



**[contractnaam]**  
**[perceel # en naam]**

**[opdrachtnemer]**

**Verwerkers-  
Overeenkomst  
ARBIT**

**Nummer:**

**Ingangsdatum:**

Uitgegeven door: Politie, Politiedienstencentrum - Dienst Verwerving

Status: Kies op dropdown om status te kiezen

Versie: Klik hier als je tekst wilt invoeren.

Versie datum: Klik op dropdown om datum in te invoeren.

# Inhoudsopgave

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

## Verwerkersovereenkomst

inzake de Overeenkomst <aangeven op welke Overeenkomst de Verwerkersovereenkomst betrekking heeft>

a) met daarop aanvullend van toepassing de ARBIT-2018

b) Referentienummer: <nummer>

### De ondergetekenden:

1. De Politie, gevestigd te Den Haag,  
te dezen rechtsgeldig vertegenwoordigd door de korpschef van politie,  
te dezen rechtsgeldig vertegenwoordigd door <functie>, <naam>  
hierna te noemen: 'de Politie',

en

2. naam <leverancier>, (statutair) gevestigd te <plaats>  
te dezen rechtsgeldig vertegenwoordigd door <functie>, <naam>  
hierna te noemen: 'Opdrachtnemer',

hierna gezamenlijk te noemen: 'Partijen;

### OVERWEGENDE DAT:

- Partijen de Overeenkomst inzake <naam/onderwerp overeenkomst> met kenmerk <nummer> (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 Persoonsgegevens 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 <naam/onderwerp overeenkomst> met kenmerk <nummer>, waarin de Politie onder zijn verantwoordelijkheid vallende Persoonsgegevens en/of Politiegegevens door Opdrachtnemer wil 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 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 **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 Hulpleverancier 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 Hulpleverancier om de Persoonsgegevens en/of Politiegegevens uitsluitend in opdracht en volgens de instructies van Opdrachtnemer te verwerken;
  - een verplichting van de Hulpleverancier om zelf geen sub-opdrachtnemers in te schakelen, zonder de voorafgaande schriftelijke toestemming van de Politie;
  - een verplichting dat de Hulpleverancier 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 Hulpleverancier 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 Hulpleverancier 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 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 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

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

## 5. Voortdurende verplichtingen

In aanvulling op artikel 34 van de ARBIT-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 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.
- 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

Onder verwijzing naar artikel 8 van de ARBIT-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 18.1 van de ARBIT-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 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 Hulpleverancier. Deze bepaling is van toepassing op incidenten bij de Opdrachtnemer en haar eventuele Hulpleveranciers.
- 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 17.1 van de ARBIT-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 17.2 van de ARBIT-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:
- de verwerkingen en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer dan wel die van door Opdrachtnemer ingeschakelde Hulpleveranciers controleren,
  - en
  - 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.
- 11.3 Opdrachtnemer zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde Hulpleveranciers 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

Onverminderd het bepaalde in artikel 26 van de ARBIT-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 Hulpleverancier(s).

## 14. 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.

## 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 op de laatste van de twee hierna genoemde data overeengekomen in 16 artikelen en twee bijlagen en in tweevoud ondertekend,

de *Opdrachtgever*  
De Politie,

Namens deze,

<functie>

<naam>

de *Opdrachtnemer*  
Namens <leverancier>

Namens deze,

<functie>

<naam>

## Bijlage 1 Werkprocessen, autorisaties en functiegroepen verwerking

De verwerking door Opdrachtnemer ziet toe op de volgende gegevens:

### Categorieën Betrokkenen

<omschrijving>

### De te verwerken (categorieën) Persoonsgegevens en/of Politiegegevens

<omschrijving>

**Instructie:** Als je niet precies weet welke gegevens er allemaal worden verwerkt en je wilt dit breed houden dan kun je deze zin opnemen: '...alle gegevens waarmee [Opdrachtnemer] in het kader van de uitvoering van de opdracht in aanraking komt...'

### Doel van de verwerking

<omschrijving>

### Functierollen en/of functiegroepen van Personeel van Opdrachtnemer en hun verwerkingen;

<omschrijving>

### Bewaartermijnen

Voor de duur van de Verwerkersovereenkomst

### Contactgegevens Opdrachtnemer

<contactgegevens>

### Contactgegevens Hulpleveranciers mits goedgekeurd door de Politie

<bedrijfsnaam, adres en contactgegevens van de contactpersoon van Hulpleverancier>

### Technische en organisatorische beveiligingsmaatregelen

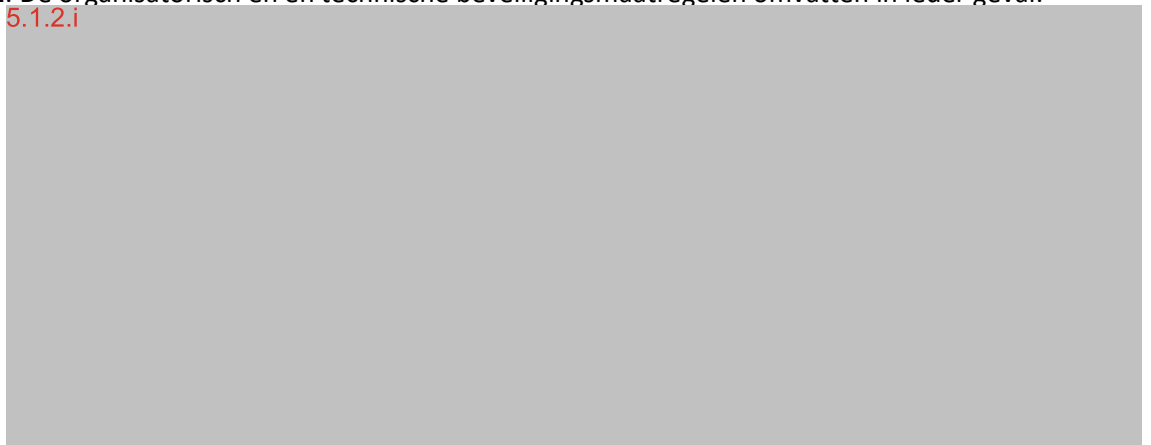
1. Opdrachtnemer en diens Hulpleverancier in het bezit te zijn\* van:

\*aankruisen wat van toepassing is

- ☐ een geschreven beveiligingsbeleid conform ISO 27001 inzake Information Security Management
- ☐ een geschreven kwaliteitsbeleid conform ISO 9001 inzake Quality Management
- ☐ anders, nl.

2. De organisatorisch en en technische beveiligingsmaatregelen omvatten in ieder geval:

5.1.2.i



5.1.2.i



## 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, emailadres, telefoonnummer>

#### Gegevens over het Datalek

- Samenvatting van het incident waarbij de inbreuk op de beveiliging van Persoonsgegevens en/of Politiegegevens zich heeft voorgedaan:

<samenvatting>

- Van hoeveel personen zijn Persoonsgegevens en/of Politiegegevens betrokken bij de inbreuk?

<Vul de aantallen in>

a) Minimaal: <vul aan>

b) Maximaal: <vul aan>

- Omschrijving van de groep mensen van wie Persoonsgegevens en/of Politiegegevens zijn betrokken bij het incident

<omschrijving>

- Wanneer vond de inbreuk plaats?

<Kies een van de volgende opties en vul waar nodig aan>

a) Op <datum>

b) Tussen <begindatum periode> en <einddatum periode>

c) Nog niet bekend

- Wat is de aard van de inbreuk ?

<meerdere mogelijkheden aankruisen>

☐ a) Lezen (vertrouwelijkheid)

☐ b) Kopiëren

☐ c) Veranderen (integriteit)

☐ d) Verwijderen of vernietigen (beschikbaarheid)

☐ e) Diefstal

☐ f) Nog niet bekend

- Om welk type Persoonsgegevens en/of Politiegegevens gaat het?

< meerdere mogelijkheden aankruisen>

☐ 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): <geef aan welke bijzondere persoonsgegevens>
- ☐ j) Overige gegevens, namelijk <vul aan>

- Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

<meerdere mogelijkheden aankruisen>

- ☐ 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 beschermingsmaatregelen

- Zijn de Persoonsgegevens en/of Politiegegevens versleuteld, gehasht of op een andere manier

onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

<Kies een van de volgende opties en vul waar nodig aan>

- ☐ 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 u bij de vorige vraag gekozen heeft voor optie a of optie c. 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?

< Kies een van de volgende opties>

- ☐ a) Ja
- ☐ b) Nee
- ☐ c) Nog niet bekend





# **Bijlage 3**

## **Concept Nadere overeenkomst EASP2019 Perceel 2**

**Nadere overeenkomst**

**5.1.2.i**

**Monitoringtool  
meldkamerwerk-  
plekken**

**Nummer:**

**Ingangsdatum:**

1. Politie, (statutair) gevestigd te 's-Gravenhage, te dezen vertegenwoordigd door de korpschef de heer E.S.M. Akerboom, namens deze de 5.1.2.e 5.1.2.e), hierna te noemen: Opdrachtgever,

en

2. Naam Wederpartij, (statutair) gevestigd te XX, te dezen vertegenwoordigd door XXNaam en functie ondertekenaar, hierna te noemen: Wederpartij,

**Overwegende dat:**

*Organisatie en doelstelling van Opdrachtgever*

- a. Opdrachtgever in het kader van de uitvoering van zijn wettelijke taak onder meer verantwoordelijk is voor een goed functionerende geautomatiseerde omgeving en daarmee voor een efficiënte en effectieve bedrijfsvoering voor zijn medewerkers en door hem aangewezen gebruikers;
- b. Opdrachtgever in het kader van de uitoefening van zijn taak behoefte heeft aan de producten / diensten zoals beschreven in de Functionele uitvraag 5.1.2.i .
- c. Opdrachtgever in zijn behoefte wenst te voorzien door met Wederpartij een Nadere overeenkomst aan te gaan onder de Raamovereenkomst EASP2019 met kernmerk XXX;

*Verloop van de procedure*

- d. Opdrachtgever in verband met hetgeen hiervoor is overwogen, tot aanbesteding is overgegaan;
- e. Opdrachtgever de opdracht op heeft gegund aan Wederpartij.

**KOMEN OVEREEN:**

**Artikel 1. Begrippen**

In deze Overeenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan is gegeven in de ARBIT-2018 en de Raamovereenkomst EASP2019.

**Artikel 2. Voorwerp van de Overeenkomst**

- 2.1 Partijen sluiten hierbij op basis van de Raamovereenkomst een Nadere overeenkomst waarbij Wederpartij zich tegen de in Artikel 6 bedoelde Vergoeding verbindt tot het verrichten van de Prestatie zoals beschreven in de Nadere uitvraag met kenmerk 5.1.2.i .
- 2.2 De navolgende stukken vormen gezamenlijk de Nadere overeenkomst. Voor zover deze stukken met elkaar in tegenspraak zijn, prevaleert het eerder genoemde stuk boven het later genoemde:
  - 1) de Raamovereenkomst EASP2019;
  - 2) deze Nadere overeenkomst;
  - 3) de Nadere uitvraag (Bijlage 1 bij deze Nadere overeenkomst);
  - 4) de Nadere offerte (Bijlage 2 bij deze Nadere overeenkomst).
  - 6) de Overige voorwaarden / EULA (Bijlage 3 bij deze Nadere overeenkomst)

**Artikel 3. Contactpersonen en rapportage**

- 3.1 De personen die de contacten over de uitvoering van de Nadere overeenkomst onderhouden werken bij de Contractendesk IV; 5.1.2.i @politie.nl.
- 3.2 Wederpartij rapporteert periodiek over de wijze van uitvoering van de Nadere overeenkomst tijdens het operationeel overleg tussen Opdrachtgever en Wederpartij.

**Artikel 4. Inwerkingtreding en duur van de Nadere overeenkomst**

- 4.1 De Nadere overeenkomst treedt in werking op XXdatum.  
De Nadere overeenkomst eindigt op XXdatum.
- 4.2 Opdrachtgever kan de Nadere overeenkomst onder gelijkblijvende voorwaarden 3 maal voor een periode van 12 maanden schriftelijk verlengen.
- 4.3 Wanneer Wederpartij door toeleverancier aantoonbaar dwingend een prijsstijging krijgt opgelegd, kan Opdrachtgever de prijsstijging schriftelijk accepteren of de Nadere overeenkomst beëindigen.
- 4.4 Opdrachtgever kan de Nadere overeenkomst een maand voor het einde van de in Artikel 4.2 bedoelde looptijd of naar aanleiding van Artikel 4.3 schriftelijk beëindigen.

**Artikel 5. Aflevering, Acceptatie en Oplevering, herstel Gebrek**

- 5.1 Wederpartij draagt zorg voor Aflevering, Acceptatie en/of Oplevering volgens de Nadere uitvraag of op instructie van Opdrachtgever. Genoemde termijnen zijn Fatale termijnen.
- 5.2 Indien Opdrachtgever de Prestatie Accepteert ondanks de aanwezigheid van één of meer Gebreken volgens Opdrachtgever, herstelt Wederpartij het Gebrek binnen de termijn die Opdrachtgever daarvoor stelt.

**Artikel 6. Vergoeding, facturering**

- 6.1 Partijen komen de navolgende Vergoeding overeen:  
Prijs inclusief btw: € XXX (volgens de Nadere offerte Bijlage2).
- 6.2 Facturering geschiedt volgens procedure die Opdrachtgever aangeeft.

**Artikel 7. Algemene en bijzondere voorwaarden**

- 7.1 Onverminderd het bepaalde in Artikel 2.2 zijn tevens de Overige voorwaarden / EULA van toepassing (Bijlage 3) indien en voor zover:
- de toepasselijkheid daarvan in de Nadere uitvraag is toegestaan;
  - Wederpartij:
    - (a) de toepasselijkheid daarvan expliciet heeft bedongen;
    - (b) een exemplaar van de betreffende voorwaarden als Bijlage 3 bij deze Nadere overeenkomst is gevoegd en
    - (c) deze expliciet onderdeel uitmaken van de Nadere offerte;
  - het Overeengekomen gebruik daardoor niet (zoals achteraf blijkt) wordt uitgesloten of beperkt en;
  - Wederpartij kan aantonen dat de rechten van Opdrachtgever uit hoofde van de Nadere overeenkomst daardoor niet worden verminderd dan wel diens uit de Nadere overeenkomst voortvloeiende verplichtingen daardoor niet onredelijk worden verzwaaard.
- 7.2 Wederpartij zal op eerste verzoek van Opdrachtgever inzicht bieden in de verwerkingen van persoonsgegevens, inclusief de door of namens Opdrachtgever of gebruikers van Opdrachtgever of andere betrokkenen in het kader van de Prestatie aan Wederpartij verstrekte gegevens, door Wederpartij verzamelde of verkregen (inclusief telemetriegegevens) gegevens van lokaal geïnstalleerde programmatuur, gegevens gegenereerd door Wederpartij door de werking van een Prestatie ten behoeve van zijn legitieme bedrijfsvoering (bijvoorbeeld verwerkingen ten behoeve van de facturering aan Opdrachtgever).
- In het kader van zijn legitieme bedrijfsvoering zal Wederpartij geen persoonsgegevens, inclusief de door of namens Opdrachtgever of gebruikers van Opdrachtgever of andere betrokkenen in het kader van de Prestatie aan Wederpartij verstrekte gegevens, door Wederpartij verzamelde of

verkregen (inclusief telemetriegegevens) gegevens van lokaal geïnstalleerde programmatuur, gegevens gegenereerd door Wederpartij door de werking van een Prestatie verwerken met als doel:

- profilering inclusief, maar niet beperkt tot het creëren van psychometrische, psychografische of andere gebruikersprofielen
- adverteren (inclusief gerichte aanbevelingen op het scherm voor producten of diensten, aangeboden door Wederpartij, maar niet ingeschreven of gebruikt door de Opdrachtgever) of een vergelijkbaar commercieel doel

Opdrachtgever behoudt zich het recht voor audits uit te voeren op de naleving van hetgeen in dit artikel is bepaald. Wederpartij verleent alle benodigde medewerking aan deze audits. Daarnaast behoudt Opdrachtgever zich het recht voor ten aanzien van deze verwerkingen nadere afspraken met Wederpartij te maken.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

plaats, datum

plaats, datum

De korpschef van Politie, namens deze,  
de directeur PDC, namens deze,

Naam Wederpartij

5.1.2.e

XXNaam en functie ondertekenaar

#### **Bijlagen bij deze Nadere overeenkomst:**

Bijlage 1: de Nadere uitvraag;  
Bijlage 2: de Nadere offerte;  
Bijlage 3: de Overige voorwaarden / EULA.

# 5.1.2.i

## Developer Cloud OEM Additional Terms

The documents referenced below together with the Quotation and GTC set forth the terms and conditions of the agreement between Developer and OT regarding use of OT Cloud Services.

| <u>Description</u>        | <u>Page(s)</u> |
|---------------------------|----------------|
| Developer Cloud OEM Annex | 2 - 6          |
| Data Processing Addendum  | 7 - 13         |
| Schedule                  | 14 - 15        |

## 5.1.2.i

### **Developer Cloud OEM Annex** to the GTC referenced on the attached Quotation (this “Annex”).

---

Defined terms in the GTC have the same meaning herein except as noted below.

The term “Customer” as used in the GTC has been replaced with the term “Developer” in this Annex, the Data Processing Addendum (“DPA”), and Schedule.

The term “Cloud Service” as used in the GTC has been replaced with “OT Cloud Service” for purposes of this OEM Annex in order to more clearly distinguish it from the Developer’s proprietary Cloud Service.

