2.h

Locaties van dienstverlening en datacentra buiten de EEA, waarbij er sprake is van een Verwerking van Persoonsgegevens buiten de EEA of toegang vanuit buiten de EEA:

(1) N.v.t.

2.2 Specifieke toestemming

Politie stemt ermee in dat ^{5.1.2.i} – met in acht name van hetgeen opgemerkt in artikel 4 van deze Verwerkersovereenkomst – de volgende partijen als Subverwerker inschakelt, waarvoor Politie een specifieke toestemming geeft:

(1) N.v.t.

- Soort dienstverlening: n.v.t.

Locaties van dienstverlening en datacentra buiten de EEA, waarbij er sprake is van een Verwerking van Persoonsgegevens buiten de EEA of toegang vanuit buiten de EEA:

(1) N.v.t.

Bijlage 3 – Beveiligingsmaatregelen en toegang

In het kader van de dienstverlening van 5.1.2.i aan Politie treft 5.1.2.i passende technische en organisatorische maatregelen ter beveiliging van de Persoonsgegevens zoals nader gespecificeerd in deze bijlage. Raet draagt zorg voor het actualiseren van haar beveiligingsmaatregelen bij mogelijke veranderingen in de toekomst.

3.1 Beveiligingsmaatregelen

Met betrekking tot de Verwerkingen die plaatsvinden in het kader van de dienstverlening worden ten tijde van het sluiten van de Verwerkersovereenkomst de volgende beveiligingsmaatregelen getroffen door 5.1.2.i:

- 5.1.2.i
- 1
-
-

3.2 Doorgifte buiten de EEA

Niet van toepassing: er is geen sprake van doorgifte van Persoonsgegevens door 5.1.2.i naar een land buiten de EEA of naar een internationale organisatie in het kader van de dienstverlening aan Politie.

Bijlage 3 – Annex 1: 5.1.2.1 in control statement

Bijlage 3 – Annex 2: Statement of Applicability ISO27001



Digitaal toets-systeem

**Verwerkers-
Overeenkomst
Digitaal toets-
systeem**

Uitgegeven door: Politie, Politiedienstencentrum - Dienst Verwerving

Informatie: Inkoopmanagement

Definitief

Versie 1.0

Versie datum 7 mei 2020

2019© Politie, alle rechten voorbehouden

Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

Inhoudsopgave

1.	Begrippen	5
2.	Totstandkoming, duur en einde van de Verwerkersovereenkomst	5
3.	Voorwerp van de Verwerkersovereenkomst	5
4.	Van toepassing zijnde Voorwaarden	6
5.	Teruggave Persoonsgegevens en/of Politiegegevens	6
6.	Beveiliging	7
7.	Meldplicht Datalekken en beveiligingsinbreuken	7
8.	Geheimhouding, beschikbaarheid en integriteit	7
9.	Controle	8
10.	Informereren van betrokkenen	8
11.	Vrijwaring	9
12.	Maatregelen toezichthouder	9
13.	Wijziging	9
14.	Slotbepalingen	9

Verwerkersovereenkomst

inzake de Overeenkomst voor het leveren van een digitaal toetsysteem

De ondergetekenden:

1. De Politie, gevestigd te Den Haag, te dezen rechtsgeldig vertegenwoordigd door de korpschef van politie, namens deze, de directeur PDC, namens deze, J. W.C.H. Jansen, wnd directeur Dienst ICT: "de Politie",

en

2. ^{5.1.2.i} ^{5.1.2.e} te dezen rechtsgeldig vertegenwoordigd door ^{5.1.2.e} hierna te noemen: 'Opdrachtnemer',

hierna gezamenlijk te noemen: "Partijen";

OVERWEGENDE DAT:

- Partijen de Overeenkomst inzake het leveren van een digitaal toetsysteem met kenmerk ^{5.1.2.i} (hierna te noemen: de Overeenkomst) hebben gesloten;
- in het kader van de uitvoering daarvan Persoonsgegevens in de zin van artikel 4 sub 1 van de Algemene Verordening Gegevensbescherming EU 2016/679 (hierna te noemen: AVG) worden verwerkt en/of Politiegegevens in de zin van artikel 1 onder a van de Wet Politiegegevens (Wpg);
- Opdrachtnemer die in het kader van de uitvoering van de Overeenkomst met de Politie Persoonsgegevens en/of Politiegegevens verwerkt is aan te merken als Verwerker in de zin van de AVG en/of Wpg;
- De Politie als Opdrachtgever Verantwoordelijke is voor de Persoonsgegevens en Politiegegevens;
- Partijen middels deze Verwerkersovereenkomst nadere afspraken over het verwerken van de Persoonsgegevens en/of Politiegegevens door Opdrachtnemer als Verwerker en de geldende wettelijke verplichtingen uit de AVG en/of Wpg waaronder meldplicht Datalek wensen vast te leggen.

KOMEN OVEREEN:

1. Begrippen

Aanvullend op de AVG en Wpg geldt dat de hierna en hiervoor in deze Verwerkersovereenkomst vermelde, met een hoofdletter geschreven begrippen, de volgende betekenis hebben:

1. AP: Autoriteit Persoonsgegevens (<https://autoriteitpersoonsgegevens.nl>)
2. AVG: Algemene Verordening Gegevensbescherming EU 2016/679.
3. Datalek: een inbreuk op de beveiliging, in de zin van artikel 33 en 34 AVG, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van Persoonsgegevens en/of Politiegegevens waaronder een inbreuk op vertrouwelijkheid, verlies, wijziging van gegevens.
4. Hulpleverancier: een partij of derde die door Opdrachtnemer is ingeschakeld om te ondersteunen bij het uitvoeren van de Overeenkomst. Indien de Hulpleverancier in opdracht van Opdrachtnemer Persoonsgegevens en/of Politiegegevens verwerkt, is Hulpleverancier tevens aan te merken als sub-opdrachtnemer.
5. Overeenkomst: de overeenkomst inzake digitaal toetssysteem met kenmerk ^{5.1.2.1} [REDACTED] waarin de Politie onder haar verantwoordelijkheid vallende Persoonsgegevens en/of Politiegegevens door Opdrachtnemer wil laten bewerken.
6. Partij: De Politie of Opdrachtnemer, afhankelijk van de context.
7. Verwerkersovereenkomst: deze overeenkomst c.a..
8. Wpg: Wet Politiegegevens.

2. Totstandkoming, duur en einde van de Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst treedt in werking na ondertekening door beide Partijen en niet eerder dan op de datum waarop de Overeenkomst in werking treedt.
- 2.2 Deze Verwerkersovereenkomst zal van kracht zijn gedurende de looptijd van de Overeenkomst. Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst van rechtswege.
- 2.3 Geen van beide Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

3. Voorwerp van de Verwerkersovereenkomst

- 3.1 Opdrachtnemer verwerkt in opdracht van de Politie uitsluitend de in de Nadere Overeenkomst beschreven categorieën Persoonsgegevens en/of Politiegegevens van de Politie voor het daarin genoemde doel.
- 3.2 Opdrachtnemer zal de Persoonsgegevens en/of Politiegegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de AVG, Wpg en andere toepasselijke regelgeving betreffende de Verwerking van Persoonsgegevens verwerken.
- 3.3 Opdrachtnemer Verwerkt Persoonsgegevens en/of Politiegegevens slechts in opdracht van de Politie voor zover noodzakelijk om de diensten zoals omschreven in de Overeenkomst aan de Politie te verlenen en volgt alle instructies van de Politie dienaangaande op, behoudens afwijkende wettelijke verplichtingen. Het product of de dienst van Opdrachtnemer is niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.
- 3.4 Opdrachtnemer heeft geen zeggenschap over het doel en de middelen voor de Verwerking van Persoonsgegevens en/of Politiegegevens. Voor zover niet anders is bepaald in deze Verwerkersovereenkomst, neemt Opdrachtnemer geen beslissingen over het gebruik van de Persoonsgegevens en/of Politiegegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens en/of Politiegegevens. De zeggenschap over de

Persoonsgegevens en/of Politiegegevens verstrekt onder deze Verwerkersovereenkomst komt nimmer bij Opdrachtnemer te berusten.

- 3.5. Voor de werking van dit artikel wordt verwezen naar antwoord 9 in de tweede nota van inlichtingen.
- 3.6. Het is Opdrachtnemer uitdrukkelijk niet toegestaan Persoonsgegevens en/of Politiegegevens aan anderen dan de Politie te verstrekken, tenzij op schriftelijk verzoek van de Politie, of met diens schriftelijke toestemming. Opdrachtnemer is na verleende toestemming verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden, waarbij hij binnen 30 dagen exact de verstrekte Persoonsgegevens en/of Politiegegevens, de Betrokkene(n), de ontvanger(s) en het moment van verstrekking gedocumenteerd aan de Politie dient te beschrijven.
- 3.7. Indien Opdrachtnemer op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert Opdrachtnemer de grondslag van het verzoek en de identiteit van de verzoeker en informeert hij onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, de Politie ter zake.
- 3.8. Opdrachtnemer verleent de Politie volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG en/of Wpg, meer in het bijzonder de rechten van Betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens en/of Politiegegevens en het uitvoeren van een gehonoreerd aangetekend verzet, als de Politie niet zelf kan voldoen aan deze verplichtingen.
- 3.9. Indien Opdrachtnemer onrechtmatige Verwerkingen of inbreuken op de in artikel 8.1 van deze Verwerkersovereenkomst genoemde beveiligingsmaatregelen signaleert, zal hij de Politie hierover onmiddellijk inlichten en alle redelijkerwijs benodigde maatregelen treffen om deze en verdere onrechtmatige Verwerkingen of inbreuken te beëindigen, te voorkomen of te beperken en een en ander onverminderd de verplichting van Opdrachtnemer om de eventueel door de Politie daardoor geleden schade te vergoeden.
- 3.10. De eventuele met de in de artikelen 3.8, artikel 3.9 en artikel 9 van deze Verwerkersovereenkomst gemoeide kosten komen voor rekening van degene die die kosten maakt.
- 3.11. De Politie en Opdrachtnemer zorgen ervoor dat de Functionaris voor de gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van Persoonsgegevens en/of Politiegegevens.
- 3.12. Opdrachtnemer documenteert alle inbreuken die in artikel 33 lid 5 AVG zijn beschreven.
- 3.13. Opdrachtnemer verleent alle benodigde medewerking in het kader van een gegevensbeschermings-effectbeoordeling in het kader van artikel 35 AVG, als de Politie de betreffende werkzaamheden niet zelf kan uitvoeren. Voor het verlenen van deze medewerking is de Politie geen (aanvullende) vergoeding aan Opdrachtnemer verschuldigd.