**ADDITIONAL DEFINITIONS.** The following terms have the following meanings:

- 1.1 “**API**” means the set of application programming interface functions made available by OT that allows access to and interaction with an OT Cloud Service. The API delivers sender’s information to an OT Cloud Service and sends the OT Cloud Service response back to the sender.
- 1.2 “**API Call**” means one request to an OT Cloud Service and the corresponding response. Each API Call is metered (and decremented against the balance of the API Calls purchased by you) unless it results in an error code or relates to a purely administrative function associated with an OT Cloud Service (such as user management), in which case it is not included within the definition of an ‘API Call’.
- 1.3 “**API Documentation**” means any API documentation, specifications or other API materials made available by OT for you to develop Developer Cloud Services that consume the OT Cloud Services.
- 1.4 “**API Key**” means the security key OT makes available for you to access an OT Cloud Service API.
- 1.5 “**Change of Control**” means: (i) the consummation of a reorganization, merger or consolidation, or sale or other disposition of substantially all of the assets of Developer; or (ii) the acquisition by any individual, entity or group of beneficial ownership of more than 50% of either (a) the then-outstanding shares of common stock of Developer, or (b) the combined voting power of the then-outstanding voting securities of Developer entitled to vote generally in the election of directors.
- 1.6 “**Developer Cloud Services**” mean Developer’s cloud offering that consume one or more APIs and that are made available to Subscribers as Software as a Service.
- 1.7 “**OCP**” means the Open Text Cloud Platform.
- 1.8 “**Organization**” means the organizational account from which Developer manages OT Cloud Services. Authorized Users will have access to an Organization within a Build and Test region/data center and an Organization within each production region/data center for which Developer has purchased an applicable OT Cloud Service, as indicated by the Developer’s address on the Order and specified in a purchase order accepted by OT.
- 1.9 “**Subscriber**” means an ultimate end customer of Developer that has the granted rights by Developer to use and/or access Developer Cloud Services solely for the Subscriber’s internal business use.
- 1.10 “**Subscription**” means the rights granted under an agreement that authorizes a Subscriber to access and use the Developer Cloud Services.
- 1.11 “**Territory**” means the territory set forth in the Order.
- 1.12 “**Trademarks**” has the meaning provided thereto in Section 4.3.

#### **2. LICENSE AND SERVICES.**

- 2.1 **License Grant.** Subject to and conditioned on your compliance with all terms and conditions set forth in the Agreement, OT hereby grants you a limited, revocable, non-exclusive, non-transferable, non-sublicensable right during the term of the Agreement to: (a) use the API Documentation solely for your internal business purposes in developing Developer Cloud Services that will communicate and interoperate with the OT Cloud Services; and (b) display certain OT Marks in compliance with usage guidelines that we may specify from time to time including those accessed at <https://www.5.1.2.i.com/who-we-are/copyright-information/trademark-logo-usage-policy> and <https://www.5.1.2.i.com/brandcentral/> solely in connection with the use of OT Cloud Services. You acknowledge that there are no implied licenses or rights granted under the Agreement. We reserve all rights that are not expressly granted. You may not use the API Documentation or any OT Mark or the Service for purpose not expressly granted without our prior written consent.
- 2.2 **Services.** For purposes of Section 5.1 of the GTC, use of the OT Cloud Services for ‘internal business purposes’

includes use of the OT Cloud Services by Developer in providing the Developer Cloud Services to Subscribers in compliance with all the terms and conditions of the Agreement. Such use shall not be considered a resale of OT Cloud Services for purposes of Section 5.2 of the GTC.

2.3 **Additional Restrictions.** Developer shall not change, sublicense, assign, sell, or transfer (electronically or otherwise), the API Documentation. Developer shall ensure that each Subscriber resides in the Territory. The Developer Cloud Services may not compete with the OT Cloud Services.

2.4 **Non-Exclusive.** OT can market and provide the OT Cloud Services and any of OT's other present or future services to developers and customers worldwide either directly or through any form of channel.

### 3. Build / Test / Commercialize

3.1 **Build & Test.** Subject to compliance with the terms and conditions of the Agreement, during the Term you have the right to access certain OT Cloud Service tenants or APIs to build and test Developer Cloud Services. Upon purchasing a Build and Test subscription, OT will upgrade your existing Trial subscription to a Developer Cloud Service, thus providing your Authorized User with access to the Organization, tenant(s) and APIs. The credentials for your Trial account will be used as the Authorized User for your Developer Cloud Service. It is the Developer's responsibility to notify OT of changes to the contact details for your designated administrator. Depending on the OT Cloud Service, the administrator may provision a number of additional Authorized User accounts. An email address will be the user ID for each Authorized User provisioned. Only one Authorized User may be associated with any single, unique email address. Developer agrees to keep such account provisioning information accurate, complete, and up to date.

(a) Your Developer Cloud Service enables access to an organizational account from which you can manage the Developer Cloud Services during the build and test phase of your application(s). The Developer Cloud Service will be provisioned within a designated Build and Test region/data center with the features and entitlements as indicated in the Schedule(s) attached to this document.

(b) During the Term, when your Developer Cloud Service has exhausted the bundled API Calls and data storage entitlement, you may submit a purchase order to OT to purchase additional API Calls and data storage capacity for the same Build and Test region/data center with the features and entitlements as indicated in the Schedule(s) attached to this document. OT may accept or reject a purchase order. If accepted, the API Calls and/or storage will be added to your OT Developer Organization within the Build and Test region/data center and the updated information will be reflected in the administration interface(s) available to Developer.

3.2 **Commercial Phase.** During the Term, when your application is ready for commercialization, you may submit a purchase order to OT to purchase API Calls and data storage capacity for a designated production region/data center with the features and entitlements as indicated in the Schedule(s) attached to this document. OT may accept or reject a purchase order. On receipt and approval of your first order for a production region/data center, OT will provision a production Organization within the production region/data center, which will provide access to the Organization, tenant(s) and APIs to your designated Authorized User. Purchased API Calls and/or storage will be added to your OT Developer production Organization and the updated information will be reflected in the administration interface(s) available to Developer.

(a) During the Term, you may submit a purchase order to OT to purchase additional API Calls and data storage capacity for your production region/data center. These will be assigned to your production Organization as outlined above.

(b) API Calls purchased by Developer within a given region/data center can be used with respect to any OT Cloud Service. Any inventory (remaining balance) of API Calls as of the termination of the OT Cloud Service expire without payment of any refund to Developer except as otherwise stated in the Agreement. Order details regarding API Calls and storage are summarized in the attached Service Schedule.

3.3 **Invoicing.** OT will invoice Developer for the OT Cloud Service described in the Order. OT will invoice Developer in arrears for applicable overage charges (if any). For Clarity, OT will issue the first invoice to Developer for the OT Cloud Services within thirty (30) days from the effective date of the Order.

3.4 **Renewal.** The initial subscription term begins on the effective date of the Order. After the initial subscription term, the OT Cloud Service will automatically renew annually unless a party terminates the Agreement by notifying the other party in writing no less than thirty (30) days prior to the expiration of the then-current term.

3.5 **Data Center Region.** The primary data zones for ordered OT Cloud Services will be determined by the OT USA and EU data center regions that correspond to Developer's address on the Order. OT may use a third-party cloud infrastructure provider to provide portions of the OT Cloud Services. Obligations related to security are held as shared obligations by OT and such third-party cloud infrastructure vendor, as applicable (for example, OT may provide copies of the third-party cloud infrastructure vendors security reports or certifications to Developer regarding the portion of the OT Cloud Service they provide). Access to such reports or other audit activities requested by Developer, or any data protection authorities having jurisdiction over Developer, may be limited in scope to that allowed by such third-party cloud infrastructure provider and may be subject to additional charges which will be the responsibility of Developer. If Developer intends to utilize a third-party auditor, OT or its third-party cloud infrastructure provider may object in writing to such auditor where such auditor is: (i) not reasonably qualified; or (ii) not independent; or (iii) a competitor of OT or such

third-party cloud infrastructure provider. Where Developer requires specific functionality, which requires any additional processing service offered by a third party cloud infrastructure provider (such as online language translations services), such additional services may be conditional on Developer's acceptance of the additional terms and restrictions of such third-party cloud infrastructure provider. OT shall make available such additional terms to Developer prior to the implementation of such functionality. A third-party cloud infrastructure provider shall be considered a sub-processor. Such third-party infrastructure provider may utilize sub-contractors provided that such use shall be subject to the limitations set forth in this Agreement.

- 3.6 **Data.** The OT Cloud Services are not intended to be used for (i) activities where the failure of the OT Cloud Services could lead to death, serious personal injury, or severe environmental or property damage, or (ii) materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State. Any use of the OT Cloud Services for such activities by Developer will be at Developer's own risk, and Developer will be solely liable for the results of any failure of the OT Cloud Services when used for such activities.

If Developer processes personal information of any individuals, including without limitation, information concerning the health of any individuals, Developer represents and warrants that it has obtained any required consent of such individuals under applicable law. Developer will take appropriate measures to limit its use of such information within the OT Cloud Services to the minimum extent necessary for Developer to carry out its authorized use of such information.

- 3.7 **Service Level Agreement.** OT shall endeavor to operate the OT Cloud Services in such a manner that they are available to Developer for a specific amount of time each month (expressed as a percent); seven days per week, 24 hours per day (the "**Target Service Availability**" or "**TSA**"). The TSA for OT Cloud Services is 99.9%. Developer may terminate the Order if OT fails to meet the TSA by ten percent or more (a) during three (3) consecutive months or (b) during at least five (5) months (consecutive or not) over a twelve (12) month period. Such termination will be deemed termination for Cause. In the event that the Developer terminates the Order under this clause, OT will refund the portion of the prepaid annual Test and Development subscription fees (if any) attributable to the remaining days in the Term, and the unused API Calls.

- 3.8 **Backup & Recovery.** The Content associated with OT Cloud Services is backed up by means of regularly scheduled replication between the primary and alternate data center facilities in the assigned data center region.

In the event OT declares a disaster event that impacts delivery of the OT Cloud Services from the primary data center facility OT will restore service from an alternate facility for that data center region. The target recovery time objective ("**RTO**") following an OT declared disaster is 72 hours and the target recovery point objective ("**RPO**") is 4 hours.

- 3.9 **Support and Maintenance.** Support for OT Cloud Services is described in the Cloud Support Program Handbook for Multitenant Services published on [www.5.1.2.i.com/agreements](https://support.5.1.2.i.com/agreements) ("Cloud Handbook").

Developer acknowledges that OT will from time to time during the term be required to temporarily reduce or interrupt access to the OT Cloud Services for the purpose of maintaining or Updating the Services, as provided in the Cloud Handbook ("Routine Maintenance"). OT publishes a Routine Maintenance Schedule (available via the Developer Service Portal (My Support) located at <https://support.5.1.2.i.com>) detailing the regular cadence of reserved maintenance windows, which are available for use upon advance notice from OT to Developer.

OT and Developer also may mutually agree to conduct maintenance or implement changes on the OT Cloud Services outside of the predefined Routine Maintenance windows (conduct "Scheduled Developer Maintenance"). OT may temporarily limit or suspend the availability of all or part of the OT Cloud Services if it is necessary to conduct emergency maintenance to action an urgent situation that could not have been prevented by OT using IT industry standard practices and preventive measures described in this Agreement for reasons of public safety, interoperability of services, data protection; or to perform work that is immediately necessary for operational, technical or security reasons

#### 4. MARKETING

- 4.1 **Intellectual Property.** All rights, title, and interest in and to OT trademarks related to the OT Cloud Services are retained by OT.
- 4.2 **Private Label.** Developer shall market and distribute Developer Cloud Services under its own name. Developer shall include copyright information where appropriate on OT Cloud Services user interfaces in the Developer Cloud Service.
- 4.3 **Trademarks.** Developer is authorized to use the OT trademarks, trade names or logos applicable to the OT Cloud Services (collectively, the "Trademarks"), but only for the purpose of promoting the Developer Cloud Service and only during the Term of the Agreement.
- 4.4 **Representations.** Developer shall make no representations or warranties concerning OT or the OT Cloud Services.
- 4.5 **Marketing.** Developer agrees to use its reasonable commercial efforts to promote, market and distribute Developer Cloud Services, and in particular, Developer agrees:
- (a) to demonstrate Developer Cloud Services at trade shows and marketing events where demonstration is considered by Developer appropriate;

- (b) to participate in a press release on its relationship with OT and this Agreement; and
- (c) that OT may publish Developer's name and the Developer Cloud Service name(s) for the purpose of publicizing Developer's relationship with OT.

**5. TERMINATION.** The following provisions supplement Section 8 of the GTCs

**5.1 Termination.**

The Agreement shall terminate automatically, without notice:

- (i) upon a Change of Control;
- (ii) upon the institution by or against either party of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of its debts and such proceeding is not dismissed within 60 days of its being filed;
- (iii) upon either party making an assignment for the benefit of creditors;
- (iv) upon either party's dissolution or liquidation; or
- (v) upon either party's attempt to assign the Agreement in contravention hereof.

**5.2 Consequences.** In the event of any termination or expiration of the Agreement, Developer will immediately discontinue access to and use of any OT Cloud Services, as well as any user interface connecting to any OT Cloud Service and return all API Documentation to OT, and the rights granted to each party under the Agreement shall revert to their respective owners, except that access by Developer to the OT Cloud Service for any Subscription entered into prior to the termination or expiration date shall continue in accordance with their terms for up to 12 months from the date of termination of the Agreement (so long as such terms, at the date entered into, are not otherwise inconsistent with the Agreement, but only so long as Developer complies with all terms and conditions of the Agreement) and provided further that obligations of Developer to pay fees with respect to use of the OT Cloud Service shall continue in accordance the Agreement.

**6. PROPRIETARY INFORMATION.** The following supplements Section 13 of the GTCs.

**6.1 Definition.** OT and Developer each acknowledge and agree that certain information which it may receive from the other party shall be proprietary to the disclosing party. Such information includes, without limitation:

- (a) the fact that the disclosing party intends to develop or market any particular cloud service offering;
- (b) the API Documentation;
- (c) any other information the disclosure of which might harm or destroy a competitive advantage of the disclosing party (all of items (a) through (c) shall be collectively referred to as the "Proprietary Information").

**6.2 Proprietary Information.** Each of the parties agrees that it shall not, directly or indirectly, either during or subsequent to the term of the Agreement:

- (a) disclose any Proprietary Information of the other party, other than to its own employees and consultants, and those of its Affiliates who participate directly in the performance of the receiving party's respective obligations under the Agreement;
- (b) copy or use any Proprietary Information of the other party except for the purpose of fulfilling its respective obligations hereunder; or
- (c) publish any Proprietary Information of the other party without the prior written consent of such party.

The degree of care employed by each of the parties to protect and safeguard the Proprietary Information of the other party shall be no less protective than the degree of care used by such party to protect its own confidential information of like importance. Each party agrees that all employees and consultants, and those of its Affiliates to whom Proprietary Information is disclosed will have signed a confidentiality agreement in the form customarily used by such party prior to receiving such disclosure, and which is at least as protective as the terms of this Article 6.

The obligations of each party with respect to each item of Confidential Information disclosed to it shall terminate three years after the date of disclosure of such item of Confidential Information, except in the case of the API Documentation or an API or any software, for which such obligations shall not terminate until the occurrence of any circumstance listed in Section 13 (i) through (v) of the GTC. After the obligations with respect to an item of Confidential Information end as provided in the previous sentence, use of that item of Confidential Information shall continue to be governed by applicable law, including, without limitation, trade secret, patent and copyright law.

**7. REPRESENTATIONS, WARRANTIES AND LIABILITIES.**

**7.1 OT's Representations.** OT represents and warrants for the benefit of Developer that:

- (a) OT possesses full power and authority to enter into the Agreement to fulfill its obligations thereunder, and to grant the access rights concerning the OT Cloud Services, free of any liens or encumbrances, herein granted to Developer; and,
- (b) the performance of OT's obligations hereunder shall not breach any separate agreement by which OT is bound;

**7.2 No Warranty Pass Through.** Developer shall not pass through to its Subscribers or any third party any warranties made by OT and will expressly indicate to its Subscribers that they must look solely to Developer in connection with any problems, warranty claims or other matters concerning a Developer Cloud Service that consumes an OT Cloud Service.

### 7.3 **Developer's Representations.**

- (a) Developer represents and warrants for the benefit of OT that:
  - (i) Developer possesses full power and authority to enter into the Agreement to fulfill its obligations thereunder, free of any liens or encumbrances;
  - (ii) the performance of the Agreement and of Developer's obligations hereunder shall not breach any separate agreement by which Developer is bound; and
  - (iii) so long as the Agreement remains in effect, Developer shall not make or enter into any agreement or arrangement with any third party which is inconsistent with any of the provisions of the Agreement.
- (b) Developer shall comply with all applicable federal, state, provincial, and local laws and regulations in connection with its performance relating to the Agreement. Developer shall not engage in any deceptive or unethical practices that may be detrimental to OT. Developer shall comply with the Foreign Corrupt Practices Act of the U.S., the Bribery Act of the U.K., and any applicable local laws or regulations (collectively, the "Anti-Corruption Laws") including their prohibitions regarding the direct or indirect payment or giving of anything of value to an official of a foreign government, political party or governmental or non-governmental agency for the purpose of influencing an act or decision in their official capacity or inducing the official to use their or their organization's influence to obtain or retain business involving Developer Cloud Services. Developer shall not violate or knowingly let anyone violate the Anti-Corruption Laws with respect to the sale, licensing and use of the Developer Cloud Services or OT Cloud Services or related services. Developer warrants that none of Developer's principals, staff, officers or key employees are government officials, candidates of political parties, or other persons who might assert illegal influence on its behalf. OT shall have the right to: (i) audit Developer's books and records at any time on ten days' notice to verify Developer's compliance with this Section; and (ii) immediately terminate the Agreement for cause if OT has reason to believe that Developer has violated its obligations under this Section. Developer shall indemnify and hold harmless OT against and from any claim, loss, damage or expense (including attorneys' fees and disbursements): (a) arising from any breach by Developer of any representation, warranty, covenant or other obligation of Developer under this Section; (b) resulting from any unlawful act committed by Developer or any agent of Developer thereof; or which OT may sustain by reason of any act, omission or misrepresentation of Developer or any agent thereof relating to this Section 7.3(d). Developer agrees to maintain an effective program to comply with the Anti- Corruption Laws during the Term. Developer agrees to certify or recertify compliance with this Section promptly upon request of OT.

- 7.4 **Indemnification.** Developer shall indemnify and hold OT harmless from and against any and all claims, losses, liabilities, costs, expenses or fines (including reasonable attorney's fees and expenses) which result from, arise in connection with, or are related in any way to: (i) Developer's failure to comply with the terms of the Agreement;(ii) Developer Cloud Services; or (iii) any wrongful conduct of Developer or its employees.

# Data Processing Addendum

## 1. Background; Definitions.

### 1.1 Background.

1.1.1 This Data Processing Addendum (this “DPA”, which includes the Appendices and incorporations by reference) forms part of the Agreement between OT and Developer under which OT shall carry out certain Services which include the Processing of Personal Data. Data Protection Legislation (defined below) applies to Developer’s use of the Services.

1.1.2 This DPA is in addition to, and does not relieve, remove, or replace either party’s obligations under the Data Protection Legislation.

1.1.3 If there is any conflict between the provisions of this DPA and the provisions of the Standard Contractual Clauses (defined below), the provisions of the Standard Contractual Clauses shall prevail to the extent of any such conflict. For the avoidance of doubt, where this DPA further specifies Sub-processor and audit rules in Sections 2.3 and 2.11, such specifications also apply in relation to, and satisfy Developer’s and its Subscribers’ rights under the respective provisions of the Standard Contractual Clauses.