4. Van toepassing zijnde Voorwaarden

Op deze Verwerkersovereenkomst zijn de bepalingen van de Overeenkomst van toepassing voor zover daarvan in deze Verwerkersovereenkomst niet wordt afgeweken.

5. Teruggave Persoonsgegevens en/of Politiegegevens

- 5.1. Na afloop van de Overeenkomst en de Verwerkersovereenkomst dienen alle Persoonsgegevens en/of Politiegegevens, kopieën en bewerkingen daarvan, alsmede alle gegevensdragers waarop de Persoonsgegevens en/of Politiegegevens, kopieën of bewerkingen daarvan zijn of zullen worden vastgelegd, onmiddellijk op eerste verzoek van Politie te worden geretourneerd c.q. verstrekt aan de Politie (of een door de Politie aan te

wijzen derde), dan wel te worden vernietigd, een en ander naar de keuze van de Politie. De Politie kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Op het moment dat deze Verwerkersovereenkomst eindigt, zal Opdrachtnemer bovendien al zijn medewerking verlenen ter zake van de overdracht van de werkzaamheden inzake de Verwerking van de Persoonsgegevens en/of Politiegegevens aan de Politie of een opvolgende opdrachtnemer en wel op een zodanige wijze dat vanaf het moment dat de overdracht plaatsvindt de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Opdrachtnemer wordt belemmerd.

- 5.2 De kosten gemoeid met de inspanningen van Opdrachtnemer als genoemd in 5.1, komen voor rekening van de Politie voor zover deze kosten niet inbegrepen zijn in de overeengekomen prijzen en vergoedingen van Opdrachtnemer voortvloeiende uit de uitvoering van de Overeenkomst.
- 5.3 Opdrachtnemer zal te allen tijde de beschreven data-portabiliteit waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

6. Beveiliging

- 6.1 Opdrachtnemer rapporteert periodiek met een frequentie van 1 maal per jaar, de eerste keer uiterlijk 30 juni 2020 aan de Politie over de door Opdrachtnemer genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.
- 6.2 De met de rapportage gemoeide kosten zijn voor rekening van Opdrachtnemer.
- 6.3 Opdrachtnemer Verwerkt geen Persoonsgegevens en/of Politiegegevens buiten een lidstaat van de Europese Unie.

7. Meldplicht Datalekken en beveiligingsinbreuken

- 7.1 In het geval van een vermoedelijk(e) of daadwerkelijk(e) (i) Datalek; (ii) schending van de beveiligingsmaatregelen; (iii) schending van de geheimhoudingsplicht of (iv) verlies van vertrouwelijke gegevens zal Opdrachtnemer de Politie direct, doch uiterlijk binnen 24 uur na de eerste ontdekking van het incident, informeren. De Opdrachtnemer zal alle redelijkerwijs benodigde maatregelen treffen om (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige verwerking te voorkomen of te beperken en een schending van beveiligingsmaatregelen, schending van de geheimhoudingsplicht of verder verlies van vertrouwelijke gegevens te beëindigen en in de toekomst te voorkomen, onverminderd enig recht van de Politie op schadevergoeding of andere maatregelen voor zover het incident toerekenbaar is aan Opdrachtnemer of de door haar in te zetten Hulpverlancier. Deze bepaling is van toepassing op incidenten bij de Opdrachtnemer en haar eventuele Hulpverleners.
- 7.2 Opdrachtnemer zal op verzoek van de Politie meewerken aan het informeren van de bevoegde autoriteiten en betrokkene(n).

8. Geheimhouding, beschikbaarheid en integriteit

- 8.1 Indien en voor zover de Politie daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer ten aanzien van de daarbij aangeduide Persoonsgegevens en/of Politiegegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken Persoonsgegevens

en/of Politiegegevens of informatie zodra de noodzaak voor Opdrachtnemer om daarvan nog langer kennis te nemen, is komen te vervallen.

- 8.2 Na afloop van de Overeenkomst en deze Verwerkersovereenkomst blijft dit artikel en de hierin besproken geheimhouding van kracht.

9. Controle

- 9.1 De Politie controleert op elk door haar gewenst moment dan wel laat op elk door haar gewenst moment de verwerkingen en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer dan wel die van door Opdrachtnemer ingeschakelde Hulpleveranciers controleren, als na het bestuderen van de beschikbare certificeringen en rapportages van reeds uitgevoerde controles gereede twijfel blijft bestaan over de verwerkingen en/of de naleving.
- 9.2 De rapportage in het kader van de jaarlijkse audit voor ISO 27001 bij Opdrachtnemer geldt als verklaring door een onafhankelijke externe deskundige voor de genoemde naleving. De Politie mag het certificaat opvragen en op verzoek de auditrapportage inzien. Opdrachtnemer stelt de Politie binnen 14 werkdagen op de hoogte als het certificaat verloopt of wordt ingetrokken.
- 9.3 Opdrachtnemer zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen dat ook de door hem ingeschakelde Hulpleveranciers hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.
- 9.4 Het uitvoeren van een controle zal niet tot een vertraging van de door Opdrachtnemer in het kader van de Overeenkomst en deze Verwerkersovereenkomst te verrichten werkzaamheden mogen leiden. Indien dat onverhoopt toch het geval is, zullen Partijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.
- 9.5 De met de controle gemoeide kosten zijn voor rekening van de Politie tenzij uit de controle blijkt dat Opdrachtnemer is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Verwerkersovereenkomst en/of de Overeenkomst.
- 9.6 Opdrachtnemer en Politie zullen in overleg treden over een realistische termijn. Als er sprake is van een niet-toerekenbare tekortkoming, dan zullen zij (...) in gesprek gaan over de kosten. Dit geldt niet in geval er sprake is van een toerekenbare tekortkoming (wanprestatie). Deze kosten zullen voor rekening en risico komen van Opdrachtnemer.

10. Informeren van betrokkenen

- 10.1 Opdrachtnemer zal haar volledige medewerking verlenen opdat de Politie kan voldoen aan zijn wettelijke verplichtingen in het geval dat een Betrokkene zijn rechten uitoefent op grond van de AVG, Wpg of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens en/of Politiegegevens, als de Politie(academie) niet zelf kan voldoen aan deze verplichtingen.
- 10.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten onder de AVG en/of Wpg direct contact opneemt met Opdrachtnemer, dan neemt Opdrachtnemer het verzoek van Betrokkene niet in behandeling en verwijst Opdrachtnemer Betrokkene door naar de Politie.
- 10.3 Als Opdrachtnemer zijn diensten in het kader van de Overeenkomst rechtstreeks aanbiedt aan eindgebruikers van wie Persoonsgegevens en/of Politiegegevens worden verwerkt, dan is Opdrachtnemer verplicht om op een makkelijk toegankelijke en permanent beschikbare manier de Politie te informeren over het volgende:

- a. de naam en het adres van de Opdrachtnemer;

- b. de doeleinden waarvoor Opdrachtnemer de Persoonsgegevens en/of Politiegegevens verwerkt;
- c. de categorieën Persoonsgegevens en/of Politiegegevens die de Opdrachtnemer verwerkt;
- d. de derden aan wie de Persoonsgegevens en/of Politiegegevens toegankelijk worden gemaakt;
- e. de landen waarnaar de Persoonsgegevens en/of Politiegegevens worden overgedragen;
- f. het recht op inzage, correctie en verwijdering van de Persoonsgegevens en/of Politiegegevens.

De Opdrachtnemer zal de Politie laten weten waar deze informatie gepubliceerd is.

11. Vrijwaring

- 11.1 Opdrachtnemer vrijwaart de Politie voor directe aanspraken van derden, daaronder begrepen Betrokkenen, die jegens de Politie mochten worden ingesteld wegens een aan Opdrachtnemer of door haar ingeschakelde Hulpleverancier, toe te rekenen schending van de AVG of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens en/of Politiegegevens tot een maximum van 2 miljoen euro per jaar en maximaal 1 miljoen euro per aanspraak.

12. Maatregelen toezichthouder

Indien de AP in het kader van haar taak als handhaver een maatregel of boete oplegt aan de Politie en indien de oorzaak voor het opleggen van de maatregel of boete te wijten is aan het niet nakomen van de in de Verwerkersovereenkomst gemaakte afspraken door Opdrachtnemer of diens Hulpleverancier, dan kan de Politie alle kosten voor deze maatregel of boete verhalen op de Opdrachtnemer. Tevens heeft de Politie het recht om de Overeenkomst in bovengenoemde situatie met onmiddellijke ingang te ontbinden zonder dat de Opdrachtnemer aanspraak kan maken op enige vorm van schadevergoeding.

13. Wijziging

- 13.1 Indien een functionele wijziging in de te verwerken Persoonsgegevens en/of Politiegegevens of een controle daartoe aanleiding geeft treden Partijen op eerste verzoek van de Politie in overleg over het aanpassen van de gemaakte afspraken binnen deze Verwerkersovereenkomst.
- 13.2 De nieuw te maken afspraken dienen voorafgaand aan de toepassing daarvan schriftelijk te zijn vastgelegd en deel uit te maken van deze Verwerkersovereenkomst.
- 13.3 De wijzigingen kunnen nooit tot gevolg hebben dat de Politie niet kan voldoen aan de AVG, Wpg en overige relevante wet- en regelgeving met betrekking tot Persoonsgegevens en/of Politiegegevens.

14. Slotbepalingen

- 14.1 Afwijkingen van deze Verwerkersovereenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.

- 14.2 Algemene leveringsvoorwaarden dan wel andere algemene of bijzondere voorwaarden van Opdrachtnemer en diens Hulpleverancier zijn niet van toepassing op deze Verwerkersovereenkomst en worden door de Politie uitdrukkelijk van de hand gewezen.
- 14.3 Deze Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst. Bij strijdigheid tussen bepalingen uit deze Verwerkersovereenkomst en de Overeenkomst prevaleren de bepalingen uit deze Verwerkersovereenkomst.
- 14.4 Op deze Verwerkersovereenkomst is het Nederlands recht van toepassing.

Aldus overeengekomen en ondertekend,

de *Opdrachtgever*
De Politie,

Namens deze,

Directeur PDC

Namens deze,

5.1.2.e



de *Opdrachtnemer*

5.1.2.e



5.1.2.e





DATA PROCESSING AGREEMENT

Customer/ Controller: De Polite academie

Contact person (Reseller): 5.1.2.e, 5.1.2.i

Processor: 5.1.2.i

This Data Processing Agreement ("DPA") forms part of 5.1.2.i provision to Customer of access to software and related services (jointly referred to as the "Services"), as further specified in the applicable agreement between Customer and 5.1.2.i, and all documents and exhibits incorporated therein (jointly referred to as the "Agreement"), to reflect the parties' agreement with regard to 5.1.2.i Processing of Personal Data on behalf of Customer, in accordance with the requirements of applicable Data Protection Laws and regulations.

1. Guarantees

5.1.2.i will carry out processing on behalf of the Customer, and therefore guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

2. Definitions

"**Agreement**" means the separate agreement(s) between 5.1.2.i and the customer where the content and scope of the services provided by 5.1.2.i to Customer is agreed.

"**Controller**" means "controller", as defined in GDPR Article 4. The parties agree that Customer is Controller under this Data Processing Agreement, and that Customer therefore must adhere to obligations for Controllers following the GDPR.

"**Data Subject**" means "data subject" as defined in GDPR Article 4.

"**GDPR**" means REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"**Personal Data**" means "personal data", as defined in GDPR Article 4.

"**Processing**" means "processing" as defined in the GDPR article 4.

"**Processor**" means "processor", as defined in GDPR Article 4. The parties agree that 5.1.2.i is Processor under this Data Processing Agreement, and that 5.1.2.i therefore must adhere to obligations for Processors following the GDPR.

"**Respondent**" means a Data Subject who provides data by entering data into surveys made available to them by Customer.

"**Sensitive Personal Data**" means special categories of data as defined in GDPR Article 9.

"**Software**" means the standard online software to which Customer is granted access in the Agreement.

"**Sub-processor**" means a third party subcontractor engaged by any member of 5.1.2.i Group which Processes Personal Data on 5.1.2.i behalf.

5.1.2.i mean members of the 5.1.2.i Group that may assist in the performance of the Agreement.

5.1.2.i means, for the purpose of this data processing agreement, 5.1.2.i, 5.1.2.i, and any wholly or fully owned subsidiaries of 5.1.2.i

Other terms have the definitions provided for them in the GDPR, the Agreement or as otherwise specified below.

3. The subject-matter of the processing

Please see Appendix A

4. The duration of the processing

Please see Appendix A.

5. The nature of the processing

Please see Appendix A.

6. The purpose for the processing

Please see Appendix A.

7. Categories of Data Subjects

Please see Appendix A.

8. The types of Personal Data

Please see Appendix A.

9. Customer's Instructions

During the term of the Agreement, Customer may provide written instructions, hereunder e-mail, to 5.1.2.i in addition to those specified in the Agreement with regard to processing of Personal Data. 5.1.2.i will comply with such written instructions without additional charge, to the extent necessary for 5.1.2.i to comply with laws applicable to 5.1.2.i as a Processor in the performance of the Agreement.

Any other instructions or change in the Agreement may be subject to separate agreement and additional fees.

5.1.2.i is not obligated to perform legal research and/or to provide legal advice to Customer.

10. Controller

The control of Personal Data remains solely with Customer, and Customer will at all times remain the Controller for the purposes of Personal Data processed under the Agreement, and this Data Processing Agreement. Customer is responsible for compliance with its obligations as Controller under the GDPR and other applicable data protection laws, hereunder for justification of any transmission of Personal Data to 5.1.2.i (including providing any required notices and obtaining any required consents), and for its decisions concerning the Processing and use of the data.

In particular, Customer will:

- a) Ensure that the information in Appendix A is correct and complete, and updated if Customer regards necessary.
- b) Provide the information to Data Subject that is required under GDPR
- c) Ensure that it has and maintains a lawful basis, as defined in the GDPR, for processing of all Personal Data it performs during the term of this DPA towards Data Subject.
- d) Inform 5.1.2.i without undue delay in the event i) the legal basis for Customer's data processing in accordance with the GDPR ceases to exist (e.g. withdrawal of consent by Data Subject), and ii) Customer obtains information that create suspicion of unauthorized access to or handling of Personal Data. Customer shall provide all relevant information. Section 18 of this DPA applies accordingly.

11. Processor

5.1.2.i is the Processor for Personal Data processed on Controller's behalf under the Agreement and this Data Processing Agreement. 5.1.2.i is responsible for compliance with its obligations as Processor under the GDPR and other applicable data protection laws, hereunder to process data according to written instructions from Customer.

In particular, 5.1.2.i will:

- a) process the Personal Data only on documented written instructions from the Customer,
- b) not transfer the Personal Data to a third country or an international organisation that does not ensure an adequate level of protection in accordance with GDPR Article 45, or within the safeguards defined in GDPR Article 46,
- c) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality

ensure where a (sub-)processor is engaged, the same data protection obligations as set out in this Data Processing Agreement shall be imposed on that other processor by way of a contract

- d) take into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights laid down in GDPR Chapter III
- e) assist the Customer in ensuring compliance with the obligations pursuant to GDPR Articles 32 to 36 taking into account the nature of processing and the information available to the processor
- f) make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in GDPR Article 28 and allow for audits by the Customer.
- g) immediately inform the Customer if, in 5.1.2.i opinion, an instruction infringes the GDPR.

5.1.2.i shall assist the Customer in ensuring compliance with applicable law, including assisting the Customer with: Customer Complying with duty of notification to supervisory authorities and data subjects in case of a personal data breach;

Conduct data privacy impact assessments;

Conduct prior consultations with supervisory authorities when a privacy impact assessment makes it necessary;

Notice to the Controller if the Processor is of the opinion that an instruction from the Controller is non-compliant with applicable data protection regulations.

Assistance as set out above, shall be carried out to the extent necessary, taking into account the Controller's need, the nature of the processing and the information available to the Processor.

12. Right to edit or delete Personal Data

5.1.2.i will at all times grant Customer, as agreed in the Agreement, electronic access to online software environment that holds Customer's Personal Data, allowing Customer to delete, release, correct or block access to specific Personal Data, as Customer requires at all times. Customer may, to the extent permitted by applicable law, provide detailed written instructions to 5.1.2.i to delete, release, correct or block access to Respondent Personal Data. If Customer requires 5.1.2.i to perform such deletion, release, correction or blocking of access to data that Customer could itself have performed, Customer agrees to pay 5.1.2.i then-current fees associated with such performance.

13. Data Transfer within EEA

With respect to Personal Data stored by the 5.1.2.i Group in data centres in the European Economic Area (EEA), 5.1.2.i shall ensure compliance by members of the 5.1.2.i Group as follows: (i) for members of the 5.1.2.i Group, 5.1.2.i and other relevant entities have binding intra-company agreements requiring compliance with all applicable security and data privacy policies and standards, and (ii) for Sub processors, 5.1.2.i Group has entered into contracts with Sub processors which provide that the Sub processor will undertake data protection and confidentiality obligations consistent with 5.1.2.i security standards.

14. Data Transfer to countries outside EEA

5.1.2.i will not transfer personal data outside the EEA, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data, or (ii) not covered by a suitable safeguard recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules, Binding Corporate Rules for Processors and EU Standard Model Clauses.

If Customer, or a party on Customer's behalf, will access Personal Data stored in 5.1.2.i storage area in the EEA, or transfer Personal Data stored in 5.1.2.i storage area in the EEA from, the EEA storage area, it is Customer's responsibility to ensure that either the transfer of data takes place based on a adequacy decision by the European Commission as defined in GDPR Article 45, or appropriate safeguards defined in GDPR Article 46 are in place for such access or transfer.

15. Affiliates and Sub-processors

Some or all of 5.1.2.i obligations under the Agreement may be performed by 5.1.2.i Affiliates.

5.1.2.i may also engage third party Sub-processors to assist in the provision of software access in the Agreement. 5.1.2.i will provide a list of Sub-processors that may Process the Personal Data to Customer upon request.