1.1.4 The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them elsewhere in the Agreement.

1.1.5 The term “Customer” in Appendix 3 through 6 referred to in this DPA means “Developer”

### 1.2 Definitions.

1.2.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly.

A. “Affiliate” means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of management and the policies of an entity, whether through ownership of voting securities, by contract or otherwise.

B. “Data Protection Legislation” means, (i) the GDPR (and any laws of Member States of the European Economic Area (“EEA”) implementing or supplementing the GDPR), (ii) UK Data Protection Law and (iii) data protection or privacy laws of Switzerland, in each case, to extent applicable to the Processing of Personal Data under this DPA and the Agreement.

C. “EEA Standard Contractual Clauses” means the EEA Controller to Processor SCCs and EEA Processor to Processor SCCs.

D. “EEA Controller to Processor SCCs” means the clauses set out at <https://www.5.1.2.i.com/assets/documents/en-US/pdf/5.1.2.i-eea-controller-to-processor-clauses-module-2-en.pdf> (and also sometimes referred to as ‘Appendix 4’) which are incorporated into this DPA by reference, as may be amended, updated or replaced from time to time.

E. “EEA Processor to Processor SCCs” means the clauses set out at <https://www.5.1.2.i.com/assets/documents/en-US/pdf/5.1.2.i-eea-processor-to-processor-clauses-module-3-en.pdf> (and also sometimes referred to as “Appendix 5”) which are incorporated into this DPA by reference, as may be amended, updated or replaced from time to time.

F. “GDPR” means EU General Data Protection Regulation 2016/679.

G. “Restricted Transfer” means a transfer of Personal Data which, subject to the paragraph below, is:

(1) from an exporter subject to GDPR which is only permitted in accordance with GDPR if a Transfer Mechanism is applicable to that transfer (“EEA Restricted Transfer”); from an exporter subject to UK Data Protection Law which is only permitted in accordance with UK Data Protection Law if a Transfer Mechanism is applicable to that transfer (“UK Restricted Transfer”); and/or

(2) from an exporter subject to Data Protection Legislation applicable in Switzerland which is only permitted under that law if a Transfer Mechanism is applicable to that transfer (“Swiss Restricted Transfer”).

Transfers of Personal Data will not be considered a Restricted Transfer where:

(a) the jurisdiction to which the personal data is transferred has been approved by the European Commission under Article 45 of the GDPR or, as applicable, an equivalent provision under UK or Swiss Data Protection Law, as ensuring an adequate level of protection for the processing of Personal Data (an “Adequate Country”); or

(b) the transfer falls within the terms of a derogation as set out in Article 49 of the GDPR, equivalent under Swiss Data Protection Law or the UK GDPR (as applicable).

H. "Services" means the OT Cloud Services and other activities to be supplied to or carried out by or on behalf of OT pursuant to the Agreement.

I. "Standard Contractual Clauses" means each of the EEA Standard Contractual Clauses and the UK Standard Contractual Clauses.

J. "Sub-processor" means any third party (including any OT Affiliate) appointed by or on behalf of OT as a sub-contractor to Process Personal Data on behalf of Developer or Developer Affiliate in connection with the Agreement.

K. "Technical and Organisational Measures" means the technical and organizational measures set out at <https://www.5.1.2.i.com/assets/documents/en-US/pdf/5.1.2.i-technical-and-organizational-measures-en.pdf> (and also referred to as Appendix 3) which are incorporated into this DPA by reference, as may be amended, updated or replaced from time to time.

L. "Transfer Mechanism" means the Standard Contractual Clauses or any other appropriate safeguards under article 46 of the GDPR or equivalent under Swiss or UK Data Protection Law applicable to a relevant transfer of Personal Data that has the effect of permitting that transfer.

M. "UK Data Protection Law" means UK GDPR (as defined in the UK Data Protection Act 2018) and the UK Data Protection Act 2018.

N. "UK Controller to Processor SCCs" means the UK International Data Transfer Addendum which is made up of the provisions set out at <https://www.5.1.2.i.com/assets/documents/en-US/pdf/5.1.2.i-uk-international-data-transfer-addendum-en.pdf> (and also referred to sometimes as Appendix 6) which are incorporated into this DPA by reference, as may be amended, updated or replaced from time to time, incorporating the EEA Controller to Processor SCCs.

O. "UK Processor to Processor SCCs" means the UK International Data Transfer Addendum which is made up of the provisions set out at <https://www.5.1.2.i.com/assets/documents/en-US/pdf/5.1.2.i-uk-international-data-transfer-addendum-en.pdf> (and also referred to sometimes as Appendix 6) which are incorporated into this DPA by reference, as may be amended, updated or replaced from time to time, incorporating the EEA Processor to Processor SCCs.

P. "UK Standard Contractual Clauses" means the UK Controller to Processor SCCs and UK Processor to Processor SCCs.

1.2.2 The terms "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processing", and "Processor"; shall have the same meaning as in the applicable Data Protection Legislation. The terms "Member State", "Supervisory Authority" and "Union" shall have the same meaning as in the GDPR. The terms "data exporter" and "data importer" have the meaning set out in the applicable Standard Contractual Clauses. "including" shall mean including without limitation.

## **2. Data Processing Obligations.**

### **2.1 Controller and Processor of Personal Data, Appointment of Processor and Purpose of Processing.**

2.1.1 OT will comply with all applicable requirements of the Data Protection Legislation to the extent it imposes obligations upon OT as a Data Processor and expects Developer to also comply with Data Protection Legislation.

2.1.2 This DPA applies to the extent Developer is the Controller and OT is the Processor. It also applies to the extent that Developer is a Processor and OT is acting as a (sub) Processor. Where the Developer is a Processor, the Developer confirms that its instructions, including appointment of OT as a Processor or (sub) Processor, have been authorized by the relevant Controller.

2.1.3 Appendix 1 of this DPA sets out the scope, nature and purpose of Processing by OT, the duration of the Processing and the types of Personal Data and categories of Data Subjects.

### **2.2 OT's obligations with respect to the Developer.**

2.2.1 OT will, in relation to any Personal Data it will be Processing under the Agreement and this DPA:

- A. process such Personal Data solely for the purpose of providing the Services;
- B. process such Personal Data in accordance with documented and commercially reasonable instructions from the Developer, subject to and in accordance with the terms of the Agreement;
- C. ensure that the persons authorized by it to process such Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have received appropriate training on their responsibilities; and
- D. limit access of OT personnel to the Personal Data undergoing processing to what is necessary for provision of the Services.

2.2.2 Developer agrees that the Agreement (including this DPA) are its complete documented instructions to OT for

the Processing of Personal Data. Additional instructions, if any, require prior written agreement between the Parties. Where in the opinion of OT an instruction from the Developer infringes Data Protection Legislation, it shall inform the Developer thereof (but such communication shall not constitute legal advice by OT). However, such obligation shall not relieve the Developer from its own responsibility for compliance with Data Protection Legislation.

2.2.3 Where OT is required under applicable law to process Personal Data other than on documented instructions from the Developer, including with regard to transfers of Personal Data to a third country or an international organization, OT shall use its reasonable endeavors to inform the Developer of that legal requirement before Processing, unless such information is prohibited by law on important grounds of public interest.

## 2.3 Sub-processing.

2.3.1 Developer provides OT a general authorization to engage Sub-processors. Sub-processors may include: (i) OT's global Affiliate companies as exist from time to time (and their vendors); and/or (ii) any of the sub-contractors that OT engages in connection with the provision of certain Processing activities as at the date of this Agreement. The Parties agree that the sub-processors listed at (i) and (ii) is the 'agreed list' for sub-processors in relation to Clause 9(a) of the EEA Standard Contractual Clauses and for the UK Standard Contractual Clauses.

2.3.2 OT shall Inform the Developer at least 14 days before OT appoints a new or replacement Sub-processor to give the Developer opportunity to reasonably object to the changes. OT must receive the notice of objection in writing from the Developer within 14 days of OT informing it of the proposed changes. The Parties agree that the name of the new or replacement Sub-processor together with details of the processing activities it will carry out and the location of such activities is the information the Developer requires to exercise such right. "Inform" shall include by posting the update on a website (and providing Developer with a mechanism to obtain notice of that update), by email or in other written form. The parties confirm that this mechanism is not required where the new or replacement Sub-processor is an OT global Affiliate company.

2.3.3 The Parties agree that the Developer's right to be object shall be as set out in this Section 2.3.3 and Section 2.3.4. Any objection raised by the Developer pursuant to Section 2.3.2 must be where the Sub-processor demonstrably fails to offer the same or a reasonably comparable level of protection as that previously applicable to the relevant Processing of Personal Data.

2.3.4 If Developer has a reasonable and legitimate reason to object to the new Sub-processor pursuant to Section 2.3.3, and OT is not able to provide an alternative Sub-processor, or the Parties are not otherwise able in good faith to achieve an alternative resolution, Developer may terminate the respective part of the Services where the new Sub-processor is to be used by giving written notice to OT no later than 30 days from the date that OT receives the Developer's notice of objection and such termination shall take effect no later than 90 days following OT's receipt of Developer's notice of termination. If Developer does not terminate within this 30-day period, Developer is deemed to have accepted the new Sub-processor. Any termination under this Section 2.3.4 shall be deemed to be without fault by either Party and shall be subject to the terms of the Agreement (including any documents agreed pursuant to it).

2.3.5 OT confirms that it has entered or (as the case may be) will enter into a written agreement with its third-party company Sub-processors incorporating terms which are substantially similar to those set out in this DPA.

2.3.6 As between the Developer and OT, OT shall remain fully liable for all acts or omissions of any Sub-processor appointed by it pursuant to this Section 2.3 (unless the Sub-processor acted in accordance with instructions directly or indirectly received from Developer).

2.4 Data Subjects' Right to Information. It is the Developer's (or the party acting as Controller) responsibility to inform the Data Subject(s) concerned of the purposes and the legal basis for which their Personal Data will be processed at the time the Personal Data is collected.

## 2.5 Exercise of Data Subjects' Rights.

2.5.1 Taking into account the nature of the Processing, OT shall assist the Developer insofar as this is possible and reasonable for the fulfilment of the Developer's obligation under Data Protection Legislation to respond to requests for exercising the Data Subject's rights of: access, rectification, erasure and objection, restriction of processing, data portability, not to be subject to a decision based solely on automated processing.

2.5.2 Where the Data Subjects submit requests to OT to exercise their rights, OT shall forward these requests by email to a Developer email address on file with OT. If Developer wishes for OT to forward Data Subject requests to a specific email address, it shall notify OT of such address. OT shall not respond to a Data Subject request unless and to the extent instructed by Developer to do so.

## 2.6 Notification of Personal Data Breach.

2.6.1 OT shall notify the Developer of a Personal Data Breach without undue delay after OT becoming aware of it by email to a Developer email address on file with OT, along with any necessary documentation to enable the Developer, where necessary, to notify this breach to the Data Subject and / or the competent Supervisory Authority.

2.6.2 If available and taking into account the nature of the Processing, the notification in accordance with Section 2.6.2 shall at least:

A. 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;

B. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

C. describe the likely consequences of the Personal Data Breach; and

D. describe the measures taken or proposed to be taken by OT to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

2.6.3 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

2.6.4 The Developer (or the party acting as Controller) is responsible to notify the Personal Data Breach to the Supervisory Authority, and to the Data Subjects, when this is required by the applicable Data Protection Legislation.

## 2.7 Assistance lent by OT to the Developer regarding Compliance with Developer's Obligations under the Data Protection Legislation.

2.7.1 Where requested by the Developer and to the extent required by Data Protection Legislation, OT shall, taking into account the nature of processing and the information available to OT, provide reasonable assistance to the Developer:

A. in carrying out data protection impact assessments; or

B. should the Developer need prior consultation with a Supervisory Authority.

## 2.8 Security Measures.

2.8.1 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, the Developer and OT shall both be responsible to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

2.8.2 OT agrees to implement the Technical and Organizational Measures in respect of the Services.

2.8.3 Developer shall procure implementation and maintenance of privacy protections and security measures for the Developer Cloud Service (including the OT Cloud Service) that Developer provides or controls. Developer shall apply the principle of data minimization and limit OT access to Developer systems or Personal Data to only where essential for the performance of the OT Cloud Services (and procure the same from Subscribers). Developer shall not store any Personal Data in a non-production environment unless it has production environment equivalent controls in place (and procure the same from Subscribers).

2.9 Data Return or Destruction. Where OT has stored Personal Data as part of the Services: at the end of the Service(s) upon Developer's written instruction, OT may (i) offer a data return service or (ii) following a reasonable data retention period delete the Personal Data unless applicable law requires further storage of the Personal Data. OT may charge a fee for any data return services.

2.10 The Data Protection Officer. OT has designated a data protection officer in accordance with Data Protection Legislation. They can be contacted by email via [5.1.2.1@5.1.2.1.com](mailto:5.1.2.1@5.1.2.1.com).

## 2.11 Inspections and Audits.

2.11.1 The right of audit, including inspections, which the Developer may have under Data Protection Legislation and under the Standard Contractual Clauses, are as set out in this Section 2.11.

2.11.2 Upon written request from Developer OT shall, where available, provide a copy of the latest Service Organization Control (SOC) audit report and/or other third-party audit reports or information to demonstrate the processing activities of OT relating to the Personal Data is in compliance with its obligations under this DPA.

2.11.3 Developer may request evidence of OT's relevant policies and other related documents to verify that OT is complying with its obligations under this DPA.

2.11.4 Developer may conduct an on-site inspection at OT's premise either by itself or by an independent third-party auditor (not to include a competitor of OT) where the information under Sections 2.11.2 and 2.11.3 has failed to verify compliance by OT of its obligations under this DPA or such an inspection is formally required by the Supervisory Authority.

2.11.5 General Procedure: The following Sections 2.11.6, 2.11.7 and 2.11.8 shall apply to each of Sections 2.11.2, 2.11.3 and 2.11.4.

2.11.6 Unless otherwise mandated by a Supervisory Authority, Developer shall: (a) give OT at least 30 days' prior written notice of its intention to conduct an audit, including inspection, under this Section 2.11; and (b) agree with

OT the frequency and duration of these, which shall not extend beyond two consecutive business days nor be more than once per contract year.

2.11.7 Any audit, including inspections, must be conducted during local business hours, not unreasonably disrupt OT business operations and not burden the provision of services by OT to its Developers. Developer shall limit these to remote audits or meetings with senior representatives of OT as far as possible and will avoid or minimize the need for an audit (including inspection), without limitation by using current certifications, other audit reports or combining them with others under the Agreement. Additionally, these rights are subject to limitations set out in the Agreement. Any audit, including inspections, shall be subject to OT's relevant policies and procedures.

2.11.8 Conditions of confidentiality and the scope of an audit, including inspection, shall be agreed in advance between OT and Developer. Developer shall provide OT the results of any audit, including inspection. Developer bears all expenses related to inspections and audits.

## **2.12 Developer Information and related Restrictions.**

2.12.1 Instructions by Developer related to the Processing of Personal Data must be provided in writing duly signed by an authorized representative of Developer.

2.12.2 Developer is responsible to have all necessary consents and notices in place and confirms it is entitled to lawfully transfer the Personal Data to OT.

## **3. International Transfers.**

3.1 Personal Data may be processed in the EEA, the United Kingdom and Switzerland (each a "Designated Country") and in countries outside of a Designated Country ("Other Countries") by OT or its Sub-processors. The transfer to Other Countries shall be in accordance with Data Protection Legislation (to the extent it applies).

3.2 The Parties shall have in place a Transfer Mechanism in respect of any Restricted Transfer:

3.2.1 In the event of an EEA Restricted Transfer where Personal Data is transferred from Developer as data exporter acting as a Controller or Processor (as applicable), to OT as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the EEA Controller to Processor SCCs where the Developer acts as a Controller and the EEA Processor to Processor SCCs where the Developer acts as a Processor.

3.2.2 In the event of a UK Restricted Transfer, where Personal Data is transferred from Developer as data exporter acting as a Controller or Processor (as applicable) to OT as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the UK Controller to Processor SCCs where the Developer acts as a Controller and the UK Processor to Processor SCCs where the Developer acts as a Processor.

3.2.3 In the event of a Swiss Restricted Transfer, whereby Personal Data is transferred from Developer as data exporter, acting as a Controller or Processor (as applicable), to 5.1.2.1 as data importer acting as a Processor, the Parties shall, as part of this DPA, comply with the corresponding module of the EEA Standard Contractual Clauses.

3.2.4 The Standard Contractual Clauses will not apply to a Restricted Transfer to the extent that OT has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Restricted Transfers.

3.3 Where pursuant to the Standard Contractual Clauses OT attempts to redirect a request from a public authority, including judicial authorities ("Government Request") to the Developer, and/or determines that a requirement to challenge or appeal a Government Request regarding Developer's Personal Data exists, Developer agrees to participate in and support such challenge as reasonably requested. Where possible, the Developer itself will seek a protective order or other appropriate remedy in response to the Government Request.

## **4. General Provisions.**

4.1 The Parties agree that with respect to the period on and after the date that this DPA comes into effect between the Parties (or if earlier, the mandatory date when the relevant Standard Contractual Clauses must apply), this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that Developer and OT may have previously entered into in connection with the Services.

## **APPENDIX 1**

### **DETAILS OF PROCESSING OF DEVELOPER PERSONAL DATA**

See Appendix 2 of this DPA for each of following: *Subject matter and duration of the Processing of Personal Data, the nature and purpose of the Processing of Personal Data, the types of Personal Data to be processed, special categories of data (if appropriate) and the categories of Data Subject to whom the Developer Personal Data relates.*

## APPENDIX 2 DESCRIPTION OF TRANSFER

### Categories of data subjects whose personal data is transferred

Data Subjects may include employees, contractors, business partners or other individuals having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by OT.

### Categories of personal data transferred

Developer determines the categories of Personal Data which are processed by OT in connection with the Services in accordance with the terms of the Agreement (and documentation governed by it). Developer submits Personal Data for processing after careful evaluation of compliance with applicable laws. The Personal Data may include the following categories of data: name, phone numbers, e-mail address, time zone, address data, company name, plus any application-specific data.

**Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

None.

The choice and type of Personal Data that will be processed using the OT Services remains solely within the discretion and choice of the Developer. In selecting the Personal Data of any categories, the Developer shall ensure that such Personal Data is suitable for processing with and through the Services in compliance with applicable data protection laws. OT disclaims all liabilities in relation to the selection of data for use with the Services.