5.1.2.i shall remain responsible at all times for compliance with the terms of the Agreement and this Data Processing Agreement by 5.1.2.i Affiliates and Sub-processors.

Customer consents to 5.1.2.i use of 5.1.2.i Affiliates and Sub-processors in the performance of the

Agreement in accordance with this Data Processing Agreement.

If 5.1.2.i plans to change sub-contractors or plans to use a new sub-contractor, 5.1.2.i shall notify the Customer in writing 4 months prior to any Processing by the new sub-contractor, and the Controller is entitled to object to the change of sub-contractors within 1 month upon the receipt of such notice. Should the Controller object to the change, Controller may terminate the Agreement in writing upon 3 months' notice. To the extent Controller does not terminate the Agreement, the change of sub-processor is rendered as accepted.

16. Technical and Organizational Measures

When Processing Personal Data on behalf of Customer in connection with fulfilment of the Agreement, 5.1.2.i shall ensure that it implements and maintains compliance with appropriate technical and organizational security measures for the Processing of such data. Accordingly, 5.1.2.i will implement the technical and organizational measures, hereunder 5.1.2.i Technical and Organizational Measures and 5.1.2.i IT governance policy.

17. Audit Rights

Customer may audit 5.1.2.i compliance with the terms of the Agreement and this Data Processing Agreement up to once per calendar year, or to the extent required by applicable law. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and 5.1.2.i. Any person conducting the audit on behalf of Customer, either its employees or a third party, must execute a written confidentiality agreement acceptable to 5.1.2.i before conducting the audit.

To request an audit, Customer must submit a detailed audit plan at least two weeks in advance of the proposed audit date to 5.1.2.i describing the proposed scope, duration, and start date of the audit. 5.1.2.i will review the audit plan and provide Customer with any concerns or questions (for example, any request for that could compromise 5.1.2.i security, privacy, or employment policies). 5.1.2.i will work cooperatively with Customer to agree on a final audit plan.

The audit must be conducted during regular business hours at the applicable facility, subject to 5.1.2.i policies, and may not unreasonably interfere with 5.1.2.i business activities. 5.1.2.i will make reasonable efforts to provide requested information required for such an audit to Customer or external auditor authorized according to this agreement.

Customer will provide 5.1.2.i with any audit reports generated in connection with any audit under this section, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of the Agreement and this Data Processing Agreement. The audit reports are Confidential Information of the parties under the terms of the Agreement.

Any audits are at the Customer's expense. Any request for 5.1.2.i to provide assistance with an audit is considered a separate service, and will be invoiced at 5.1.2.i then current hourly rates.

18. Incident Management and Breach Notification

5.1.2.i evaluates and responds to incidents that create suspicion of unauthorized access to or handling of Personal Data. 5.1.2.i will work with Customer, within internal 5.1.2.i lines of business, with the appropriate technical teams and, where necessary, with outside law enforcement to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability

of the software environment, and to establish root causes and remediation steps.

5.1.2.i shall without delay, and no later than within 60 hours, upon becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed by 5.1.2.i notify the Customer: Where the information is available for 5.1.2.i the notification shall at least:

- (i) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (ii) communicate the name and contact details of the data protection officer or other contact point at the Data Processor where more information can be obtained;
- (iii) describe the likely consequences of the personal data breach;
- (iv) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

To the extent required under the GDPR, and upon Customer's request, 5.1.2.i will assist Customer in its obligation to notify the supervisory authority of a personal data breach. If Customer requires 5.1.2.i to provide such assistance, Customer agrees to pay 5.1.2.i then-current fees associated with such assistance.

19. Requests from Data Subject

Considering the nature of the Processing, 5.1.2.i shall implement appropriate technical and organisational measures to support the Customer's obligation to respond to requests regarding exercising the rights of the data subject. 5.1.2.i shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment or deletion of that person's Personal Data. 5.1.2.i shall not respond to any such Data Subject request without Customer's prior written consent, except to confirm that the request relates to Customer.

To the extent Customer, in its use or receipt of the Services, does not have the possibility to correct, amend, block or delete Personal Data, as required by Data Protection Laws, 5.1.2.i shall comply with any reasonable request by Customer to facilitate such actions to the extent 5.1.2.i is legally permitted to do so.

Customer hereby instructs 5.1.2.i to allow, to the extent technically possible, for Customer's access to, and option to edit, the Personal Data from individual Respondents.

The responsibility for ensuring that processing is compliant with applicable law when Customer accesses and edits Personal Data from individual Respondents remains solely with Customer.

5.1.2.i shall provide Customer with reasonable cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use or receipt of the Services.

5.1.2.i may not disclose or provide access to the Data Subject's Personal Data to third parties. Should a request for such disclosure or access be directed to 5.1.2.i 5.1.2.i shall forward this request to Customer.

20. Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, 5.1.2.i will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

5.1.2.i shall take steps to ensure that any natural person acting under 5.1.2.i authority who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by applicable EEA law.

21. Personnel

5.1.2.i shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality and such obligations survive the termination of that persons' engagement with 5.1.2.i

5.1.2.i shall ensure that 5.1.2.i access to Personal Data is limited to those personnel who require such access to perform the Agreement.

Questback Group have appointed data protection officer(s) where such appointment is required by Data Protection Laws. The appointed person(s) may be contacted on the address listed on 5.1.2.i

L

22. Deletion of Personal Data

Following termination of the Agreement, 5.1.2.i will delete all Personal Data in accordance with 5.1.2.i then-current deletion routines, except as may be required by law.

23. Service Analyses

5.1.2.i may (i) compile statistical and other information related to the performance, operation and use of the software provided under the Agreement, and (ii) use data from the software environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes.

5.1.2.i may make analyses as described herein publicly available; however, the analyses will not incorporate Customer's Content or Confidential Information in a form that could serve to identify Customer or any Data Subject, and Service Analyses do not constitute Personal Data.

5.1.2.i retains all intellectual property rights in analyses described herein.

24. Choice of law and legal venue

If the choice of law under the Agreement is the laws of a country in the EEA, the choice of law will apply to this DPA. If the choice of law under the Agreement is the laws of a country outside the EEA, the laws of Norway will govern this DPA, and any disputes that arise out of or are related to this DPA. The parties then submit to the exclusive jurisdiction of any court sitting Norway for the purpose of any action that arises out of or relates to this DPA brought by any party hereto.

Signature

The individuals signing below represent they have authority to bind the named parties to this Data Processing Agreement. Accepted by:

	De Polite academie	5.1.2.i on behalf of 5.1.2.i
Name in print:	5.1.2.i	5.1.2.e
Title:		5.1.2.e
Date:	11-08-2020	16 maart 2020
Signature:	5.1.2.e	5.1.2.e

Appendices::

- Appendix A to Data Processing Agreement

APPENDIX A TO DATA PROCESSING AGREEMENTCustomer/ Controller: **POLICE ACADEMY**

Contact person (Reseller): 5.1.2.e, 5.1.2.i

Processor: 5.1.2.i

Description of Data and Processing

In order to comply with the requirements of the GDPR, the parties must be informed of certain details related to the Personal Data that will be processed.

The list below includes the required information, ref. GDPR Article 28

Subject-matter of the processing:	- Providing software: The Subject-matter of the processing is 5.1.2.i provision of access to its software to Customer, in order to make Customer able to collect, process, store and analyse feedback in 5.1.2.i software accordance with the Agreement. - Support and other services: If applicable in the Agreement, the subject-matter includes provision of Support, Advisory Services and Professional Services related to Customer's access to and use of the software.
Duration of the processing	- Providing software: The duration of the data processing is defined by the Customer in the software on a case-by-case basis, but under no event longer than the duration set forth in the Agreement. - Support and other services: Personal Data will be stored for as long as required ii) to fulfill all obligations deriving from the execution of the Agreement, this DPA or, if applicable, any additional agreements between Customer and 5.1.2.i or ii) required by applicable statutory laws. - Personal Data will be deleted by 5.1.2.i in accordance with its then-current deletion routine.
Nature of the processing in 5.1.2.i provision of access to software:	- User data: In order to fulfil the Agreement, 5.1.2.i collects User data. During registration in 5.1.2.i software, Customer provides information used by 5.1.2.i to identify and store contact persons within Customer's organization in 5.1.2.i system. Furthermore, the information is required in order for 5.1.2.i to know who the registered users of its software are, in accordance with the Agreement. Customer can at any time access and edit, update or delete contact details by logging in with username/password to 5.1.2.i software. Customer may have access to create several users with different privilege levels within their account, depending on the Agreement. The Personal Data will be stored in the environment provided by 5.1.2.i under the Agreement, it will be accessed in case of support inquiries, and it will be used for sending required information relating to software, services and the Agreement to relevant contact persons. - Respondent data: 5.1.2.i provides access to feedback management software online. Surveys used for gathering feedback are created by Customer, who makes them available to relevant individual Respondents of Customer's choice. The Personal data will be provided to the software by the Respondents themselves, and stored in environment provided by 5.1.2.i under the Agreement.
Nature of the processing in 5.1.2.i provision of Support to Customer:	- User data: The Personal Data stored in the environment provided by 5.1.2.i under the Agreement will be accessed by 5.1.2.i Support personnel in case of support inquiries, and it will be used for sending required information relating to software, services and the Agreement to the relevant contact persons. - Respondent data: Access to the Personal Data may take place if customer has support enquiries. If such support enquiries so require, 5.1.2.i support personnel may access, extract, store and change information, including personal data.
Nature of the processing in 5.1.2.i provision of advisory services and Professional Services to Customer, if applicable:	- User data: The Personal Data stored in the environment provided by 5.1.2.i under the Agreement will be accessed by 5.1.2.i Support personnel in case of support inquiries, and it will be used for sending required information relating to software, services and the Agreement to the relevant contact persons. - Respondent data: Access to the Personal Data may take place if specific projects are defined in Agreement. If such specific projects so require, 5.1.2.i consultants may access, extract, store and change information, including personal data.
Purpose for the processing:	5.1.2.i shall process Personal Data solely for the purpose of fulfilling of the Agreement with Customer, and shall not otherwise Process and use Personal Data for purposes other than those set forth in this DPA, the Agreement, or as instructed in writing by Customer. Customer has defined its purpose for the processing of Personal Data in the Software on a case-by-case basis, or in the Agreement. If Customer has not defined the purpose for the data processing, data processing is limited to the following purposes:

	• [purpose to be listed, if applicable]
The Categories of Data Subjects	As the controller, Customer may choose to add or specify Categories of Data subjects. Customer will list such additional or specified categories herein, or inform 5.1.2.i separately in writing. If Customer has not added such additional or specified categories of Data Subjects, the following Categories will be processed: • Users: Data subjects may include, depending on the Agreement, Customer's employees and/or contractors who are determined by Customer to access and use software online, provided to Customer under the Agreement to make or publish surveys, to access reports or for other purposes. • Respondents: Data subjects may include, depending on the Agreement, Customer's employees who respond to employee surveys as Respondents, Customer's clients or potential clients who respond to Customer's customer surveys as Respondents, or any other party who is invited to respond to surveys as Respondents. • [additional categories to be listed, if applicable]
The types of Personal Data	Non-sensitive data: As the controller, Customer may choose to add or specify Types of Personal Data. Customer will list such additional or specified Types of Personal Data herein, or inform 5.1.2.i separately in writing. If Customer has not added such additional or specified Types of Personal Data, the following Types may be processed: • Personal data from Users. Name, e-mail address, telephone number, role, Area of interest, Address. • Personal data from Respondents: Any data in data fields specifically tagged by Customer as Personal Data in the software, Name, e-mail address, address, telephone number, role, Age, Date of Birth, Marital Status, Number of children, Area of interest, employment details business address • [additional types to be listed, if applicable] Sensitive data: As the controller, Customer may choose to collect Special Categories of Data, as described in GDPR Article 9. Customer will list such additional or specified categories herein, or inform 5.1.2.i separately in writing. If Customer has not added such additional or specified special categories of Data, no special categories of data will be processed: • [special categories to be listed, if applicable]

Contact persons

5.1.2.i appoints the following personnel for inquiries and requests related to data protection and/or IT security:

General Counsel/Compliance Officer:	5.1.2.e
Privacy Counsel	5.1.2.e
Group Information Security Officer	5.1.2.e

5.1.2.i has appointed the following persons to act as Data Protection Officer:

Group Data Protection Officer:	5.1.2.e
Data Protection Officer(5.1.2.i)	5.1.2.e

Sub-Processors

The entities listed below may process Personal Data under this DPA. The 5.1.2.i entity which is the Processor under this DPA will be Processor, the remaining entities will be sub-processors.

Sub-processor	Address	Role of sub-processor	Location
---------------	---------	-----------------------	----------

5.1.2.h

Signature

The individuals signing below represent they have authority to bind the named parties to this Appendix A to Data Processing Agreement.

Accepted by:

	POLICE ACADEMY	5.1.2.i on behalf of 5.1.2.i
Name in print:	5.1.2.e	5.1.2.e
Title:		5.1.2.e
Date:	12-08-2020	16 maart 2020
Signature:	5.1.2.e	5.1.2.e



Bezorging dienstkleding en uitrusting (pakketpost)

5.1.2.i

**Verwerkers –
overeenkomst
ARVODI**

Nummer: 5.1.2.i

Ingangsdatum: 9 september 2020

Uitgegeven door: Politie, Politiedienstencentrum - Dienst Verwerving.

Informatie: Inkoopmanagement

Status: Definitief

Versie 1.0

Versie datum 7 september 2020

© Politie, alle rechten voorbehouden.

Niets uit deze uitgave mag worden veeelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

Inhoudsopgave

1.	Begrippen	5
2.	Totstandkoming, duur en einde van de Verwerkersovereenkomst	5
3.	Voorwerp van de Verwerkersovereenkomst	5
4.	Van toepassing zijnde Voorwaarden	6
5.	Voortdurende verplichtingen	7
6.	Teruggave Persoonsgegevens en/of Politiegegevens	7
7.	Intellectuele eigendomsrechten	7
8.	Beveiliging	7
9.	Meldplicht Datalekken en beveiligingsinbreuken	8
10.	Geheimhouding, beschikbaarheid en integriteit	8
11.	Controle	8
12.	Informereren van betrokkenen	9
13.	Aansprakelijkheid	9
14.	Maatregelen toezichthouder	9
15.	Wijziging	10
16.	Slotbepalingen	10

Verwerkersovereenkomst

Inzake de Overeenkomst 'bezorging dienstkleding en uitrusting (pakketpost)'

a) met daarop aanvullend van toepassing de ARVODI-2018

b) Referentienummer: 5.1.2.i

De ondergetekenden:

1. Politie, gevestigd te Den Haag, te dezen vertegenwoordigd door de korpschef van Politie, namens deze mevrouw P.F. Bosman, directeur Politiedienstencentrum, hierna te noemen: de Politie,

en

2. 5.1.2.i (statutair) gevestigd te Eerbeek, te dezen vertegenwoordigd door 5.1.2.e, algemeen directeur, hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- Partijen de Overeenkomst 'bezorging dienstkleding en uitrusting (pakketpost)' met kenmerk 5.1.2.i (hierna te noemen: de Overeenkomst) hebben gesloten;
- in het kader van de uitvoering daarvan Persoonsgegevens in de zin van artikel 4 sub 1 van de Algemene Verordening Gegevensbescherming EU 2016/679 (hierna te noemen: AVG) worden verwerkt en/of Politiegegevens in de zin van artikel 1 onder a van de Wet Politiegegevens (Wpg);
- Opdrachtnemer die in het kader van de uitvoering van de Overeenkomst met de Politie Persoonsgegevens en/of Politiegegevens verwerkt is aan te merken als Verwerker in de zin van de AVG en/of Wpg;
- De Politie als Opdrachtgever Verwerkingsverantwoordelijk is voor de Persoonsgegevens en Politiegegevens;
- Partijen middels deze Verwerkersovereenkomst nadere afspraken over het verwerken van de Persoonsgegevens en/of Politiegegevens door Opdrachtnemer als Verwerker en de geldende wettelijke verplichtingen uit de AVG en/of Wpg waaronder meldplicht Datalek wensen vast te leggen;

KOMEN OVEREEN:

1. Begrippen

Aanvullend op de AVG en Wpg geldt dat de hierna en hiervoor in deze Verwerkersovereenkomst vermelde, met een hoofdletter geschreven begrippen, de volgende betekenis hebben:

1. AP: Autoriteit Persoonsgegevens (<https://autoriteitpersoonsgegevens.nl>)
2. AVG: Algemene Verordening Gegevensbescherming EU 2016/679.
3. Betrokkene: degene op wie de Persoons- of Politiegegevens betrekking hebben.
4. Datalek: een inbreuk op de beveiliging, in de zin van artikel 33 en 34 AVG, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van Persoonsgegevens en/of Politiegegevens waaronder een inbreuk op vertrouwelijkheid, verlies, wijziging van gegevens.
5. Hulpleverancier: een partij of derde die door Opdrachtnemer is ingeschakeld om te ondersteunen bij het uitvoeren van de Overeenkomst. Indien de Hulpleverancier in opdracht van Opdrachtnemer Persoonsgegevens en/of Politiegegevens verwerkt, is Hulpleverancier tevens aan te merken als sub-verwerker.
6. Overeenkomst: de overeenkomst inzake 'bezorging dienstkleiding en uitrusting (pakketpost)' met kenmerk 5.1.2.i. Politie wil onder zijn verantwoordelijkheid vallende Persoonsgegevens en/of Politiegegevens door Opdrachtnemer laten bewerken.
7. Partij: de Politie of Opdrachtnemer, afhankelijk van de context.
8. Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.
9. Wpg: Wet Politiegegevens.