**The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).**

Transfers shall be made on a continuous basis.

### Nature of the processing

OT offers its Services, and in doing so, OT requires to process Personal Data.

The Personal Data is subject to the basic processing activities as set out in the Agreement which may include:

- (a) use of Personal Data to provide the Services;
- (b) storage of Personal Data;
- (c) computer processing of Personal Data for data transmission; and
- (d) other processing activities to deliver the Services.

### Purpose(s) of the data transfer and further processing

See "nature of processing" above.

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

The duration of the Processing of the Personal Data is set out in the Agreement (and documentation governed by it) and this DPA.

### Subject matter, nature and duration of the processing for transfer to (sub-) processors

As above.

**NOTE.** Personal Data shall also include that of Subscribers (as defined in the Annex).

For purposes of Appendix 3 (see Section 1.2.1 (K) of the Data Processing Addendum), "Developer systems" refers to those of the Developer. Notwithstanding the foregoing, this shall not release the Developer of its obligations, in the Agreement or otherwise, and Developer shall remain responsible for the decisions, acts and omissions of Subscribers, and shall procure that Subscribers comply with the above Data Processing Addendum provisions.

## Service Schedule

| OT Cloud Service               | OT Cloud Services                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                    | 5.1.2.e [Redacted]<br>[Redacted]<br>[Redacted]                                                                                                                                                                                                                                                                                                                                                                                 |
| Use Case(s)                    | 5.1.2.e [Redacted]<br>[Redacted]<br>[Redacted].                                                                                                                                                                                                                                                                                                                                                                                |
| Available SKU's / Product Name | 5.1.2.e [Redacted]<br>[Redacted] [Redacted]<br>[Redacted]<br>[Redacted] [Redacted]<br>[Redacted] [Redacted]<br>[Redacted] [Redacted]                                                                                                                                                                                                                                                                                           |
| Available Data Center Regions* | 5.1.2.e [Redacted]<br>[Redacted]                                                                                                                                                                                                                                                                                                                                                                                               |
| Unit of Measure                | 5.1.2.e [Redacted]<br>[Redacted]<br><br>5.1.2.e [Redacted]<br>[Redacted]<br><br>5.1.2.e [Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted]<br><br>5.1.2.e [Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted]<br><br>5.1.2.e [Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted]<br><br>5.1.2.e [Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted]<br>[Redacted] |
| Overage Items                  | 5.1.2.e [Redacted]<br>[Redacted]                                                                                                                                                                                                                                                                                                                                                                                               |

|                                 |                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | 5.1.2.e [REDACTED]                                                                                                                                    |
| Client Side Software Components | 5.1.2.e [REDACTED]                                                                                                                                    |
| Application specific Terms      | <div>5.1.2.e [REDACTED]</div> <div>5.1.2.e [REDACTED]</div> <div>5.1.2.e [REDACTED]</div> <div>5.1.2.e [REDACTED]</div> <div>5.1.2.e [REDACTED]</div> |

\*OT may add data center locations from time to time and will provision based on the then current list.

## 5.1.2.1 Private Cloud Platform Addendum

This Addendum ("Addendum") shall amend the \_\_\_\_\_ Agreement executed on or near \_\_\_\_\_, by and between \_\_\_\_\_ ("\_\_\_\_\_") and 5.1.2.1 Inc. or its Affiliates, ("5.1.2.1" ("Agreement"). This Amendment shall be effective as of the date last signed below.

### 1. Overview

Subject to Customer's compliance with the terms of this Addendum and the Agreement, 5.1.2.1 will install and operate an on-site 5.1.2.1 Private Cloud Platform which shall consist of computing hardware such as storage, network, and server components ("Hardware"), Software (defined below) and the Cloud Services provided by 5.1.2.1 as described in this Amendment (collectively the "Platform") at Customer's designated business location(s) (the "Facility"). The Platform is designed to enable the Customer to process Customer Data on the Platform and deliver Customer Data and/or Reports through the Platform. Functionality of the Cloud Services provided through the Platform will depend, in part, on Customer's compliance with the provisions and specifications set forth herein including those set forth in the then-current 5.1.2.1 Private Cloud Platform Deployment Guide (referred herein as the "Implementation Guide").

### 2. 5.1.2.1 Private Cloud Platform

#### 2.1 Implementation

5.1.2.1 and Customer will agree upon a schedule and responsibilities for implementation of the Platform at the Facility including an expected date of implementation ("Implementation Date"). -Each party must complete its obligations in accordance with the agreed-upon schedule (see attached). -Any delay caused by Customer shall excuse 5.1.2.1 performance until Customer has completed its responsibilities. 5.1.2.1 may invoice Customer for the applicable fees on the earlier of (a) the date on which Customer may access the Cloud Services through the Platform ("Access Date") or (b) the agreed-upon implementation start date if -Customer's access to the Cloud Services via the Platform is delayed due to Customer's failure to meet the schedule. In the event that no agreed-upon schedule is attached, 5.1.2.1 will have the right to invoice 45 days after delivery of the platform. If the implementation service is delayed for more than 60 days due to Customer's failure to meet the schedule, 5.1.2.1 will deem the service effective date to be the agreed-upon implementation start date or the 60th day after delivery of the platform if no agreed-upon schedule is attached.

#### 2.2 Software

5.1.2.1 will deliver and install the software used to operate the Cloud Services (the "Software") within the Platform. 5.1.2.1 will update the Software in the Platform for the duration of the subscription as described herein.

#### 2.3 Platform components

During the term of the subscription, 5.1.2.1 agrees to upgrade, replace, or add additional components of Hardware, as necessary, to support delivery of the Cloud Services and meet the level of the Cloud Services level as detailed in the Cloud Services Level Agreement through the Platform

#### 2.4 Data Processing

As long as Customer maintains the Facility as set forth herein, 5.1.2.1 will provide the Cloud Services via the Platform in accordance with the Performance Levels set forth in Schedule 1, attached hereto. -In no event shall 5.1.2.1 transfer any Customer Data (other than application, system and monitoring logs / alerts) from the Platform to 5.1.2.1 location.

### 3. Specific Customer Responsibilities

#### 3.1 Facility

Customer will maintain the Facility in which the Platform will be located in accordance with acceptable industry standards and practices including but not limited to providing adequate utilities, furnishings, environmental conditions, physical security, and data connections as needed for the Platform to deliver the Cloud Services. Customer will be responsible for any loss or damage to the Platform caused by Customer's failure to follow acceptable industry standards and practices. Customer will also supply all equipment or hardware at the Facility that is (a) unrelated to the operation of the Cloud Services (such as an external firewall); or (b) required to deliver the Cloud Services provided via the Platform (such as IP network connectivity and valid digital certificates) other than any such equipment, hardware and elements 5.1.2.i is to deliver pursuant to Section 1. 5.1.2.i will not be liable for any failure to provide the Cloud Services, any degradation in Cloud Services, or any compromise in the security of the Platform or the Customer Data to the extent attributable to Customer's failure to maintain the Facility in accordance with acceptable security industry standards and practices.

#### 3.2 Remote Access by 5.1.2.i

Customer will provide 5.1.2.i IP connectivity to facilitate remote access to the Platform by a virtual private network ("VPN") through which 5.1.2.i may configure and maintain the Platform and the Software. 5.1.2.i will provide the VPN software and/or appliances (as further described in the Implementation Guide) to enable VPN connectivity. Customer acknowledges that remote access to the Platform is essential to enable 5.1.2.i to provide the Cloud Services. 5.1.2.i will not be liable for any failure to provide the Cloud Services or any degradation in Cloud Services quality caused by Customer's failure to provide access in accordance with this Section 3.2.

#### 3.3 Access by Customer

Customer may access the Platform for the purpose of rebooting or restarting the Platform, in consultation with 5.1.2.i as necessary to permit continued operability of the Cloud Services. Customer may shut down the Platform if, in Customer's reasonable determination, continued operation of the Cloud Services via the Platform jeopardizes the Facility or Customer's network. From time-to-time, 5.1.2.i may direct Customer to access the Platform for the limited purposes of performing upgrades, maintenance or to conduct diagnostic tests of the Platform or its components. In doing so, Customer hereby agrees to implement 5.1.2.i-directed upgrades, maintenance or diagnostic tests to the Platform only according to the reasonable instructions provided by 5.1.2.i. Customer may not access the Platform for any other purpose (including, without limitation, for the purpose of changing the configuration of the Platform, Platform components, or to access the Software). Customer will be responsible for any loss or damage caused by Customer's unauthorized access, or attempt to gain unauthorized access, to the Platform or the Software.

#### 3.4 Customer Support

In furtherance of Customer obligations hereunder, Customer will provide 5.1.2.i access to its support organization as set forth in Schedule 1, attached hereto.

### 4. Removal of Platform

Upon any termination of this Agreement, Customer and 5.1.2.i will use their good faith reasonable efforts to establish a mutually acceptable process to ensure that all elements of the Platform (excluding Customer Data) are securely removed from the Facility and returned to 5.1.2.i.

## SCHEDULE 1: 5.1.2.1 PRIVATE CLOUD PLATFORM PERFORMANCE LEVELS

### 1. Implementation Schedule

5.1.2.1 and Customer will agree upon a schedule for implementation of the Platform at the Facility over a specified period as described in the Cloud Services Order for the Cloud Services.

### 2. Software Update Schedule

5.1.2.1 will update the Software with packages designated by 5.1.2.1 for use with the Platform, according to the following schedule:

2.1 Vulnerability Signatures – updated within 24 hours after signatures are released for general availability

2.2 Scan Engine – updated within 2 weeks after released for general availability

2.3 5.1.2.1 User Interface – updated within 90 days after general availability subject to customer acceptance and availability of adequate downtime.

### 3. Remote Support

During the term of any subscription under this Agreement, 5.1.2.1 will provide Customer, via the Designated Contact, with remote support and assistance as follows:

3.1 5.1.2.1 shall maintain an email address and telephone number for receiving support requests from Customer.

3.2 5.1.2.1 shall keep the electronic mail and telephone help support open to Customer on a twenty-four (24) hour basis.

3.3 5.1.2.1 shall use commercially reasonable efforts to meet the response times described according to the categories of support incidents described below:

| Incident | Status   | Condition                                                                                                                                                                                                                        | Initial Contact     | Status update       | Management Escalation |
|----------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|---------------------|-----------------------|
| P1       | Critical | Network outage or other Error preventing Customer from accessing the 5.1.2.1 Cloud Services and/or obtaining the Customer Data or Reports                                                                                        | < two (2) hours     | Every two (2) hours | immediate             |
| P2       | High     | Customer can access the 5.1.2.1 Cloud Services and obtain Customer Data or Reports, but an Error renders one or more significant features of the 5.1.2.1 Cloud Services unavailable, such as the ability to launch a scan or map | < twelve (12) hours | twelve (12) hours   | twelve (12) hours     |

|    |     |                                                                                                                                                                |                          |                              |                              |
|----|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------|------------------------------|
| P3 | Low | Other Error that does not prevent Customer from accessing a significant feature of the<br><br>5.1.2.1 Cloud Services (e.g., a false positive or false negative | < forty-eight (48) hours | Every four (4) business days | After five (5) business days |
|----|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------|------------------------------|

Initial response is defined to be the first contact by a Support Engineer after the incident has been logged and a ticket generated. A status update will be communicated to the Customer if the incident cannot be resolved immediately. A final follow-up with the Customer occurs on the resolution date. The ticket will be processed according to Section 3.4 below. Customer acknowledges that not all P3 problems will require a workaround. 5.1.2.1 may, in its reasonable discretion, respond to a P3 problem by making the Error a feature request.

- 3.4 5.1.2.1 shall process inquiries using a ticketing procedure so that each query shall receive a ticket number enabling the status of the inquiry to be tracked until such time as the problem is closed. The support ticket will be closed once the problem has been resolved, or if, following receipt of an inquiry, 5.1.2.1 is unable to (i) successfully establish direct communication with Designated Contact following three (3) attempts by telephone or email or (ii) receive adequate and timely information and assistance from Designated Contact.

#### 4. On-Site Support

If 5.1.2.1 determines in its reasonable discretion that it cannot promptly resolve a P1 support incident remotely, 5.1.2.1 will provide on-site support and assistance as follows:

- 4.1 5.1.2.1 shall use commercially reasonable efforts to deploy a Cloud Services technician on site within 5 business days (or longer if travel limitations apply) of 5.1.2.1 and Customer's determination that on-site support is required.
- 4.2 If 5.1.2.1 and Customer determine in its reasonable discretion that resolution of a support incident requires replacement of Platform equipment, 5.1.2.1 will use commercially reasonable efforts to ship a replacement of such Platform equipment within 5 business days of 5.1.2.1 determination that such replacement is required.
- 4.3 5.1.2.1 on-site support obligations are subject to Customer providing physical access to the Platform and the Facility and cooperating as reasonably requested by 5.1.2.1 to facilitate 5.1.2.1 provision of support.

**Met opmerkingen [KR1]:** Is 5 werkdagen voor de politie acceptabel voor P1 incidenten? Wellicht dat daar nog over onderhandeld kan worden.

#### 5. Compatibility

The Cloud Services will maintain compatibility with the common Internet browser software including Microsoft Internet Explorer, Google Chrome and Firefox.

#### 6. Platform Fault Tolerance

5.1.2.1 shall maintain the Platform with physical hardware redundancy and fault tolerance according to 5.1.2.1 design and build procedure and chosen architecture by the customer, including, but not limited to redundant power distribution; computing, networking, and storage systems; which are configured with RAID or similar technology. Based on the considerations mentioned earlier the platform is logically configured in a manner designed for fault tolerance and provisioned to make use of the physical hardware

redundancy. Customer acknowledges and agrees that when customer choses an architecture without in-build redundancy, the platform may not contain all of the above features.

## 7. Disaster Recovery

5.1.2.1 agrees to use commercially reasonable efforts to assist Customer with necessary retention and recovery of the Customer Data on the Platform should the need arise. Customer acknowledges and agrees that only when Customer opts for a resilient architecture, 5.1.2.1 will maintain one backup copy of Database locally on the platform which can allow for recovery in the event of minor system failure. 5.1.2.1 will not maintain any additional copies of Customer Data at any location. 5.1.2.1 shall use commercially reasonable efforts to assist Customer in incorporating the Customer Data stored on the Platform into Customer's owned data backup, retention, archiving, and recovery process or systems.

## 8. Security

### 8.1 Application Traffic

Application traffic consists of Web User Interface traffic, API traffic, agent and Scanner Appliance traffic. -All traffic leverages secure HTTPS connections on port 443 inbound only to the Platform. The Platform will not communicate outbound to the Customer network for application traffic.

### 8.2 Subscription Security

Data security controls are designed to mitigate risks to the confidentiality of customer subscription and Customer Data inside the Platform. Customer subscription data is secured via data encryption methods. -Further, administrative and access controls (separation of duties) are enforced so that no single 5.1.2.1 employee will have access to both encryption keys and customer subscription data.

### 8.3 Encryption of Data at Rest

With customer chosen architecture for specific encryption needs 5.1.2.1 shall use industry standard solution for Data at Rest Encryption on platform and solution. With this, 5.1.2.1 provides built in Key Management Services on platform, which utilizes 5.1.2.1 data encryption and key management libraries to achieve Encryption on platform.

## 9. Cloud Services Credits

Within seven (7) days of receipt of a notice from Customer regarding 5.1.2.1 failure to satisfy a performance level, 5.1.2.1 as its sole obligation and liability, will (a) perform a root-cause analysis to identify the cause of such failure; (b) attempt to correct such failure; and (c) if the root-cause analysis demonstrates that such failure was due to the fault of 5.1.2.1 provide Customer with a Cloud Services credit ("Cloud Services Credit") consisting of a one-week extension of any Cloud Services subscription impacted by the applicable performance standard. Cloud Services Credits may be cumulated in the event of multiple failures of Performance Levels.

Met opmerkingen [KR2]: Dit dient de politie zich te realiseren.

**Van:** 5.1.2.e  
**Aan:** 5.1.2.e 5.1.2.e 5.1.2.e  
**Cc:** 5.1.2.e  
**Onderwerp:** Wel of geen verwerkersovereenkomst  
**Bijlagen:** [Leidraad verwerkersovereenkomst \(12 juni 2019 versie 1.4\).docx](#)  
[image001.png](#)

---

Beste 5.1.2.

Via een om weg kom ik weer terug bij jou uit.

Graag zouden wij (collega's van de sector Dienstverlening partners) met jou in gesprek gaan over het wel of niet opstellen van een verwerkersovereenkomst, aangezien jij één van de auteurs bent van het meegestuurde document.

Er is momenteel onduidelijkheid of wij als politie wel of niet als verwerkingsverantwoordelijke of verwerker optreden iert het opvoeren van persoonsgegevens van de medewerkers van ketenpartners in 5.1.2.i ten behoeve van een politie-account om zo toegang te krijgen tot politiesystemen.

Bovenstaande in relatie tot de verwerkingsverantwoordelijkheid vanuit de Wpg en verantwoordelijkheid voor o.a. passende autorisatie en logging. Een medewerker van een ketenpartner voert verwerkingen uit onder verantwoordelijkheid van de korpschef en/of onder verantwoordelijkheid van de eigen verwerkingsverantwoordelijke en de eventuele gevolgen daarvan voor het opvoeren van persoonsgegevens 5.1.2.i.

Een andere mogelijkheid is de leverancier van 5.1.2.i de verwerkingsverantwoordelijke is....

Alvast bedankt voor je reactie.

Met vriendelijke groet,

5.1.2.e

Privacy adviseur

Lid Ondernemingsraad Bedrijfsvoering

06 – 5.1.2.e

5.1.2.e @politie.nl <mailto:5.1.2.e@politie.nl>

5.1.2.i @politie.nl <mailto:5.1.2.i@politie.nl>

5.1.2.i @politie.nl <mailto:5.1.2.i@politie.nl>

Werkdagen: ma, di, wo, do en vr-ochtend

Politie | PDC | Dienst IV | IV Dienstverlening Partners

Zeisterweg 1b, 3984 NH Odijk

Postbus 238, 3970 AE Driebergen

Meer informatie? Kijk op politie.nl <<https://www.politie.nl/>>

---

Niet onder reikwijdte

Niet onder reikwijdte



**Van:** 5.1.2.e  
**Aan:** 5.1.2.e 5.1.2.  
**Onderwerp:** FW: Monitoringstool meldkamerwerkplekken  
**Datum:** vrijdag 24 april 2020 15:20:33  
**Bijlagen:** [Functionele uitvraag onder EASP2019 monitoringstool meldkamerwerkplekken \(1\).pdf](#)  
[Bijlage 3 - Concept Nadere overeenkomst \(3\).pdf](#)  
[Bijlage 1 - Format Prijsuitvraag.xlsx](#)

Fyi

Het gaat volgens 5.1.2.e om andere functionaliteit?