2. Totstandkoming, duur en einde van de Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst treedt in werking na ondertekening door beide Partijen en niet eerder dan de datum waarop de Overeenkomst in werking treedt.
- 2.2 Deze Verwerkersovereenkomst zal van kracht zijn gedurende de looptijd van de Overeenkomst. Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst van rechtswege.
- 2.3 Geen van beide Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

3. Voorwerp van de Verwerkersovereenkomst

- 3.1 Opdrachtnemer Verwerkt in opdracht van de Politie uitsluitend de in Bijlage 1 beschreven categorieën Persoonsgegevens en/of Politiegegevens van de Politie voor het daarin genoemde doel.
- 3.2 Opdrachtnemer zal de Persoonsgegevens en/of Politiegegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de AVG, Wpg en andere toepasselijke regelgeving betreffende de Verwerking van Persoonsgegevens verwerken.
- 3.3 Opdrachtnemer Verwerkt Persoonsgegevens en/of Politiegegevens slechts in opdracht van de Politie voor zover noodzakelijk om de diensten zoals omschreven in de Overeenkomst aan de Politie te verlenen en volgt alle instructies van de Politie dienaangaande op, behoudens afwijkende wettelijke verplichtingen.
- 3.4 Opdrachtnemer heeft geen zeggenschap over het doel en de middelen voor de Verwerking van Persoonsgegevens en/of Politiegegevens. Voor zover niet anders is bepaald in deze Verwerkersovereenkomst, neemt Opdrachtnemer geen beslissingen over het gebruik van de Persoonsgegevens en/of Politiegegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens en/of Politiegegevens. De zeggenschap over de Persoonsgegevens en/of Politiegegevens verstrekt onder deze Verwerkersovereenkomst komt nimmer bij Opdrachtnemer te berusten.
- 3.5. Opdrachtnemer schakelt geen Hulpleveranciers in zonder schriftelijke voorafgaande toestemming van de Politie. Aan toestemming van de Politie voor de inschakeling van Hulpleveranciers zullen in ieder geval de volgende voorwaarden worden verbonden:
 - a. Opdrachtnemer heeft een schriftelijke overeenkomst met de desbetreffende Hulpleverancier waarin in ieder geval het volgende is opgenomen:
 - een verplichting dat de Hulpleverancier dient te handelen in overeenstemming met alle bepalingen uit deze Verwerkersovereenkomst;

- een verplichting dat de Hulpverlener alle aanwijzingen met betrekking tot de verwerking van Persoonsgegevens en/of Politiegegevens van de Politie en Opdrachtnemer opvolgt inclusief de verplichting tot geheimhouding en het nemen van de nodige beveiligingsmaatregelen als beschreven in Bijlage 1;
 - een verplichting van de Hulpverlener om de Persoonsgegevens en/of Politiegegevens uitsluitend in opdracht en volgens de instructies van Opdrachtnemer te verwerken;
 - een verplichting van de Hulpverlener om zelf geen sub-opdrachtnemers in te schakelen, zonder de voorafgaande schriftelijke toestemming van de Politie;
 - een verplichting dat de Hulpverlener de Opdrachtnemer (en daarmee de Politie) in staat stelt zijn verplichtingen in het geval van een vermoedelijk of daadwerkelijk Datalek na te komen.
- b. Opdrachtnemer geeft de Hulpverlener pas toegang tot de Persoonsgegevens en/of Politiegegevens na de schriftelijke toestemming van de Politie; en
- c. De Politie is gerechtigd om op eerste verzoek de gemaakte afspraken tussen Opdrachtnemer en de Hulpverlener in te zien. Opdrachtnemer zal uiterlijk 30 dagen na ontvangst van dit verzoek een afschrift aan de Politie verstrekken.

De door de Politie gegeven toestemming laat onverlet de verantwoordelijkheid en aansprakelijkheid van Opdrachtnemer voor de nakoming van zijn verplichtingen onder de Verwerkersovereenkomst.

- 3.6 Het is Opdrachtnemer uitdrukkelijk niet toegestaan Persoonsgegevens en/of Politiegegevens aan anderen dan de Politie te verstrekken, tenzij op schriftelijk verzoek van de Politie, of met diens schriftelijke toestemming. Opdrachtnemer is na verleende toestemming verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden, waarbij hij binnen 30 dagen exact de verstrekte Persoonsgegevens en/of Politiegegevens, de Betrokkene(n), de ontvanger(s) en het moment van verstrekking gedocumenteerd aan de Politie dient te beschrijven.
- 3.7 Indien Opdrachtnemer op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert Opdrachtnemer de grondslag van het verzoek en de identiteit van de verzoeker en informeert hij onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, de Politie ter zake.
- 3.8 Opdrachtnemer verleent de Politie volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG en/of Wpg, meer in het bijzonder de rechten van Betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens en/of Politiegegevens en het uitvoeren van een gehonoreerd aangetekend verzet.
- 3.9 Indien Opdrachtnemer onrechtmatige Verwerkingen of inbreuken op de in artikel 8.1 van deze Verwerkersovereenkomst genoemde beveiligingsmaatregelen signaleert, zal hij de Politie hierover onmiddellijk inlichten en alle redelijkerwijs benodigde maatregelen treffen om deze en verdere onrechtmatige Verwerkingen of inbreuken te beëindigen, te voorkomen of te beperken en en ander onverminderd de verplichting van Opdrachtnemer om de eventueel door de Politie daardoor geleden schade te vergoeden.
- 3.10 De eventuele met de in de artikelen 3.8, artikel 3.9 en artikel 9 van deze Verwerkersovereenkomst gemoeide kosten komen voor rekening van degene die die kosten maakt.
- 3.11 De Politie en Opdrachtnemer zorgen ervoor dat de Functionaris voor de gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van Persoonsgegevens en/of Politiegegevens.
- 3.12 Opdrachtnemer documenteert alle inbreuken die in artikel 33 lid 5 AVG zijn beschreven.
- 3.13 Opdrachtnemer verleent alle benodigde medewerking in het kader van een gegevensbeschermingseffectbeoordeling in het kader van artikel 35 AVG. Voor het verlenen van deze medewerking is de Politie geen (aanvullende) vergoeding aan Opdrachtnemer verschuldigd.

4. Van toepassing zijnde Voorwaarden

- 4.1 Op deze Verwerkersovereenkomst zijn de bepalingen van de Overeenkomst van toepassing voor zover daarvan in deze Verwerkersovereenkomst niet wordt afgeweken.

5. Voortdurende verplichtingen

- 5.1 In aanvulling op artikel 32 van de ARVODI-2018 geldt dat na afloop van de Overeenkomst en de Verwerkersovereenkomst de lopende verplichtingen van Opdrachtnemer in stand blijven, zoals, doch niet beperkt tot overdracht, signalering van ongeautoriseerde Verwerkingen en geheimhouding, als ook nader bepaald in de artikelen 3.8, 3.9, 8, 9 en 10 van deze Verwerkersovereenkomst.

6. Teruggave Persoonsgegevens en/of Politiegegevens

- 6.1 Binnen een maand na afloop van de Overeenkomst en de Verwerkersovereenkomst dienen alle Persoonsgegevens en/of Politiegegevens, kopieën en bewerkingen daarvan, alsmede alle gegevensdragers waarop de Persoonsgegevens en/of Politiegegevens, kopieën of bewerkingen daarvan zijn of zullen worden vastgelegd, zijn overgebracht naar een separate beveiligde digitale omgeving voor eventuele wettelijke doeleinden en na afloop van de wettelijke bewaartermijn worden vernietigd. De Politie kan Opdrachtnemer vragen gegevens beschikbaar te stellen en zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat. Op het moment dat deze Verwerkersovereenkomst eindigt, zal Opdrachtnemer bovendien al zijn medewerking verlenen ter zake van de overdracht van de werkzaamheden inzake de Verwerking van de Persoonsgegevens en/of Politiegegevens aan de Politie of een opvolgende opdrachtnemer en wel op een zodanige wijze dat vanaf het moment dat de overdracht plaatsvindt de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Opdrachtnemer wordt belemmerd.
- 6.2 De kosten gemoeid met de inspanningen van Opdrachtnemer als genoemd in 6.1, komen voor rekening van de Politie voor zover deze kosten niet inbegrepen zijn in de overeengekomen prijzen en vergoedingen van Opdrachtnemer voortvloeiende uit de uitvoering van de Overeenkomst.
- 6.3 Opdrachtnemer zal te allen tijde de hiervoor in artikel 6.1 beschreven dataportabiliteit waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

7. Intellectuele eigendomsrechten

- 7.1 Onder verwijzing naar artikel 24 van de - 2018 blijven alle (intellectuele) eigendomsrechten - daaronder begrepen auteursrechten en databankenrechten - op de verzameling van Persoonsgegevens en/of Politiegegevens, kopieën of bewerkingen daarvan, blijven te allen tijde berusten bij de Politie of haar licentiegever(s).

8. Beveiliging

- 8.1 In aanvulling op artikel 14.1 van de ARVODI-2018 zal Opdrachtnemer alle technische en organisatorische beveiligingsmaatregelen implementeren zoals beschreven in Bijlage 1. Deze maatregelen zullen, met inachtneming van de stand der techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, zulks met inachtneming van de risico's die het verwerken van de Persoonsgegevens en/of Politiegegevens, en de aard daarvan, meebrengen.
- 8.2 Opdrachtnemer rapporteert periodiek met een frequentie van 1 maal per jaar, uiterlijk op 31 december aan de Politie over de door Opdrachtnemer genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.
- 8.3 De met de rapportage gemoeide kosten zijn voor rekening van Opdrachtnemer.
- 8.4 Opdrachtnemer Verwerkt geen Persoonsgegevens en/of Politiegegevens buiten een lidstaat van de Europese Unie en/of de Europese Economische Ruimte (Noorwegen, Liechtenstein en IJsland).

9. Meldplicht Datalekken en beveiligingsinbreuken

- 9.1 In het geval van een daadwerkelijk(e) (i) Datalek; (ii) schending van de beveiligingsmaatregelen; (iii) schending van de geheimhoudingsplicht of (iv) verlies van vertrouwelijke gegevens zal Opdrachtnemer de Politie direct, doch uiterlijk binnen 24 uur na de eerste ontdekking van het incident, informeren. De Opdrachtnemer zal alle redelijkerwijs benodigde maatregelen treffen om (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige verwerking te voorkomen of te beperken en een schending van beveiligingsmaatregelen, schending van de geheimhoudingsplicht of verder verlies van vertrouwelijke gegevens te beëindigen en in de toekomst te voorkomen, onverminderd enig recht van de Politie op schadevergoeding of andere maatregelen voor zover het incident toerekenbaar is aan Opdrachtnemer of de door haar in te zetten Hulpverlenancier. Deze bepaling is van toepassing op incidenten bij de Opdrachtnemer en haar eventuele Hulpverlenici.
- 9.2 De informatie van de Opdrachtnemer behelst in ieder geval de in de Bijlage 2 beschreven gegevens voor zover toepasselijk. Opdrachtnemer garandeert dat de verstrekte informatie volledig, correct en accuraat is.
- 9.3 Opdrachtnemer zal op verzoek van de Politie meewerken aan het informeren van de bevoegde autoriteiten en betrokkene(n).