Fijn weekend,

5.1.2.e

**Van:** 5.1.2.e  
**Verzonden:** vrijdag 24 april 2020 12:31  
**Aan:** 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e  
5.1.2.e @politie.nl>  
**CC:** 5.1.2.e <5.1.2.e @politie.nl>; 5.1.2.e  
<5.1.2.e @politie.nl>; 5.1.2.e [Dienst ICT] 5.1.2.e @politie.nl>;  
5.1.2.e 5.1.2.e @politie.nl>  
**Onderwerp:** FW: Monitoringstool meldkamerwerkplekken

Beste Mannen

Bijgaande Functionele Uitvraag heb ik (omdat ik kennelijk budgethouder ben?) namens de Landelijke Meldkamers uitgezet in de markt.

Ik meende te weten dat, omdat het hier met name end-point monitoring betrof, 5.1.2.i en 5.1.2.i in hun vragen niet kunnen voorzien. In Oktober – December hebben zij daarom een proef met 5.1.2.i gedaan, die goed beviel.

Zouden jullie misschien alsnog willen verifiëren dat onze standaard 5.1.2.i toolsuite niet volstaat?

Bij voorbaat dank!

Met vriendelijke groet,

5.1.2.e

5.1.2.e

**Politie | Dienst ICT | InfraBedrijf | Beheertooling – Operations Control Room**  
Odijskerweg 19, 3972 NE Driebergen  
Postbus 238, 3970 AE Driebergen  
Mobiel: 06 5.1.2.e

Loket Beheertooling: 5.1.2.i @politie.nl  
Loket Operation Control Room: 5.1 @politie.nl



**Van:** 5.1.2.e [mailto:5.1.2.e @5.1.2.i .com]  
**Verzonden:** donderdag 23 april 2020 20:44  
**Aan:** 5.1.2.e ) <5.1.2.e @politie.nl>

cc: 5.1.2.e 5.1.2.e @5.1.2.i .com>

Onderwerp: FW: Monitoringstool meldkamerwerkplekken

Hallo 5.1.2.e ,

Even twee zaken,

1. Heb met 5.1.2.e Gesproken mbt het licentie issue, hij heeft inmiddels contact met iemand uit de support organisatie. Ik heb met hem afgesproken dat we dinsdag ochtend even contact hebben om te kijken wat we verder moeten doen. Vooralsnog zit er weer een werkende tijdelijke key in het syteem.

2. Ik heb bijgaande Functionele uitvraag ontvangen via 5.1.2.i . Het betreft een uitvraag voor een " Software Tool" voor de nieuwe landelijke Meldkamer. Als ik dit zo lees vragen ze 5.1.2.e functionaliteit gezien de eis voor een agentless oplossing.

Ik vraag me af of je hiervan af weet want dit is waarvoor de FELA uiteindelijk bedoeld is.

5.2.1

Ik bel je morgen even.

Prettige avond!

Groeten,

5.1.2.e

Met vriendelijke groet/ Best regards,

5.1.2.e / Pre-Sales Lead 5.1.2.i / +31 6 5.1.2.e  
5.1.2.e @5.1.2.i .com

**Van:** 5.1.2.e  
**Aan:** 5.1.2.e 5.1.2.  
**Onderwerp:** FW: TU 5.1.2.e Adobe licenties SPOED uitvraag  
**Datum:** donderdag 2 juli 2020 08:31:57  
**Bijlagen:** 5.1.2.e [Adobe licenties.docx](#)

---

Hi 5.1.2.e

Ter info, de as-is uitvraag voor Adobe.

Side-note: ik zie weer een bericht van 5.1. . 5.2.1

5.1.2.e

Product adviseur a.i.

Politie | Politie Diensten Centrum | Dienst ICT | Infrabedrijf | WPKA  
 Zeisterweg 1, 3984 NH Odijk  
 Postbus 238, 3970 AE Driebergen  
 M +31 5.1.2.e

Werkdagen: dinsdag t/m vrijdag

---

**Van:** 5.1.2.e

**Verzonden:** woensdag 1 juli 2020 15:14

**Aan:** 5.1.2.e 5.1.2.e @politie.nl>

**Onderwerp:** TU 5.1.2.e Adobe licenties SPOED uitvraag

Hallo 5.1.2.e

Zoals telefonisch besproken hierbij de Technische Uitvraag t.b.v. de adobe licenties.  
 Hoor graag of dit zo de bedoeling is.

Groet, 5.1.2.e

5.1.2.e

**Inkoper**

Politie | Politiedienstencentrum | Dienst Verwerving  
 Hanzelaan 150, 8017 JG Zwolle  
 Postbus 618, 7300 AP Apeldoorn

M 06 5.1.2.e  
 E 5.1.2. 5.1.2.e 5.1.2.e [politie.nl](#)  
 werkdagen: ma, di, woe, do

**Van:** 5.1.2.e 5.1.2.  
**Aan:** 5.1.2.e  
**Onderwerp:** RE: AVG-compliance contracten NP/PDC/ICT/Ontwikkeling  
**Datum:** maandag 10 augustus 2020 12:59:35

---

Dag 5.1.2.e

Degene die ik gesproken had, zou de bevestigingen nog nasturen....

Ik zal bij haar navragen of het week lukt deze week naar mij te sturen.

Bedankt voor de reminder.

Gr 5.1.2.e

---

**Van:** 5.1.2.e  
**Verzonden:** maandag 10 augustus 2020 10:03  
**Aan:** 5.1.2.e 5.1.2.e <5.1.2.e> @politie.nl  
**Onderwerp:** RE: AVG-compliance contracten NP/PDC/ICT/Ontwikkeling

Goedemorgen 5.1.2.e

Is alweer even geleden dat we contact hadden. Ik vroeg mij af of jij nog bezig bent met het verzamelen van info betreffende de contracten? Zo nee, dan moet ik even verder zoeken.

Met vriendelijke groet,

5.1.2.e  
**Inkoopadviseur**  
 Politie | Politiedienstencentrum | Dienst FM | IKM

Bezoekadres: Europalaan 93, 3526 KP Utrecht

M 06 5.1.2.e

**Inkoopvragen of inkoopadvies nodig:** 5.1.2.i @politie.nl

**Maakt deel uit van privacyteam**




---

**Van:** 5.1.2.e  
**Verzonden:** dinsdag 14 juli 2020 15:51  
**Aan:** 5.1.2.e 5.1.2.e <5.1.2.e> @politie.nl  
**Onderwerp:** RE: AVG-compliance contracten NP/PDC/ICT/Ontwikkeling

Hi 5.1.2.e

Leuk even met je gesproken te hebben. Hierbij nogmaals het bestand met toevoeging van enkele vragen per contract. Vragen zijn soms hetzelfde.

Met vriendelijke groet,

5.1.2.e  
**Inkoopadviseur**  
 Politie | Politiedienstencentrum | Dienst FM | IKM

Bezoekadres: Europalaan 93, 3526 KP Utrecht

M 06 5.1.2.e

Inkoopvragen of inkoopadvies nodig 5.1.2.i @politie.nl

Maakt deel uit van privacyteam



---

Van: 5.1.2.e

Verzonden: maandag 13 juli 2020 17:33

Aan: 5.1.2.e 5.1.2.e <5.1.2.e@politie.nl>

Onderwerp: AVG-compliance contracten NP/PDC/ICT/Ontwikkeling

Beste 5.1.2.e

Om te voldoen aan de Algemene verordening gegevensbescherming (AVG) is begin 2018 het Programma Privacy Compliance gestart. Met dit Programma beoogt de Politie om binnen afzienbare tijd te voldoen aan alle facetten van de AVG, w.o. de registerplicht, het uitvoeren van gegevensbeschermingseffectbeoordelingen (**GEB**) en het waar nodig sluiten van verwerkersovereenkomsten met derden.

Het team analyse contracten, dat deel uitmaakt van het Privacyteam, richt zich binnen het Programma op het geven van inzicht in de mate van AVG Compliance van alle op dit moment actieve contracten waarbij de Politie contractpartij is. In dat kader zijn en worden ook alle ICT-contracten onder de loep genomen. Van een aantal andere contracten is helaas onvoldoende informatie beschikbaar om te kunnen vaststellen of er persoonsgegevens verwerkt worden en zo ja, hoe deze verwerkt worden. Informatie die nodig is om te kunnen bepalen of er met de leverancier een verwerkersrelatie is en eventueel een verwerkersovereenkomst gesloten moet worden.

Bijgevoegd een overzicht van de overeenkomsten NP/PDC/ICT/Ontwikkeling waarbij jij als contractmanager geregistreerd staat. Vandaar dat ik jou nu aanschrijf om te vragen of jij mij kunt helpen bij het vergaren van de ontbrekende informatie. Wellicht zelf of door verwijzing naar een collega die mij de informatie kan aanreiken.

Kan me voorstellen dat ik je nu overval. Laat even bezinken en misschien kunnen we daarna binnenkort even contact hebben over mijn verzoek.

Met vriendelijke groet,

5.1.2.e

Inkoopadviseur

Politie | Politiedienstencentrum | Dienst FM | IKM

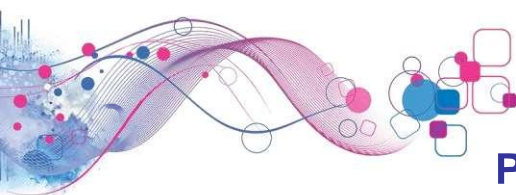
Bezoekadres: Europalaan 93, 3526 KP Utrecht

M 06 5.1.2.e

Inkoopvragen of inkoopadvies nodig 5.1.2.i @politie.nl

Maakt deel uit van privacyteam





## Pay per Use Opdrachtbevestiging

5.1.2.i fraude- en risicomanagement oplossingen

### Afnemer

|                    |                                     |                               |                          |
|--------------------|-------------------------------------|-------------------------------|--------------------------|
| Naam bedrijf       | Nationale Politie Eenheid Rotterdam | Factuuradres                  | Postbus 33137            |
| H/o                | Dienst Regionale Intelligence       | Postcode & plaats             | 3005 EC Rotterdam        |
| KvK-nummer         | 5.1.2.i                             | Ter attentie van              | Politie Team Crediteuren |
| Adres              | Doelwater 5                         | E-mailadres facturatie        | 5.1.2.i @politie.nl      |
| Postcode en plaats | 3011 AH Rotterdam                   | BTW nummer                    |                          |
| Contactpersoon     | 5.1.2.e                             | E-mailadres voor calamiteiten | 5.1.2.e @politie.nl      |
| E-mailadres        | 5.1.2.e @politie.nl                 | Website                       |                          |
| Telefoonnummer     | 06 5.1.2.e                          |                               |                          |

### Opdracht

Afnemer geeft 5.1.2.i hierbij opdracht tot het uitvoeren van de hieronder genoemde diensten onder de hieronder weergegeven voorwaarden. Op deze Opdrachtbevestiging zijn de Algemene Voorwaarden van 5.1.2.i van toepassing (zie bijlage 3, hierna: 'Algemene Voorwaarden'). Door ondertekening van deze Opdrachtbevestiging verklaart Afnemer een exemplaar van de Algemene Voorwaarden te hebben ontvangen.

5.1.2.i kan een toetsing uitvoeren in haar kredietbureau naar bovenstaande Afnemer en haar bestuurders. 5.1.2.i behoudt zich het recht voor om de toegang tot haar diensten te weigeren indien de uitkomst van de toetsing daartoe aanleiding geeft.

### Diensten (aankruisen wat van toepassing is)

☒ Online diensten\*

☒ 5.1.2.i

### Voorwaarden

De Diensten van 5.1.2.i mogen enkel gebruikt worden voor de Geoorloofde Doelen (zie bijlage 1) en in elk geval niet voor eventuele (direct) marketingactiviteiten of krediet- en/of (handels)informatiebureau activiteiten door de Afnemer of derden.

De Afnemer moet, als verantwoordelijke, garanderen dat de betrokkenen correct geïnformeerd zijn over het gebruik van de Diensten door de Afnemer, overeenkomstig de vereisten van de Algemene Verordening Gegevensbescherming met nummer (EU) 2016/679 ("AVG") van toepassing. Deze informatie omvat minstens de bedrijfsnaam van 5.1.2.i en de contactgegevens van 5.1.2.i het/de doeleinde(n) waarvoor de persoonsgegevens van de betrokkenen worden gedeeld met 5.1.2.i in het kader van de Diensten en de betrokken categorieën van persoonsgegevens. Afnemer zal 5.1.2.i vrijwaren voor enige schade die voortvloeit uit het gebruik van de persoonsgegevens (zoals geleverd als onderdeel van de Diensten) welke niet in lijn is met de Geoorloofde Doelen zoals beschreven in deze Opdrachtbevestiging.

Indien betrokkenen vragen hebben over de manier waarop zij bij 5.1.2.i geregistreerd zijn verwijst Afnemer deze betrokkenen door naar 5.1.2.i Betrokkenen kunnen contact opnemen via 0900-5.1.2.i of inzage@5.1.2.i.nl voor meer informatie.

In aanvulling op artikel 4.6 van de Algemene Voorwaarden zijn de partijen het eens dat 5.1.2.i geen enkele beslissing neemt namens de Afnemer, op welke wijze of in welke vorm dan ook. 5.1.2.i verstrekt uitsluitend informatie en de Afnemer erkent dat de Diensten van 5.1.2.i niet dienen te worden gebruikt als de enige basis voor zakelijke besluiten. Indien een getroffen persoon vragen zou hebben betreffende een dergelijke zakelijke beslissing, moet de Afnemer in staat zijn dit degelijk te motiveren.

5.1.2.i past ook de Gedragscode Verwerking Persoonsgegevens van de Nederlandse Vereniging van Handelsinformatiebureaus toe.

5.1.2.i is bevoegd de overeenkomst met onmiddellijke ingang op te zeggen, zonder dat 5.1.2.i hierdoor schadeplichtig wordt, indien als gevolg van wijzigingen in wetten, voorschriften, gedragscodes of andere regels van gelijke kracht (inclusief alle redelijke interpretaties daarvan), of enige wijziging (daaronder begrepen beëindiging) van enige door 5.1.2.i gehouden licentie, het in de redelijke visie van 5.1.2.i niet langer mogelijk of commercieel haalbaar is om de verlening van de Diensten aan Afnemer onder deze Overeenkomst voort te zetten.

### Tarieven

De op de datum van ondertekening geldende tarieven worden weergegeven op de tarievenlijst (zie bijlage 2). Tarieven zijn excl. BTW en legeskosten. In afwijking van artikel 12.6 van de Algemene Voorwaarden zijn de tarieven onderworpen aan een jaarlijkse prijsindexering, welke plaats vindt op iedere 1<sup>ste</sup> van april. Deze prijsindexering bedraagt 2%, berekend over de op dat moment geldende tarieven. De jaarlijkse administratiekosten voor de online diensten zijn € 45.

### Facturatie

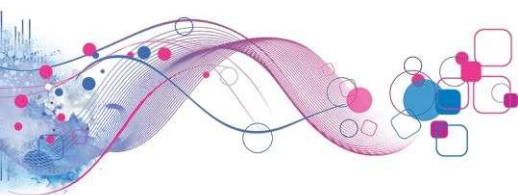
: \*Maandelijks achteraf

### Plaats en Ingangsdatum

: ..... januari 2021

### Opmerkingen

:



## Pay per Use Opdrachtbevestiging

5.1.2.i fraude- en risicomanagement oplossingen

### Ondertekening

(Handt

5.1.2.e

Nation

5.1.2.e

(Handtekening)

5.1.2.i Nederland B.V.

5.1.2.e

Graag na ondertekening scannen en mailen naar [info@nl.5.1.2.i.com](mailto:info@nl.5.1.2.i.com)

### Bijlage 1

#### Geoorloofde Doelen

##### Credit Check

Credit Check mag uitsluitend gebruikt worden voor de eigen interne zakelijke doeleinden van de Afemer ter ondersteuning van de Afemer bij diens besluitvorming, zoals gebaseerd op het eigen (krediet)beleid van de Afemer, met betrekking tot de 1) selectie van potentiële (handels)partners, 2) het al dan niet, onder bepaalde voorwaarden, aangaan, voortzetten of beëindigen van handel en/of een handelsrelatie en 3) het voorkomen van misbruik en fraude bij financiële transacties.

##### E-commerce Check

E-commerce Check mag uitsluitend gebruikt worden voor de eigen interne zakelijke doeleinden van de (e-Commerce) Afemer ter ondersteuning van de Afemer bij diens besluitvorming, zoals gebaseerd op het eigen (krediet)beleid van de Afemer, met betrekking tot de 1) de selectie van potentiële (handels)partners, 2) het al dan niet, onder bepaalde voorwaarden, aangaan, voortzetten of beëindigen van handel en/of een handelsrelatie en 3) het voorkomen van misbruik en fraude bij financiële transacties.

##### Autotrace

Autotrace mag enkel gebruikt worden voor de eigen interne zakelijke doeleinden van de Afemer om 1) de vorderingsopties te beoordelen en natuurlijke personen en/of wettelijke entiteiten op te sporen in het kader van de incassoprocedure, 2) fraude en andere misdrijven te voorkomen en op te sporen en 3) de Afemer te ondersteunen bij het nemen van beslissingen tijdens de incassoprocedure over of hij in bepaalde omstandigheden een handelsrelatie moet aangaan, voortzetten of beëindigen.

##### ID-Check

ID-Check mag uitsluitend gebruikt worden voor de eigen interne zakelijke doeleinden van de Afemer ter verificatie van de echtheid van identiteitsdocumenten zoals paspoorten, identiteitskaarten en rijbewijzen. **Dit product mag uitsluitend worden gebruikt indien en nadat het Nederlandse Ministerie van Binnenlandse Zaken daarvoor toestemming heeft gegeven.**

**Van:** 5.1.2.e 5.1. namens [PDC - FM - Team RFS Rotterdam - Bedrijfsadministratie - Contracten](#)  
**Aan:** 5.1.2.e  
**Onderwerp:** RE: dringend verzoek - 5.1.2.i - verwerkersovereenkomst  
**Datum:** woensdag 6 januari 2021 08:11:39

---

Hoi 5.1.2.e ,

Heb je ooit een antwoord gekregen op de aanvraag?

Met vriendelijke groet,

5.1.2.e 5.1.2.e  
 5.1.2.e

06 – 5.1.2.e  
 Werkdagen: ma, di, wo en do

Politie | PDC | Dienst Facility Management | Team Bedrijfsadministratie  
 Prins Frederik Hendrikstraat 40, 3051ES Rotterdam

Meer informatie? Kijk op [politie.nl](https://politie.nl)

5.1.2.i @politie.nl

---

**Van:** 5.1.2.e  
**Verzonden:** dinsdag 5 5.1.2.e 2021 13:18  
**Aan:** PDC - FM - Team RFS Rotterdam - Bedrijfsadministratie - Contracten  
 5.1.2.i @politie.nl>  
**Onderwerp:** RE: dringend verzoek - 5.1.2.i - verwerkersovereenkomst

Hoi,

Ik heb in 2018 e.e.a. in gang gezet, daarna heb ik er geen bemoeienis meer mee gehad.  
 Ik heb je net deze stukken gemailld via de mailbox.

Met vriendelijke groeten,

5.1.2.e  
**Adviseur bedrijfsvoering DRIO**  
 Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Doelwater 5,  
 3011AH Rotterdam  
 06- 5.1.2.e  
 Vrijdag is mijn roostervrije dag

5.1.2.e @politie.nl

---

**Van:** 5.1.2.e 5.1.2.e **Namens** PDC - FM - Team RFS Rotterdam - Bedrijfsadministratie - Contracten  
**Verzonden:** dinsdag 5 januari 2021 13:07  
**Aan:** 5.1.2.e 5.1.2.e @politie.nl>  
**Onderwerp:** RE: dringend verzoek - 5.1.2.i - verwerkersovereenkomst

Hoi 5.1.2.e ,

Wij kennen deze overeenkomst met 5.1.2.i helemaal niet. Kan jij zien wie deze heeft afgesloten?

Kunnen we dan een exemplaar van de overeenkomst krijgen? We weten dus ook niet wat de afspraken zijn over de verwerkingsovereenkomst.

Met vriendelijke groet,

5.1.2.e  
5.1.2.e

06 – 5.1.2.e  
Werkdagen: ma, di, wo en do

Politie I PDC I Dienst Facility Management I Team Bedrijfsadministratie  
Prins Frederik Hendrikstraat 40, 3051ES Rotterdam

Meer informatie? Kijk op [politie.nl](https://politie.nl)

5.1.2.i @politie.nl

---

**Van:** 5.1.2.e

**Verzonden:** dinsdag 5 januari 2021 09:38

**Aan:** PDC - FM - Team RFS Rotterdam - Bedrijfsadministratie - Contracten  
<5.1.2.i @politie.nl>

**Onderwerp:** FW: dringend verzoek - 5.1.2.i - verwerkersovereenkomst

Ha,

Ik neem aan dat dit hier afgehandeld moet worden?  
Zo niet dan hoor ik graag waar wel...

Bij voorbaat dank

Met vriendelijke groeten,

5.1.2.e  
**Adviseur bedrijfsvoering DRIO**  
Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Doelwater 5,  
3011AH Rotterdam  
06- 5.1.2.e  
Vrijdag is mijn roostervrije dag

5.1.2.e @politie.nl

---

**Van:** 5.1.2.e

**Verzonden:** dinsdag 5 januari 2021 08:23

**Aan:** 5.1.2.e 5.1.2.e @politie.nl>

**Onderwerp:** FW: dringend verzoek - 5.1.2.i - verwerkersovereenkomst

Hoi 5.1.2.e , kun jij onderstaand verzoek uitzetten?

Met vriendelijke groet

5.1.2.e  
Informatie Analist (OSB)  
5.1.2.e

06 – 5.1.2.e of 0900 – 8844

Werkdagen: ma, di, wo, do

Politie | [Rotterdam](#) | DRIO | BI&K | [BICC](#)

Doelwater 5, 3011AH te Rotterdam

Postbus 70023 , 3000LD te Rotterdam

06 5.1.2.e

5.1.2.e [@politie.nl](#)

[SMS](#)

---

**Van:** 5.1.2.e [\[mailto:5.1.2.e@5.1.2.i.com\]](#)

**Verzonden:** maandag 4 januari 2021 17:04

**Aan:** 5.1.2.e <5.1.2.e@politie.nl>; 5.1.2. [@politie.nl](#)

**CC:** 5.1.2.e, 5.1.2.i [.com](#)>

**Onderwerp:** dringend verzoek - 5.1.2.i - verwerkersovereenkomst

Hallo 5.1.2.e ,

5.1.2.i

Indien jullie gebruik willen blijven maken van de diensten, dienen we deze echter **zo spoedig mogelijk** in plaats te krijgen.

Hieronder een uitleg van wat te doen. Graag zien wij dit deze week retour, en zijn anders helaas genoodzaakt de dienst af te sluiten.

Als verwerkingsverantwoordelijke en/of verwerker van persoonsgegevens doet 5.1.2.i er alles aan om te voldoen aan de vereisten van de AVG.

De specifieke rol die wij aannemen kan bij elke verwerkingsactiviteit, gelet op de diensten die wij aan onze cliënten leveren, verschillend zijn.

In het kader van bovenstaand streven, hebben wij u diverse keren gevraagd om een verwerkersovereenkomst met ons te tekenen. Volgens onze administratie hebben wij deze echter nog niet getekend mogen ontvangen.

Mocht het zo zijn, dat u bij onze eerdere correspondentie een reactie heeft gegeven en hier nog niet op is gereageerd, dan verzoeken wij u vriendelijk dit nogmaals te doen naar

5.1.2.i [.com](#).

Om het u gemakkelijk te maken sturen wij u nogmaals een exemplaar van de verwerkersovereenkomst toe samen met de toelichting voor het invullen van bijlage A op pagina 13 van de verwerkersovereenkomst.

Wij vragen u de [verwerkersovereenkomst](#) digitaal volledig in te vullen (voorblad en pagina 1 (achtergrond (A) datum ondertekening overeenkomst en product ), 11, 12 (ondertekening) en 13 bijlage A invullen met behulp van de toelichting) en deze te retourneren naar

5.1.2.i [.com](#).

Veel dank voor uw medewerking.

Met vriendelijke groet / Best regards,

5.1.2.e

5.1.2.i | *Business Development Manager Data*

M: +31 (0)6 5.1.2.e / 5.1.2.e

5.1.2.i

=====

Information in this e-mail and any attachments is confidential, and may not be copied or used by anyone other than the addressee, nor disclosed to any third party without our permission. There is no intention to create any legally binding contract or other binding commitment through the use of this electronic communication, except where such contract or commitment has been confirmed and duly signed by an authorized representative of

5.1.2.i

Although 5.1.2.i has taken reasonable steps to ensure that this communication and any attachments are free from computer viruses, you are advised to take your own steps to ensure that they are actually virus free.

Registered name: 5.1.2.i

Registered office: 5.1.2.i

Chamber of Commerce number: 5.1.2.i

Van: 5.1.2.1  
 Aan: 5.1.2.1  
 Onderwerp: 5.1.2.1  
 Datum: donderdag 7 januari 2021 13:53:27

5.1.2.1 @online.nl

Met vriendelijke groet,

5.1.2.1

5.1.2.1

06-5.1.2.1 di, wo en do

Polite / POC / Dienst Facility Management / Team Bedrijfsadministratie

Pirra Frederik Hendrikstraat 40, 3015ES Rotterdam

Meer informatie? Kijk op [polite.nl](https://www.polite.nl)

5.1.2.1 @online.nl

Van: 5.1.2.1

Verzonden: donderdag 7 januari 2021 13:52

Aan: 5.1.2.1 @online.nl

Onderwerp: RE: Info betref 5.1.2.1 - Autotrace

Heb je ook het emailadres voor me?

Met vriendelijke groeten,

5.1.2.1

Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Dochter 5,

3011AH Rotterdam

Vrijdag 11 januari 2021 13:53:27

5.1.2.1 @online.nl

Van: 5.1.2.1

Verzonden: donderdag 7 januari 2021 13:27

Aan: 5.1.2.1 @online.nl

Onderwerp: RE: Info betref 5.1.2.1 - Autotrace

Hi,

Het KVK nummer is 5.1.2.1

Het factuuradres is:

5.1.2.1

1.1.1.1

Ja, graag ontvangen wij het nieuwe contract / overeenkomst.

Met vriendelijke groet,

5.1.2.1

06-5.1.2.1 di, wo en do

Polite / POC / Dienst Facility Management / Team Bedrijfsadministratie

Pirra Frederik Hendrikstraat 40, 3015ES Rotterdam

Meer informatie? Kijk op [polite.nl](https://www.polite.nl)

5.1.2.1 @online.nl

Van: 5.1.2.1

Verzonden: donderdag 7 januari 2021 12:18

Aan: POC - FM - Team RPS Rotterdam - Bedrijfsadministratie - Contracten 5.1.2.1 @online.nl

Onderwerp: RE: Info betref 5.1.2.1 - Autotrace

Hi,

Heb je voor mij ons KVK nummer en het juiste adres voor facturatie, dit moet op het nieuwe contract en werkingsovereenkomst.

Willen jullie een kopie van deze overeenkomst en het nieuwe contract?

Met vriendelijke groeten,

5.1.2.1

Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Dochter 5,

3011AH Rotterdam

Vrijdag 11 januari 2021 13:53:27

5.1.2.1 @online.nl

Van: 5.1.2.1

Verzonden: woensdag 6 januari 2021 13:49

Aan: 5.1.2.1 @online.nl

Onderwerp: RE: Info betref 5.1.2.1 - Autotrace

Hi,

5.1.2.1

We zijn er zo'n beetje uit. Het kostte even wat tijd. Sorry!

De opdrachtgever is uiteindelijk DRIO, Intelligence of Opsporing geweest.

Omdat de opdrachtgever zijn het verwerkingformulier ook alleen door die afdeling getekend worden.

Lukt het om iemand van b.v. DRIO het formulier te laten invullen en tekenen? Omdat er geen contract is kunnen wij als Contractmanagers er niets mee.

Met vriendelijke groet,

5.1.2.1

06-5.1.2.1 di, wo en do

Polite / POC / Dienst Facility Management / Team Bedrijfsadministratie

Pirra Frederik Hendrikstraat 40, 3015ES Rotterdam

Meer informatie? Kijk op [polite.nl](https://www.polite.nl)

5.1.2.1 @online.nl

Van: 5.1.2.1

Verzonden: woensdag 6 januari 2021 09:59

Aan: 5.1.2.1 @online.nl

Onderwerp: RE: Info betref 5.1.2.1 - Autotrace

Deze heb ik ook nog.

Met vriendelijke groeten,

5.1.2.1

Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Dochter 5,

3011AH Rotterdam

Vrijdag 11 januari 2021 13:53:27

5.1.2.1 @online.nl

Van: 5.1.2.1

Verzonden: vrijdag 6 september 2018 08:50

Aan: 5.1.2.1 @online.nl

CC: 5.1.2.1 @online.nl

Onderwerp: RE: Info betref 5.1.2.1 - Autotrace

De leverancier 5.1.2.1 staat bij de toets rechtmatig inkoop op rechtmatig. Onderstaande codering is ook niet onrechtmatig.

Binnen de rechtmatigheidszaken zijn een aantal coderingen onrechtmatig dit gaat om de codes 6.7 en 9.

5.1.2.1

Dienst Verwerking i.a.

Polite / POC / Verwerking i.a.

Binnendijk 106, 3015EP Zwalve

Postbus 270, 3015AE Dordrecht, Nederland

Al

Email: 5.1.2.1 @online.nl

Van: 5.1.2.1

Verzonden: donderdag 6 september 2018 11:04

Aan: 5.1.2.1 @online.nl

CC: 5.1.2.1 @online.nl

Onderwerp: RE: Info betref 5.1.2.1 - Autotrace

Hi,

Dit heb ik vernomen van 5.1.2.1 opgenomen in de CC.

Groet,

5.1.2.1

Van: 5.1.2.1

Verzonden: woensdag 5 september 2018 13:10

Aan: 5.1.2.1 @online.nl

Onderwerp: RE: Info betref 5.1.2.1 - Autotrace

Hi,

Je onderstaande mail heb ik gelezen. Ben benieuwd van wie jij uit de eenheid Rotterdam de info hebt ontvangen dat er een lijst met onrechtmatige inkoop is ontvangen in het platform bedrijfsvoering.

In het overzicht dat ik n. heb opgesteld samen met mijn collegae is een lijst met een top 22 van onrechtmatigheid die ik nog met het Platform BVO moet bespreken.

In dat overzicht top 22 niet genoemd vanwege het kleine volume. Wel 5.1.2.1 in de resultatenboets van april 2018 genoemd die wij van 5.1.2.1 business controller voor de Dienst Verwerking, hebben ontvangen.

5.1.2.1 kan je verder helpen om antwoord te geven op zijn vraag. Het gaat om het onderstaande.

|                       |         |         |         |  |         |         |                                |   |                          |
|-----------------------|---------|---------|---------|--|---------|---------|--------------------------------|---|--------------------------|
| Dienst Regionale      | 5.1.2.1 |         |         |  | 5.1.2.1 | 5.1.2.1 | business report, autotrace 12- | € | 2. Omvang opdracht onder |
| Informatieorganisatie |         | 5.1.2.1 | 5.1.2.1 |  | 5.1.2.1 | 2017    |                                |   | drempel                  |
| Dienst Regionale      | 5.1.2.1 |         |         |  | 5.1.2.1 | 5.1.2.1 | business report, autotrace     | € | 2. Omvang opdracht onder |

|                       |         |         |         |         |                               |       |                          |         |                      |
|-----------------------|---------|---------|---------|---------|-------------------------------|-------|--------------------------|---------|----------------------|
| Informatieorganisatie | BV      | 5.1.2.1 | 5.1.2.1 | 5.1.2   | 01/18                         | 5.1.2 | drempel                  | 5.1.2.1 | <a href="#">Link</a> |
| Diensit Regionale     | 5.1.2.1 |         |         | 5.1.2.1 | business report autotracc 02- | 5.1.2 | 2. Omvang opdracht onder |         |                      |
| Informatieorganisatie | 5.1.2.1 | 5.1.2.1 | 5.1.2.1 | 5.1.2   | 2018                          | 5.1.2 | drempel                  | 5.1.2.1 | <a href="#">Link</a> |
| Diensit Regionale     | 5.1.2.1 |         |         | 5.1.2   |                               | 5.1.2 | 2. Omvang opdracht onder |         |                      |
| Informatieorganisatie |         | 5.1.2.1 | 5.1.2.1 | 5.1.2   | 5.1.2.1                       | 5.1.2 | drempel                  | 5.1.2.1 | <a href="#">Link</a> |

Met vriendelijke groet,

5.1.2.e

Polite (PAC), Dienst Facility Management  
Postbus 19023, 3000 LD Rotterdam  
M 0 5.1.2.1

Werkdagen: maandag tot en met donderdag  
Afweging op vrijdag

Landelijke Serviceboek FM

T 05.1.2.1

Facilitair is slechts één -CLICK- bij je vandaan!

Van 5.1.2.1

Verzonden: Woensdag 5 september 2018 12:54

Aan 5.1.2.1 @politie.nl

Onderwerp: 5.1.2.1 - Autotracc

Ho 5.1.2.1

Ik weet niet of ik bij jou aan het juiste adres ben voor deze vraag. Vanuit de eenheid Rotterdam heb ik begrepen dat er een lijst met onrechtmatige inkoop is ontvangen in het platform bedrijfsvoering. Op deze lijst is aangegeven dat de spend bij leverancier 5.1.2.1 voor de Autotracc dienstverlening als onrechtmatig is bestempeld. Kan jij aan mij melden waarom dit als onrechtmatig is geïdentificeerd?

Met vriendelijke groet,

5.1.2.1

Polite (PAC), Dienst Verzekering (o)

Marlen Kneeling 35, 3008 AK Rotterdam

Postbus 19023, 3000 LD Rotterdam

M 0 5.1.2.1

# OVEREENKOMST INZAKE DE VERWERKING VAN GEGEVENS (AVG-VERSIE).

tussen

Politie Eenheid Rotterdam, DRIO

*(volledige bedrijfsnaam)*

en

5.1.2.i Nederland B.V.

DATUM

08 januari 2021

# INHOUD

---

## CLAUSULE

|     |                                                                |    |
|-----|----------------------------------------------------------------|----|
| 1.  | Definities en interpretatie .....                              | 1  |
| 2.  | Soorten Persoonsgegevens en verwerkingsdoeleinden .....        | 3  |
| 3.  | Verplichtingen van de Verwerker .....                          | 3  |
| 4.  | Werknemers van de Verwerker .....                              | 4  |
| 5.  | Beveiliging .....                                              | 4  |
| 6.  | Inbreuk op Persoonsgegevens .....                              | 5  |
| 7.  | Grensoverschrijdende overdracht van persoonsgegevens .....     | 6  |
| 8.  | Subverwerkers .....                                            | 6  |
| 9.  | Klachten, verzoeken van betrokkenen en rechten van derden..... | 7  |
| 10. | Informatieverplichting .....                                   | 8  |
| 11. | Duur en beëindiging .....                                      | 8  |
| 12. | Teruggave en vernietiging van gegevens .....                   | 8  |
| 13. | Gegevens.....                                                  | 9  |
| 14. | Controle .....                                                 | 9  |
| 15. | Garanties.....                                                 | 11 |
| 16. | Kennisgeving.....                                              | 11 |

## BIJLAGE

|           |                                                                |    |
|-----------|----------------------------------------------------------------|----|
| BIJLAGE A | Doeleinden en details van verwerking van persoonsgegevens..... | 13 |
| BIJLAGE B | Modelcontractbepalingen.....                                   | 14 |

Deze overeenkomst is gedateerd op 08 - 01-2021

## PARTIJEN

(1) Politie Eenheid Rotterdam (volledige bedrijfsnaam)  
gevestigd en geregistreerd in Nederland (land) met  
inschrijvingsnummer 5.1.2.i (nummer) met geregistreerd kantoor te  
\_\_\_\_\_ (adres geregistreerd kantoor) (**Verwerkingsverantwoordelijke**)

en

(2) 5.1.2.i gevestigd en geregistreerd in Nederland met  
inschrijvingsnummer 5.1.2.i met geregistreerd kantoor te 5.1.2.i  
 (**Verwerker**)

## ACHTERGROND

- (A) De Verwerkingsverantwoordelijke en Verwerker zijn  
8 januari 2021, overeenkomst autotrace (datum en beschrijving  
overeenkomst tussen Verwerkingsverantwoordelijke en Verwerker) aangegaan  
(**Raamovereenkomst**) waarbij het kan zijn dat de Verwerker Persoonsgegevens  
namens de Verwerkingsverantwoordelijke verwerkt.
- (B) Deze Overeenkomst inzake de Verwerking van Persoonsgegevens (**Overeenkomst**)  
bevat de aanvullende voorwaarden en bepalingen waarop de Verwerker  
Persoonsgegevens zal verwerken bij het verlenen van diensten in het kader van de  
Raamovereenkomst. Deze Overeenkomst bevat de verplichte clausules van artikel 28,  
lid 3, van de Algemene Verordening Gegevensbescherming ((EU) 2016/679) voor  
contracten tussen verwerkingsverantwoordelijken en verwerkers.