10. Geheimhouding, beschikbaarheid en integriteit

- 10.1 Onder verwijzing naar artikel 13.1 van de ARVODI-2018 is Opdrachtnemer gehouden tot geheimhouding, en borging van de beschikbaarheid en integriteit van alle Persoonsgegevens en/of Politiegegevens en informatie die zij als uitvloeisel van deze Verwerkersovereenkomst verwerkt, behoudens in zoverre die Persoonsgegevens of informatie klaarblijkelijk geen geheim of vertrouwelijk karakter hebben, dan wel reeds algemeen bekend zijn.
- 10.2 Indien en voor zover de Politie daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer ten aanzien van de daarbij aangeduide Persoonsgegevens en/of Politiegegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken Persoonsgegevens en/of Politiegegevens of informatie zodra de noodzaak voor Opdrachtnemer om daarvan nog langer kennis te nemen, is komen te vervallen.
- 10.3 Onder verwijzing naar artikel 13.2 van de ARVODI-2018 zal Opdrachtnemer in haar arbeids- of inhuurovereenkomsten met het personeel van Opdrachtnemer bedingen dat door die personen op overeenkomstige wijze als in artikel 10.1 en 10.2 bepaald geheimhouding zal worden betracht ten aanzien van alle Persoonsgegevens en/of Politiegegevens en informatie die zij in het kader van hun werkzaamheden verwerken. Opdrachtnemer staat er jegens de Politie voor in dat de bedoelde bedingen door de betrokken personen zullen worden nageleefd.
- 10.4 Na afloop van de Overeenkomst en deze Verwerkersovereenkomst blijft dit artikel 10 en de hierin besproken geheimhouding van kracht.

11. Controle

- 11.1 De Politie controleert op elk door haar gewenst moment dan wel laat op elk door haar gewenst moment:
 - a. de verwerkingen en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer dan wel die van door Opdrachtnemer ingeschakelde Hulpverlenici controleren, en
 - b. de naleving van de in Bijlage 2 genoemde gegevens, die nodig zijn om aan de meldplicht, bedoeld in artikel 34 AVG, te voldoen controleren.
- 11.2 Opdrachtnemer verstrekt met een frequentie van 1 maal per jaar, uiterlijk op 31 december aan de Politie een verklaring, van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving als bedoeld in artikel 11.1 a en b. en deze separaat benoemen in de audit.
- 11.3 Opdrachtnemer zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde Hulpverlenici hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.

- 11.4 Het uitvoeren van een controle zal niet tot een vertraging van de door Opdrachtnemer in het kader van de Overeenkomst en deze Verwerkersovereenkomst te verrichten werkzaamheden mogen leiden. Indien dat onverhoopt toch het geval is, zullen Partijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.
- 11.5 De met de controle gemoeide kosten zijn voor rekening van de Politie tenzij uit de controle blijkt dat Opdrachtnemer is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Verwerkersovereenkomst en/of de Overeenkomst.
- 11.6 Opdrachtnemer voert de door de Politie aangegeven aanbevelingen ter verbetering uit binnen de daartoe door de Politie te bepalen termijn.

12. Informeren van betrokkenen

- 12.1 Opdrachtnemer zal haar volledige medewerking verlenen opdat de Politie kan voldoen aan zijn wettelijke verplichtingen in het geval dat een Betrokkene zijn rechten uitoefent op grond van de AVG, Wpg of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens en/of Politiegegevens.
- 12.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten onder de AVG en/of Wpg direct contact opneemt met Opdrachtnemer, dan gaat Opdrachtnemer hierbehoudens uitdrukkelijke andersluidende instructie van de Politie - in eerste instantie niet (inhoudelijk) op in, maar bericht hij dit onverwijld aan de Politie met een verzoek om nadere instructies.
- 12.3 Als Opdrachtnemer zijn diensten in het kader van de Overeenkomst rechtstreeks aanbiedt aan Betrokkene, dan is Opdrachtnemer verplicht om op een makkelijk toegankelijke en permanent beschikbare manier de Politie te informeren over het volgende:
 - a. de naam en het adres van de Opdrachtnemer;
 - b. de doeleinden waarvoor Opdrachtnemer de Persoonsgegevens en/of Politiegegevens verwerkt;
 - c. de categorieën Persoonsgegevens en/of Politiegegevens die de Opdrachtnemer verwerkt;
 - d. de derden aan wie de Persoonsgegevens en/of Politiegegevens toegankelijk worden gemaakt;
 - e. de landen waarnaar de Persoonsgegevens en/of Politiegegevens worden overgedragen;
 - f. het recht op inzage, correctie en verwijdering van de Persoonsgegevens en/of Politiegegevens.
 De Opdrachtnemer zal de Politie laten weten waar deze informatie gepubliceerd is.

13. Aansprakelijkheid

- 13.1 Onverminderd het bepaalde in artikel 21 van de ARVODI-2018 en artikel 83 AVG, is Opdrachtnemer aansprakelijk voor een door de AP opgelegde bestuurlijke boete dan wel door Betrokkene(n) of de Politie geleden schade, voor zover die bestuurlijke boete respectievelijk die geleden schade het gevolg is van toerekenbaar tekortschieten in de nakoming van haar verplichtingen door Opdrachtnemer of zijn Hulpverlener(s).

14. Maatregelen toezichthouder

- 14.1 Indien de AP in het kader van haar taak als handhaver een maatregel of boete oplegt aan de Politie en indien de oorzaak voor het opleggen van de maatregel of boete te wijten is aan het niet nakomen van de in de Verwerkersovereenkomst gemaakte afspraken door Opdrachtnemer of diens Hulpverlener, dan kan de Politie alle kosten voor deze maatregel of boete verhalen op de Opdrachtnemer. Tevens heeft de Politie het recht om de Overeenkomst in bovengenoemde situatie met onmiddellijke ingang te ontbinden zonder dat de Opdrachtnemer aanspraak kan maken op enige vorm van schadevergoeding.

15. Wijziging

- 15.1 Indien een functionele wijziging in de te verwerken Persoonsgegevens en/of Politiegegevens of een controle als bedoeld in artikel 11 van deze Verwerkersovereenkomst daartoe aanleiding geeft treden Partijen op eerste verzoek van de Politie in overleg over het aanpassen van de gemaakte afspraken binnen deze Verwerkersovereenkomst.
- 15.2 De nieuw te maken afspraken dienen voorafgaand aan de toepassing daarvan schriftelijk te zijn vastgelegd en deel uit te maken van deze Verwerkersovereenkomst.
- 15.3 De wijzigingen kunnen nooit tot gevolg hebben dat de Politie niet kan voldoen aan de AVG, Wpg en overige relevante wet- en regelgeving met betrekking tot Persoonsgegevens en/of Politiegegevens.

16. Slotbepalingen

- 16.1 Afwijkingen van deze Verwerkersovereenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.
- 16.2 Algemene leveringsvoorwaarden dan wel andere algemene of bijzondere voorwaarden van Opdrachtnemer en diens Hulpleverancier zijn niet van toepassing op deze Verwerkersovereenkomst en worden door de Politie uitdrukkelijk van de hand gewezen.
- 16.3 Deze Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst. Bij strijdigheid tussen bepalingen uit deze Verwerkersovereenkomst en de Overeenkomst prevaleren de bepalingen uit deze Verwerkersovereenkomst.
- 16.4 Op deze Verwerkersovereenkomst is het Nederlands recht van toepassing.

Aldus overeengekomen en in tweevoud ondertekend,

De Politie

De korpschef van Politie, namens deze,

5.1.2.e



Directeur Politiedienstencentrum

5.1.2.i

5.1.2.e



5.1.2.e

Bijlage 1 Werkprocessen, autorisaties en functiegroepen verwerking

De verwerking door Opdrachtnemer ziet toe op de volgende gegevens:

Categorieën Betrokkenen

5.1.2.i [Redacted]

De te verwerken (categorieën) Persoonsgegevens en/of Politiegegevens

5.1.2.i [Redacted]

Doel van de verwerking

De genoemde gegevens worden verwerkt om:

5.1.2.i [Redacted]

Functierollen en/of functiegroepen van personeel van Opdrachtnemer en hun verwerkingen;

De medewerkers Customer Service, de medewerkers transportplanning en de chauffeurs

5.1.2.i [Redacted]

[Redacted]

Voor de duur van de Verwerkersovereenkomst en / of wettelijke bewaartermijnen.

Contactgegevens Opdrachtnemer

5.1.2.e [Redacted]

Contactgegevens Hulpverleners mits goedgekeurd door de Politie

Er wordt geen gebruik gemaakt van hulpverleners welke toegang hebben tot persoons- en/of politie gegevens.

Technische en organisatorische beveiligingsmaatregelen

1. Opdrachtnemer en diens Hulpverancier zijn in het bezit van:

X een geschreven beveiligingsbeleid conform ISO 27001 inzake Information Security Management

X een geschreven kwaliteitsbeleid conform ISO 9001 inzake Quality Management

5.1.2.i

21

Bijlage 2 Procedure en Maatregelen in verband met de meldplicht datalekken

Informatie die moet worden verstrekt bij een Datalek

Als Opdrachtnemer de Coördinator Informatiebeveiliging van de Politie moet informeren op grond van artikel 5 van de Verwerkersovereenkomst, zal zij de volgende gegevens moeten verschaffen:

Contactgegevens melder

- Naam;
- Functie;
- E-mailadres;
- Telefoonnummer.

Gegevens over het Datalek

- Samenvatting van het incident waarbij de inbreuk op de beveiliging van Persoonsgegevens en/of Politiegegevens zich heeft voorgedaan.
- Van hoeveel personen zijn Persoonsgegevens en/of Politiegegevens betrokken bij de inbreuk?
 - a) Minimaal aantal personen
 - b) Maximaal aantal personen
- Omschrijving van de groep mensen van wie Persoonsgegevens en/of Politiegegevens zijn betrokken bij het incident.
- Wanneer de inbreuk plaats vond?
 - a) Datum
 - b) Tussen (begindatum periode) en (einddatum periode)
 - c) Nog niet bekend
- Wat de aard van de inbreuk is (meerdere mogelijkheden mogelijk):
 - a) Lezen (vertrouwelijkheid)
 - b) Kopiëren
 - c) Veranderen (integriteit)
 - d) Verwijderen of vernietigen (beschikbaarheid)
 - e) Diefstal
 - f) Nog niet bekend
- Om welke type Persoonsgegevens en/of Politiegegevens het gaat (meerdere mogelijkheden mogelijk):
 - a) Naam -, adres - en woonplaatsgegevens
 - b) Telefoonnummers
 - c) E - mailadressen of andere adressen voor elektronische communicatie
 - d) Toegangs - of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
 - e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
 - f) Burgerservicenummer (BSN) of sofinummer
 - g) Paspoortkopieën of kopieën van andere legitimatiebewijzen
 - h) Geslacht, geboortedatum en/of leeftijd
 - i) Bijzondere Persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
 - j) Overige gegevens, namelijk <vul aan>
- Welke gevolgen de inbreuk kan hebben voor de persoonlijke levenssfeer van de betrokkenen (meerdere mogelijkheden mogelijk):
 - a) Stigmatisering of uitsluiting

- b) Schade aan de gezondheid
- c) Blootstelling aan (identiteits)fraude
- d) Blootstelling aan spam of phishing
- e) Anders, namelijk <vul aan>

Vervolgacties naar aanleiding van het Datalek

- De volgende technische en organisatorische maatregelen zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen:
<beschrijving technische en organisatorische maatregelen>

Technische beschermingsmaatregelen

- Zijn de Persoonsgegevens en/of Politiegegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
 - a) Ja
 - b) Nee
 - c) Deels, namelijk: <vul aan>
- Als de Persoonsgegevens en/of Politiegegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?
<Beantwoord deze vraag als bij de vorige vraag optie a of optie c van toepassing is. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.>

Internationale aspecten

- Heeft de inbreuk betrekking op personen in andere EU-landen?
 - a) Ja
 - b) Nee
 - c) Nog niet bekend



**RAAMOVEREENKOMST VERWERKING PERSOONSGEGEVENS TNO-(POLITIE)ACADEMIE
KENNIS OPBOUW POLITIE (KOP)**

1. SAMENWERKENDE PARTNERS	
(1)	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO , een publiekrechtelijke rechtspersoon op basis van artikel 3 van de TNO-wet, thans kantoorhoudende aan het Anna van Buerenplein 1, 2595 DA te Den Haag, te dezen rechtsgeldig vertegenwoordigd door haar Raad van Bestuur, namens deze ^{5.1.2.e} , hierna te noemen ' TNO ',
(2)	De politie , gevestigd te Den Haag, te dezen vertegenwoordigd door de Directie Strategie en Innovatie, namens deze, Directeur van de directie Jeroen van Vugt, hierna te noemen ' politie ', en
(3)	De Politieacademie , gevestigd te Apeldoorn, te dezen vertegenwoordigd door de directie van ZBO Politieacademie namens deze ^{5.1.2.e} , hierna te noemen: ' Politieacademie ',

TNO, de Politie en de Politieacademie worden gezamenlijk ook aangeduid als "**Samenwerkende Partners**" en elk afzonderlijk tevens als "**Partner**"

2. INLEIDING
Deze regeling heeft tot doel om de verantwoordelijkheden van Samenwerkende Partners te beschrijven in verband met de Verwerking van persoonsgegevens in het kader van het Kennis Opbouw Politie (KOP). De programmering KOP is een samenwerking tussen de samenwerkende partners. De programmering KOP heeft als voornaamste doel om de politie proactief te laten inspelen op nieuwe technologieën en maatschappelijke ontwikkelingen. Het werken met state-of-the-art intelligence en technologie is een van de strategische prioriteiten van de politie en de Politieacademie om een veiligere samenleving te kunnen blijven garanderen. TNO is daarbij een partner door de kracht in multidisciplinaire kennis van mens & technologie. Hierdoor kunnen er voor de politie toepassingsgerichte integrale resultaten worden geleverd. Een onderdeel van KOP richt zich op de verdere ontwikkeling van politiemedewerkers als veiligheidsprofessional. Veiligheidsprofessionals moeten weerbaar zijn om te functioneren in de wereld waar ze dagelijks in opereren. Het programma onderzoekt wat technologische- en intelligence-ontwikkelingen in combinatie met maatschappelijke veranderingen vragen van vakmanschap, weerbaarheid en adaptief vermogen van de professional. KOP draagt bij op het vermogen van de politieorganisatie om hierop in te spelen. Een voorbeeld hiervan is het weerbaarheidsdashboard voor leidinggevend. Een ander onderdeel van KOP richt zich op de flexibilisering van leren en ontwikkelen bij de politie. Hierbij wordt onderzocht op welke manier het onderwijs op de Politieacademie flexibeler en meer praktijkgericht kan worden ingericht, gebruikmakend van learning analytics (verzamelde leerdata), en welke 21st century skills nodig zijn voor het toekomstig politiewerk, met name in de opsporing. Het programma KOP bestaat uit verschillende onderzoeksprojecten die gezamenlijk worden uitgevoerd door de samenwerkende partners. Ten behoeve van de doeleinden van KOP kunnen persoonsgegevens van politiemedewerkers worden verwerkt. Binnen de programmering KOP kan iedere samenwerkende partner een rol hebben bij de gegevensverwerking. Deze rol is niet altijd evenredig verdeeld. Nu sprake is van gezamenlijke doeleinden binnen het programma KOP waarvoor persoonsgegevens worden verwerkt, wensen de samenwerkende partners deze raamovereenkomst vast te stellen waarin hun verantwoordelijkheden ten aanzien van de verplichtingen die volgen uit de AVG worden vastgelegd.

Deze raamovereenkomst geldt als een regeling voor gezamenlijke verwerkingsverantwoordelijken als bedoeld in artikel 26 van de AVG. De Samenwerkende Partners stellen immers gezamenlijk de doeleinden van en de middelen voor de verwerking van Persoonsgegevens binnen de onderzoeksprojecten van KOP vast. Samenwerkende Partners trachten met deze regeling ervoor te zorgen dat Persoonsgegevens op een consistente en legitieme wijze worden verwerkt opdat de vertrouwelijkheid van de Persoonsgegevens blijft gewaarborgd. De Samenwerkende Partners zorgen er in ieder geval voor dat het gebruik van Persoonsgegevens in het kader van het onderzoek/ project tot het minimale beperkt blijft waarbij tevens het uitgangspunt is dat zoveel mogelijk gebruik wordt gemaakt van Persoonsgegevens die niet meer direct te herleiden zijn tot een individu. In Annex A worden bepaalde termen die in deze regeling worden gehanteerd nader gedefinieerd.

3. PERSOONSGEGEVENS

De Politie verwerkt ten behoeve van het onderzoek de volgende Persoonsgegevens:

- Persoonsgegevens (contactgegevens);
- Persoonsgegevens gerelateerd aan personeelsdata zoals functie, opleiding, eenheid en interactie met IT systemen;

De Politieacademie verwerkt ten behoeve van het onderzoek de volgende Persoonsgegevens:

- Toetsresultaten van studenten;
- Gevolgde modules door studenten.
- Evaluatieresultaten van studenten.

Naast de gegevens die door de Politie en de Politieacademie worden verwerkt, verzamelt TNO ook zelf Persoonsgegevens onder medewerkers die deelnemen aan onderzoek. Daarbij kan TNO, voor zover noodzakelijk, ook bijzondere Persoonsgegevens verzamelen en verder Verwerken, zoals:

- Gegevens over gezondheid (vragenlijsten en via wearables);
- Gegevens over motivatie, welbevinden (vragenlijsten)
- Gegevens over psychosociale arbeidsbelasting (o.a. ervaren incidenten);
- Gegevens over prestatie (zelfevaluatie, beoordeling instructeur).

Deze gegevens worden nooit aan de politie en Politieacademie verstrekt. TNO verstrekt onderzoeksresultaten in rapportages aan de Politie die niet direct te herleiden te zijn tot een individu, door de gegevens te aggregeren op minimaal n=10 niveau zodat die niet meer te herleiden zijn tot een individuele medewerker van de Politie of Politieacademie.

4. VERWERKINGEN

De politie en de Politieacademie voeren ten aanzien van de persoonsgegevens de volgende verwerkingen uit:

- Verzamelen en verstrekken van contactgegevens;
- Verzamelen en verstrekken van persoonsgegevens gerelateerd aan personeelsdata zoals functie, opleiding, eenheid en interactie met IT systemen.
- Pseudonimiseren van persoonsgegevens.

De politieacademie kan daarnaast uitdrukkelijk wel pseudonieme persoonsgegevens ontvangen van TNO ten behoeve van gezamenlijk onderzoek binnen de doelstellingen van KOP.

TNO voert ten aanzien van de persoonsgegevens de volgende verwerkingen uit:

- Ontvangen van contactgegevens;