## OVEREENGEKOMEN VOORWAARDEN

### 1. Definities en interpretatie

De volgende definities en interpretatieregels zijn in deze overeenkomst van toepassing.

#### 1.1 Definities:

**Bevoegde Personen:** de personen of categorieën van personen die de  
Verwerkingsverantwoordelijke machtigt om de Verwerker instructies voor de verwerking  
van persoonsgegevens te geven, zoals omschreven in BIJLAGE A.

**Zakelijke Doeleinden:** de in de Raamovereenkomst beschreven diensten of enig ander  
specifiek in BIJLAGE A genoemd doel.

**Betrokkene:** een persoon die het onderwerp is van Persoonsgegevens.

**Persoonsgegevens:** alle informatie betreffende een geïdentificeerd of identificeerbaar  
natuurlijk persoon die door de Verwerker wordt verwerkt als gevolg van of in verband  
met de verlening van de diensten in het kader van de Raamovereenkomst; als  
identificeerbaar natuurlijk persoon wordt beschouwd een persoon die direct of indirect

kan worden geïdentificeerd, met name aan de hand van een identificatiecode, zoals naam, identificatienummer, locatiegegevens, een online-identificatiecode of een of meer specifieke kenmerken van de fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit van die natuurlijke persoon.

**Verwerken, verwerkingen en verwerking:** ofwel elke activiteit die het gebruik van Persoonsgegevens met zich meebrengt, ofwel omdat de Wetgeving Inzake Gegevensbescherming het verwerken, verwerkingen en verwerking op een andere manier kan definiëren. Het omvat elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of reeksen van persoonsgegevens, al dan niet met behulp van geautomatiseerde middelen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, aanpassen of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of anderszins beschikbaar stellen, samenbrengen, samenvoegen beperken, wissen of vernietigen. De verwerking omvat ook de overdracht van Persoonsgegevens aan derden.

**Wetgeving Inzake Gegevensbescherming:** alle toepasselijke wetten op het gebied van privacy en gegevensbescherming, met inbegrip van de Algemene Verordening Gegevensbescherming ((EU) 2016/679) en alle toepasselijke nationale uitvoeringswetten, regelgeving en secundaire wetgeving in Nederland met betrekking tot de verwerking van Persoonsgegevens en de privacy van elektronische communicatie, zoals van tijd tot tijd gewijzigd, vervangen of bijgewerkt.

**Inbreuk op Persoonsgegevens:** schending van de veiligheid die leidt, hetzij per ongeluk, hetzij onrechtmatig, tot vernietiging, verlies, vervalsing en ongeoorloofde vrijgave van of toegang tot Persoonsgegevens die worden overgedragen, bewaard of anderszins verwerkt.

**Modelcontractbepalingen (MCB):** de standaardcontractbepalingen van de Europese Commissie voor de doorgifte van Persoonsgegevens van de Europese Unie aan in derde landen gevestigde verwerkers (doorgifte van verwerkingsverantwoordelijke naar verwerkers), zoals bepaald in de bijlage bij Besluit 2010/87/EU van de Commissie, waarvan een ingevuld exemplaar is bijgevoegd als BIJLAGE B.

- 1.2 Deze Overeenkomst is onderworpen aan de voorwaarden van de Raamovereenkomst en is opgenomen in de Raamovereenkomst. Op de interpretatie van deze overeenkomst zijn interpretaties en gedefinieerde termen uit de Raamovereenkomst van toepassing.
- 1.3 De Bijlagen maken deel uit van deze Overeenkomst en zijn van kracht alsof zij volledig in deze Overeenkomst zijn opgenomen. Elke verwijzing naar deze Overeenkomst omvat de Bijlagen.
- 1.4 Een verwijzing naar schriftelijk of schrijven omvat faxen en e-mail.
- 1.5 In geval van een conflict of ambiguïteit tussen:
  - (a) de bepalingen in deze Overeenkomst en de bepalingen in de Bijlagen, hebben de bepalingen in deze Overeenkomst voorrang;
  - (b) de voorwaarden van de begeleidende facturen of andere documenten die aan deze Overeenkomst zijn gehecht en debepalingen in de Bijlagen, prevaleren de bepalingen in de Bijlagen;

- (c) de bepalingen van deze Overeenkomst en de bepalingen van de Raamovereenkomst, prevaleren de bepalingen van deze Overeenkomst; en
- (d) de bepalingen van deze Overeenkomst en van de uitgevoerde MCB, prevaleren de bepalingen van de uitgevoerde MCB.

## **2. Soorten Persoonsgegevens en verwerkingsdoeleinden**

- 2.1 De Verwerkingsverantwoordelijke en de Verwerker erkennen dat voor de toepassing van de Wetgeving Inzake Gegevensbescherming de Verwerkingsverantwoordelijke de verwerkingsverantwoordelijke is en de Verwerker de verwerker.
- 2.2 De Verwerkingsverantwoordelijke behoudt de controle over de Persoonsgegevens en blijft verantwoordelijk voor de naleving van zijn verplichtingen krachtens de toepasselijke Wetgeving Inzake Gegevensbescherming, met inbegrip van gerechtvaardigde verwerkingsgronden, het verstrekken van alle vereiste kennisgevingen en het verkrijgen van de vereiste toestemmingen, en voor de verwerkingsinstructies die hij aan de Verwerker geeft.
- 2.3 BIJLAGE A beschrijft het onderwerp, de duur, de aard en het doel van de verwerking en de categorieën van Persoonsgegevens en soorten Betrokkenen ten aanzien waarvan de Verwerker mag verwerken om de Zakelijke Doeleinden van de Raamovereenkomst te verwezenlijken.

## **3. Verplichtingen van de Verwerker**

- 3.1 De Verwerker dient de Persoonsgegevens alleen te verwerken voor zover dit noodzakelijk is voor de Zakelijke Doeleinden in overeenstemming met de schriftelijke instructies van de Verwerkingsverantwoordelijke van Bevoegde Personen. De Verwerker zal de Persoonsgegevens niet verwerken voor andere doeleinden of op een manier die niet in overeenstemming is met deze Overeenkomst of de Wetgeving Inzake Gegevensbescherming. De Verwerker moet de Verwerkingsverantwoordelijke onmiddellijk in kennis stellen als de instructie van de Verwerkingsverantwoordelijke naar zijn mening niet in overeenstemming is met de Wetgeving Inzake Gegevensbescherming.
- 3.2 De Verwerker moet zonder onnodige vertraging gevolg geven aan elk verzoek van de Verwerkingsverantwoordelijke of instructie van Bevoegde Personen om de Persoonsgegevens te wijzigen, over te dragen, te verwijderen of anderszins te verwerken, of om ongeoorloofde verwerking te stoppen, te beperken of te verhelpen.
- 3.3 De Verwerker zal de vertrouwelijkheid van alle Persoonsgegevens waarborgen en zal geen Persoonsgegevens aan derden bekendmaken, tenzij de Verwerkingsverantwoordelijke of deze Overeenkomst of de Raamovereenkomst specifiek toestemming geeft voor de bekendmaking of zoals vereist door de wet. Indien een wet, rechtbank, regelgever of toezichthoudende autoriteit de Verwerker verplicht Persoonsgegevens te verwerken of openbaar te maken, moet de Verwerker eerst de Verwerkingsverantwoordelijke op de hoogte brengen van de wettelijke of reglementaire vereisten en de Verwerkingsverantwoordelijke in de gelegenheid stellen om bezwaar aan te tekenen of de eis aan te vechten, tenzij de wet een dergelijke kennisgeving verbiedt.

- 3.4 De Verwerker zal de Verwerkingsverantwoordelijke redelijkerwijs bijstaan in het nakomen van de verplichtingen van de Verwerkingsverantwoordelijke uit hoofde van de Wetgeving Inzake Gegevensbescherming, rekening houdend met de aard van de verwerking door de Verwerker en de informatie waarover de Verwerker beschikt, onder meer met betrekking tot de rechten van de Betrokkene, gegevensbeschermingseffectbeoordelingen en rapportage aan en overleg met toezichthoudende autoriteiten uit hoofde van de Wetgeving Inzake Gegevensbescherming.
- 3.5 De Verwerker moet de Verwerkingsverantwoordelijke onverwijld in kennis stellen van alle wijzigingen in de Wetgeving Inzake Gegevensbescherming die een nadelig effect kunnen hebben op de uitvoering van de Raamovereenkomst door de Verwerker.

#### **4. Werknemers van de Verwerker**

- 4.1 De Verwerker dient ervoor te zorgen dat alle werknemers:
- (a) op de hoogte zijn van het vertrouwelijke karakter van de Persoonsgegevens en dat zij gebonden zijn aan geheimhoudingsverplichtingen en gebruiksbeperkingen ten aanzien van de Persoonsgegevens;
  - (b) een training hebben gevolgd over de Wetgeving Inzake Gegevensbescherming met betrekking tot de omgang met Persoonsgegevens en de wijze waarop deze van toepassing is op hun specifieke taken; en
  - (c) op de hoogte zijn van zowel de plichten van de Verwerker als van zijn persoonlijke plichten en verplichtingen uit hoofde van de Wetgeving Inzake Gegevensbescherming en deze Overeenkomst.

#### **5. Beveiliging**

- 5.1 De Verwerker moet te allen tijde passende technische en organisatorische maatregelen treffen tegen ongeoorloofde of onrechtmatige verwerking, toegang, bekendmaking, openbaarmaking, kopiëren, wijziging, opslag, reproductie, weergave of verspreiding van Persoonsgegevens, en tegen toevallig of onrechtmatig verlies, vernietiging, wijziging, openbaarmaking of beschadiging van Persoonsgegevens. De Verwerker moet deze maatregelen schriftelijk vastleggen en periodiek, ten minste eenmaal per jaar, herzien om ervoor te zorgen dat zij actueel en volledig blijven.
- 5.2 De Verwerker moet dergelijke maatregelen nemen om te zorgen voor een beveiligingsniveau dat is afgestemd op het betrokken risico, ook waar nodig:
- (a) de pseudonimisering en encryptie van Persoonsgegevens;
  - (b) het vermogen om de blijvende vertrouwelijkheid, integriteit, beschikbaarheid en weerbaarheid van verwerkingssystemen en diensten te waarborgen;
  - (c) de mogelijkheid om de beschikbaarheid van en toegang tot persoonsgegevens tijdig te herstellen in geval van een fysiek of technisch incident; en
  - (d) een proces voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van beveiligingsmaatregelen.

## **6. Inbreuk op Persoonsgegevens**

- 6.1 De Verwerker zal de Verwerkingsverantwoordelijke onmiddellijk en zonder onnodige vertraging op de hoogte stellen als er Persoonsgegevens verloren gaan, vernietigd worden of beschadigd of gecorrumpeerd of onbruikbaar worden. De Verwerker zal deze Persoonsgegevens op eigen kosten herstellen.
- 6.2 De Verwerker zal binnen 24 uur en zonder onnodige vertraging de Verwerkingsverantwoordelijke op de hoogte stellen als hij van het volgende op de hoogte is:
- (a) elke accidentele, ongeoorloofde of onwettige verwerking van de Persoonsgegevens; of
  - (b) elke Inbreuk op Persoonsgegevens.
- 6.3 Wanneer de Verwerker kennis krijgt van (a) en/of (b) zoals hierboven vermeld, verstrekt hij de Verwerkingsverantwoordelijke zonder onnodige vertraging de volgende informatie:
- (a) beschrijving van de aard van (a) en/of (b), met inbegrip van de categorieën Persoonsgegevens en bij benadering het aantal Betrokkenen en Persoonsgegevens;
  - (b) de waarschijnlijke gevolgen; en
  - (c) beschrijving van de maatregelen die zijn genomen of worden voorgesteld ten aanzien van (a) en/of (b), inclusief maatregelen om de mogelijke negatieve effecten ervan te beperken.
- 6.4 Onmiddellijk na ongeoorloofde of onwettige verwerking van Persoonsgegevens of Inbreuk op Persoonsgegevens zullen de partijen met elkaar samenwerken om de zaak te onderzoeken. De Verwerker zal in redelijkheid met de Verwerkingsverantwoordelijke samenwerken bij de behandeling van de zaak door de Verwerkingsverantwoordelijke, waaronder:
- (a) meewerken aan elk type onderzoek;
  - (b) de Verwerkingsverantwoordelijke fysieke toegang te verschaffen tot alle betrokken faciliteiten en activiteiten;
  - (c) het faciliteren van gesprekken met de medewerkers van de Verwerker, voormalige medewerkers en andere betrokkenen bij de zaak;
  - (d) het beschikbaar stellen van alle relevante dossiers, logboeken, bestanden, gegevensrapportages en ander materiaal dat nodig is om te voldoen aan alle Wetgeving Inzake Gegevensbescherming of zoals anderszins redelijkerwijs vereist door de Verwerkingsverantwoordelijke; en
  - (e) het nemen van redelijke en snelle maatregelen om de effecten te beperken en de schade als gevolg van de Inbreuk op Persoonsgegevens of onwettige verwerking van Persoonsgegevens tot een minimum te beperken.
- 6.5 De Verwerker zal geen enkele derde partij op de hoogte stellen van een Inbreuk op Persoonsgegevens zonder voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke, behalve wanneer de wet dit vereist.

6.6 De Verwerkingsverantwoordelijke is verantwoordelijk voor:

- (a) de kennisgeving van de Inbreuk op Persoonsgegevens aan Betrokkenen, toezichthoudende autoriteiten, regelgevers, wetshandhavinginstanties of anderen, zoals vereist door de wet of regelgeving of naar goeddunken van de Verwerkingsverantwoordelijke, met inbegrip van de inhoud en de wijze van kennisgeving; en
- (b) het al dan niet aanbieden van enige vorm van genoegdoening aan de betreffende Betrokkenen, met inbegrip van de aard en omvang van die genoegdoening.

6.7 De Verwerker dekt alle redelijke kosten verbonden aan de uitvoering van de verplichtingen onder bepalingen 6.2 en 6.4, tenzij de zaak het gevolg is van specifieke instructies van de Verwerkingsverantwoordelijke of diens nalatigheid, opzettelijk verzuim of schending van deze overeenkomst, in welk geval de Verwerkingsverantwoordelijke alle redelijke kosten dekt.

6.8 De Verwerker vergoedt de Verwerkingsverantwoordelijke ook de werkelijke, redelijke kosten die de Verwerkingsverantwoordelijke maakt bij het reageren op een Inbreuk op Persoonsgegevens, voor zover de Verwerker een dergelijke Inbreuk op Persoonsgegevens heeft veroorzaakt, met inbegrip van alle kosten van kennisgeving en redelijke verhaalsmogelijkheden zoals bepaald in bepaling 6.6.

6.9 Alle beperkingen en uitsluitingen van aansprakelijkheid zoals vastgelegd in de Raamovereenkomst zijn eveneens van toepassing op deze Overeenkomst.

## **7. Grensoverschrijdende overdracht van persoonsgegevens**

7.1 De MCB's zijn van toepassing op de overdracht of andere verwerking van Persoonsgegevens buiten de Europese Economische Ruimte (**EER**).

## **8. Subverwerkers**

8.1 De Verwerkingsverantwoordelijke verleent de Verwerker hierbij een algemene machtiging voor het inschakelen van een andere verwerker (subverwerker) voor de verwerking van de Persoonsgegevens. De Verwerker informeert de Verwerkingsverantwoordelijke over voorgenomen wijzigingen met betrekking tot de toevoeging of vervanging van andere verwerkers en stelt de Verwerkingsverantwoordelijke in de gelegenheid om bezwaar te maken tegen dergelijke wijzigingen binnen vijf dagen nadat de Verwerker de Verwerkingsverantwoordelijke alle gegevens over de andere verwerker heeft verstrekt;

8.2 De Verwerker mag een andere verwerker alleen toestemming geven om de Persoonsgegevens te verwerken indien:

- (a) de Verwerker met de andere verwerker een schriftelijke overeenkomst sluit die in wezen dezelfde voorwaarden bevat zoals in deze Overeenkomst zijn opgenomen, met name met betrekking tot het eisen van passende technische en organisatorische maatregelen op het gebied van de beveiliging van gegevens, en op schriftelijk verzoek van de Verwerkingsverantwoordelijke de

Verwerkingsverantwoordelijke kopieën van dergelijke overeenkomsten verstrekt;

- (b) de Verwerker de controle behoudt over alle Persoonsgegevens die hij aan de andere verwerker toevertrouwt; en
- (c) de overeenkomst van de andere verwerker eindigt automatisch bij beëindiging van deze Overeenkomst om welke reden dan ook.

8.3 Indien de andere verwerker zijn verplichtingen uit hoofde van een dergelijke schriftelijke overeenkomst niet nakomt, blijft de Verwerker volledig aansprakelijk jegens de Verwerkingsverantwoordelijke voor de nakoming door die andere verwerker van zijn verplichtingen uit hoofde van de overeenkomst.

8.4 De Partijen zijn van oordeel dat de Verwerker zeggenschap heeft over alle Persoonsgegevens die worden beheerd door of in het bezit zijn van zijn subverwerkers.

8.5 Op schriftelijk verzoek van de Verwerkingsverantwoordelijke controleert de Verwerker of een subverwerker zijn verplichtingen met betrekking tot de Persoonsgegevens van de Verwerkingsverantwoordelijke nakomt en verstrekt hij de resultaten van de audit aan de Verwerkingsverantwoordelijke.

## **9. Klachten, verzoeken van betrokkenen en rechten van derden**

9.1 De Verwerker moet zonder extra kosten de passende technische en organisatorische maatregelen nemen en de Verwerkingsverantwoordelijke onverwijld de informatie verstrekken die de Verwerkingsverantwoordelijke redelijkerwijs nodig heeft om te voldoen aan:

- (a) de rechten van de Betrokkenen in het kader van de Wetgeving Inzake Gegevensbescherming, met inbegrip van de toegangsrechten van de betrokkenen, het recht om persoonsgegevens te corrigeren en te wissen, bezwaar te maken tegen de verwerking en geautomatiseerde verwerking van persoonsgegevens en de verwerking van persoonsgegevens te beperken; en
- (b) informatie of beoordelingsberichten die in het kader van de Wetgeving Inzake Gegevensbescherming door een toezichthoudende autoriteit aan de Verwerkingsverantwoordelijke worden betekend.

9.2 De Verwerker moet de Verwerkingsverantwoordelijke zonder onnodige vertraging op de hoogte brengen als hij een klacht, kennisgeving of mededeling ontvangt die direct of indirect betrekking heeft op de verwerking van de Persoonsgegevens of op de naleving van de Wetgeving Inzake Gegevensbescherming door een van beide partijen.

9.3 De Verwerker moet de Verwerkingsverantwoordelijke binnen acht werkdagen op de hoogte brengen als hij van een Betrokkene een verzoek ontvangt om toegang tot zijn Persoonsgegevens of om een van zijn rechten uit hoofde van de Wetgeving Inzake Gegevensbescherming uit te oefenen.

9.4 De Verwerker verleent de Verwerkingsverantwoordelijke zijn volledige medewerking en ondersteuning bij het behandelen van klachten, kennisgevingen, mededelingen of verzoeken van de Betrokkene.

- 9.5 De Verwerker mag de Persoonsgegevens niet bekendmaken aan een Betrokkene of aan een derde partij anders dan op verzoek of instructie van de Verwerkingsverantwoordelijke, zoals bepaald in deze Overeenkomst of zoals vereist door de wet.

## **10. Informatieverplichting**

- 10.1 Voor zover het volgende van toepassing is, is het de verantwoordelijkheid van de Verwerkingsverantwoordelijke om de Betrokkenen ervan op de hoogte te stellen dat hun Persoonsgegevens kunnen worden gedeeld met **5.1.2.i** die deze gegevens gebruikt om een lijst bij te houden van alle aanvragen voor abonnementen, leningen en aankopen (de "Credit Application Previous Searches"), en dat de doeleinden voor het bijhouden van een dergelijke lijst zijn:
- Kredietrapportage en kredietwaardigheidscontrole;
  - Gegevensvalidatie, opschoning en verrijking van gegevens ten behoeve van klantenbeheer;
  - Traceerbaarheid en debiteurenbeheer;
  - Het voorkomen en opsporen van frauduleuze activiteiten;
  - Het verifiëren van gegevens voor identificatiedoeleinden; en
  - Statistische analyse, scores genereren (inclusief profilering) en modelleren.

## **11. Duur en beëindiging**

- 11.1 Deze Overeenkomst blijft volledig van kracht zolang:
- (a) de Raamovereenkomst van kracht blijft, of
  - (b) de Verwerker alle Persoonsgegevens met betrekking tot de Raamovereenkomst in zijn bezit of onder zijn beheer houdt (**Duur**).
- 11.2 Elke bepaling van deze Overeenkomst die uitdrukkelijk of impliciet van kracht wordt of blijft bij of na beëindiging van de Raamovereenkomst ter bescherming van Persoonsgegevens, blijft volledig van kracht.
- 11.3 Indien een wijziging in de Wetgeving Inzake Gegevensbescherming een van beide partijen verhindert om aan alle of een deel van haar verplichtingen uit hoofde van de Raamovereenkomst te voldoen, zullen de partijen de verwerking van Persoonsgegevens opschorten totdat die verwerking voldoet aan de nieuwe vereisten. Indien de partijen er niet in slagen om de verwerking van Persoonsgegevens binnen twee maanden in overeenstemming te brengen met de Wetgeving Inzake Gegevensbescherming, kunnen zij de Raamovereenkomst beëindigen met schriftelijke kennisgeving aan de andere partij.

## **12. Teruggave en vernietiging van gegevens**

- 12.1 Op verzoek van de Verwerkingsverantwoordelijke geeft de Verwerker de Verwerkingsverantwoordelijke een kopie van of toegang tot alle of een deel van de Persoonsgegevens in bezit of in beheer van de Verwerkingsverantwoordelijk in het format en op de door de Verwerkingsverantwoordelijke redelijkerwijs gespecificeerde media.

- 12.2 Bij beëindiging van de Raamovereenkomst, om welke reden dan ook of bij het verstrijken van de looptijd ervan, zal de Verwerker alle Persoonsgegevens met betrekking tot deze Overeenkomst in zijn bezit of onder zijn beheer veilig verwijderen of vernietigen, danwel op schriftelijk verzoek van de Verwerkingsverantwoordelijke teruggeven en niet bewaren, met uitzondering van één exemplaar dat hij slechts één jaar mag bewaren en gebruiken voor auditdoeleinden, tenzij in de Raamovereenkomst een langere periode of andere doeleinden zijn vastgelegd.
- 12.3 Indien een wet, voorschrift of overheid of regelgevende instantie de Verwerker verplicht documenten of materiaal te bewaren dat de Verwerker anders verplicht zou zijn terug te zenden of te vernietigen, stelt hij de Verwerkingsverantwoordelijke schriftelijk in kennis van die bewaarplicht, met vermelding van de documenten of materialen die hij moet bewaren, de wettelijke basis voor het bewaren en het vaststellen van een specifieke tijdslijn voor vernietiging zodra de bewaarplicht eindigt.
- 12.4 De Verwerker verklaart schriftelijk dat hij de Persoonsgegevens heeft vernietigd binnen 14 dagen nadat de vernietiging heeft plaatsgevonden.

### **13. Gegevens**

- 13.1 De Verwerker houdt gedetailleerde, nauwkeurige en actuele schriftelijke gegevens bij over elke verwerking van Persoonsgegevens die hij voor de Verwerkingsverantwoordelijke uitvoert, met inbegrip van, maar niet beperkt tot, de toegang tot, de controle en beveiliging van de Persoonsgegevens, erkende subverwerkers en gelieerde ondernemingen, de verwerkingsdoeleinden, categorieën van verwerking, elke overdracht van persoonsgegevens naar een derde land en de daarmee verband houdende waarborgen, en een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen waarnaar wordt verwezen in bepaling 5.1 (**Registratie**).
- 13.2 De Verwerker zorgt ervoor dat de registers toereikend zijn om de Verwerkingsverantwoordelijke in staat te stellen na te gaan of de Verwerker zijn verplichtingen uit hoofde van deze Overeenkomst nakomt, en de Verwerker verstrekt de Verwerkingsverantwoordelijke een kopie van de registers indien deze hierom verzoekt.
- 13.3 De Verwerkingsverantwoordelijke en de Verwerker moeten de in de Bijlagen van deze Overeenkomst vermelde gegevens eenmaal per jaar evalueren om de huidige nauwkeurigheid ervan te bevestigen en deze, indien nodig, bijwerken in het licht van de huidige omstandigheden.

### **14. Controle**

- 14.1 De Verwerker staat de Verwerkingsverantwoordelijke en andere door de Verwerkingsverantwoordelijke gemachtigde auditors toe om gedurende de looptijd van de Overeenkomst te controleren of de Verwerker zijn verplichtingen uit hoofde van de Overeenkomst nakomt, met inachtneming van een kennisgevingstermijn van ten minste 14 dagen. De Verwerker verleent de Verwerkingsverantwoordelijke en andere door de Verwerkingsverantwoordelijke gemachtigde auditors alle nodige assistentie om dergelijke audits uit te voeren.

- 14.2 Als er een Inbreuk op Persoonsgegevens plaatsvindt of als de Verwerker zich bewust wordt van een inbreuk op een van zijn verplichtingen uit hoofde van deze Overeenkomst of de Wetgeving Inzake Gegevensbescherming, zal de Verwerker:
- (a) zonder onnodige vertraging een eigen audit uitvoeren om de oorzaak vast te stellen;
  - (b) een schriftelijk verslag opstellen met gedetailleerde plannen om de in de audit vastgestelde tekortkomingen te verhelpen;
  - (c) de Verwerkingsverantwoordelijke een kopie van het schriftelijke auditverslag verstrekken; en
  - (d) de tijdens de audit vastgestelde tekortkomingen binnen 14 dagen verhelpen.
- 14.3 Op schriftelijk verzoek van de Verwerkingsverantwoordelijke zal de Verwerker:
- (a) een informatiebeveiligingscontrole uitvoeren voordat er begonnen wordt met de verwerking van Persoonsgegevens en deze controle jaarlijks herhalen;
  - (b) een schriftelijk verslag opstellen met gedetailleerde plannen om de bij de controle vastgestelde beveiligingstekortkomingen te verhelpen; en
  - (c) de Verwerkingsverantwoordelijke een kopie van het schriftelijke controleverslag verstrekken.
- 14.4 Op schriftelijk verzoek van de Verwerkingsverantwoordelijke stelt de Verwerker alle relevante auditrapporten aan de Verwerkingsverantwoordelijke ter beschikking. De Verwerkingsverantwoordelijke behandelt dergelijke auditrapporten in het kader van deze Overeenkomst als vertrouwelijke informatie van de Verwerker.
- 14.5 De Verwerker dient onmiddellijk de uitzonderingen die in de auditrapporten worden vermeld te verhelpen met behulp van de ontwikkeling en uitvoering van een corrigerend actieplan door het management van de Verwerker.

## 15. Garanties

### 15.1 De Verwerker verklaart dat:

- (a) haar werknemers, subverwerkers, agenten en alle andere personen die namens haar toegang hebben tot Persoonsgegevens, betrouwbaar zijn en de vereiste training hebben gevolgd met betrekking tot de Wetgeving Inzake Gegevensbescherming ten aanzien van Persoonsgegevens;
- (b) zij en iedereen die namens haar optreedt de Persoonsgegevens zal verwerken in overeenstemming met de Wetgeving Inzake Gegevensbescherming en andere wetten, verordeningen, beschikkingen, normen en andere soortgelijke instrumenten;
- (c) zij geen reden heeft om aan te nemen dat de Wetgeving Inzake Gegevensbescherming haar belet om diensten te verlenen in het kader van de Raamovereenkomst; en
- (d) rekening houdend met de huidige technologische omgeving en de implementatiekosten zij passende technische en organisatorische maatregelen zal nemen om de ongeoorloofde of onwettige verwerking van Persoonsgegevens en het onopzettelijk verlies, vernietiging of beschadiging van Persoonsgegevens te voorkomen en een passend beveiligingsniveau te waarborgen:
  - (i) de schade die het gevolg zou kunnen zijn van een dergelijke ongeoorloofde of onwettige verwerking of van een toevallig verlies, vernietiging of beschadiging;
  - (ii) de aard van de beschermde Persoonsgegevens; en
  - (iii) voldoen aan alle toepasselijke Wetgeving Inzake Gegevensbescherming en het informatie- en beveiligingsbeleid van de organisatie, met inbegrip van de in bepaling 5.1 vereiste beveiligingsmaatregelen.

### 15.2 De Verwerkingsverantwoordelijke verklaart dat het verwachte gebruik van de Persoonsgegevens door de Verwerker voor de Zakelijke Doeleinden en zoals specifiek opgedragen door de Verwerkingsverantwoordelijke in overeenstemming zal zijn met de Wetgeving Inzake Gegevensbescherming.

## 16. Kennisgeving

### 16.1 Elke kennisgeving of andere mededeling aan een partij onder of in verband met deze Overeenkomst dient schriftelijk te worden gedaan aan:

Voor de Verwerkingsverantwoordelijke Politie Eenheid Rotterdam,  
(naam bedrijf) DRIO  
(t.a.v.) 5.1.2.i  
(adres) Doelwater 5  
(adres) 3031AH Rotterdam (land)

Voor de Verwerker: 5.1.2.i .

T.a.v. Functionaris voor Gegevensbescherming  
Postbus 13128  
2501 EC Den Haag

- 16.2 Bepaling 15.1 is niet van toepassing op de betekening van procedures of andere documenten in een gerechtelijke procedure of, indien van toepassing, op arbitrage of een andere wijze van geschillenbeslechting.
- 16.3 Een kennisgeving op grond van deze overeenkomst is niet geldig indien deze per e-mail wordt verzonden.

Deze overeenkomst is gesloten op de datum die aan het begin van de overeenkomst is vermeld.

|                                                                                                                                                                                                                                                      |                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Ondertekend door een directeur</p> <p>voor en namens</p> <div data-bbox="188 860 847 898" style="border: 1px solid black; padding: 2px;">Politie Eenheid Rotterdam, drio</div> <p style="text-align: center;"><i>(volledige bedrijfsnaam)</i></p> | <div data-bbox="890 701 1394 987" style="background-color: #cccccc; text-align: center; font-size: 48px; color: red; font-weight: bold;">5.1.2.i</div> <p>Naam: 5.1.2.e _____</p> |
| <p>Ondertekend door een directeur</p> <p>voor en namens 5.1.2.i</p>                                                                                                                                                                                  | <p>Naam: 5.1.2.e</p>                                                                                                                                                              |

## BIJLAGE A Doeleinden en details van verwerking van persoonsgegevens

Onderwerp van verwerking:

Fraude preventie

Duur van verwerking:

zolang de overeenkomst loopt

Aard van verwerking:

data inventarisatie

Zakelijke doeleinden:

voorkomen en opsporen fraude

Categorieën van persoonsgegevens

voorletters, achternaam, geboorte datum, postcode, huisnummer

Soorten betrokkenen:

prive personen

Bevoegde personen:

Roger van Lith, Rob van Dijk

Identificeer de rechtsgrond van de Verwerker voor de verwerking van Persoonsgegevens buiten de EER om te voldoen aan de beperkingen van de grensoverschrijdende overdracht (kies er een):

- Gelegen in een land waarvan de toereikendheid op dit moment wordt vastgesteld (noem land): Nederland.
- Bindende bedrijfsregels.
- Standaardcontractbepalingen tussen de Verwerkingsverantwoordelijke als "gegevensexporteur" en de Verwerker als "gegevensimporteur".
- Standaardcontractbepalingen tussen de Verwerker als "gegevensexporteur" en de Verwerkingsverantwoordelijke of subverwerker als "gegevensimporteur".
- EU-VS-privacyschild gecertificeerd.
- Anders (geef in detail aan):  
.

## BESLUIT VAN DE COMMISSIE

### BIJLAGE B

#### MODELCONTRACTBEPALINGEN („VERWERKERS”)

Voor de toepassing van artikel 28, lid 3 sub c, van de Algemene Verordening Gegevensbescherming, voor de doorgifte van persoonsgegevens aan verwerkers die gevestigd zijn in derde landen die geen passend beschermingsniveau waarborgen

Naam van de organisatie die de gegevens uitvoert: 5.1.2.i

Adres: 5.1.2.i

Tel: +3170 5.1.2.i

E-mail: Info 5.1.2.i .com

(de **gegevensexporteur**)

en

Naam van de organisatie die de gegevens invoert: De gegevensimporteurs zijn opgenomen in Aanhangsel 4 Lijst van gegevensimporteurs.

(de **gegevensimporteur**)

elk afzonderlijk „partij” en gezamenlijk „de partijen” genoemd,

ZIJN OVEREENGEKOMEN de volgende contractbepalingen, hierna „de bepalingen” genoemd, vast te stellen teneinde voldoende waarborgen te bieden ten aanzien van de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, bij de doorgifte van de in aanhangsel 1 vermelde persoonsgegevens door de gegevensexporteur aan de gegevensimporteur.

## *Bepaling 1*

### **Definities**

Voor de toepassing van de bepalingen:

- a) gelden voor „persoonsgegevens”, „verwerken/verwerking”, „voor de verwerking verantwoordelijke”, „verwerker”, „betrokkene” en „toezichthoudende autoriteit” dezelfde definities als in de Algemene Verordening Gegevensbescherming (AVG) 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 <sup>(1)</sup>;
- b) wordt onder „gegevensexporteur” verstaan: de voor de verwerking verantwoordelijke die de persoonsgegevens doorgeeft;
- c) wordt onder „gegevensimporteur” verstaan: de verwerker die overeenkomt van de gegevensexporteur persoonsgegevens te ontvangen om deze na doorgifte namens de gegevensexporteur te verwerken in overeenstemming met zijn instructies en de voorwaarden van de bepalingen, en die niet onderworpen is aan een regeling van een derde land die passende bescherming biedt in de zin van artikel 46, lid 3 sub a, van de AVG;
- d) wordt onder „subverwerker” verstaan: een verwerker die door de gegevensimporteur of een andere voor de gegevensimporteur werkende subverwerker is gecontracteerd en die overeenkomt van de gegevensimporteur of van een andere voor de gegevensimporteur werkende subverwerker persoonsgegevens te ontvangen, uitsluitend ten behoeve van de verwerkingsactiviteiten die namens de gegevensexporteur worden verricht na de doorgifte, overeenkomstig de instructies van de gegevensexporteur, de voorwaarden van de bepalingen en de voorwaarden van het schriftelijke contract inzake subverwerking;
- e) wordt onder „toepasselijk recht inzake gegevensbescherming” verstaan: de wettelijke bepalingen ter bescherming van de fundamentele rechten en vrijheden van personen, en met name hun recht op bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens, die in de lidstaat van vestiging van de gegevensexporteur van toepassing zijn op een voor de verwerking verantwoordelijke;
- f) wordt onder „technische en organisatorische beveiligingsmaatregelen” verstaan: maatregelen die tot doel hebben persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking de doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking.

## *Bepaling 2*

### **Bijzonderheden betreffende de doorgifte**

De bijzonderheden betreffende de doorgifte, van persoonsgegevens worden nader omschreven in aanhangsel 1, dat een integrerend deel van de bepalingen vormt.

## *Bepaling 3*

### **Derdenbeding**

1. De betrokkenen kunnen deze bepaling en bepaling 4, onder b) tot en met i), bepaling 5, onder a) tot en met e) en g) tot en met j), bepaling 6, leden 1 en 2, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 als derde begunstigen tegenover de gegevensexporteur afdwingen.
2. De betrokkenen kunnen deze bepaling, bepaling 5, onder a) tot en met e) en onder g), bepaling 6, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 tegenover de gegevensimporteur afdwingen in gevallen waarin de gegevensexporteur feitelijk is verdwenen of heeft opgehouden rechtens te bestaan, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen en daardoor de rechten en verplichtingen van de gegevensexporteur op zich neemt; in dit geval kunnen betrokkenen de genoemde bepalingen tegenover deze rechtsopvolger afdwingen.
3. De betrokkenen kunnen deze bepaling, bepaling 5, onder a) tot en met e) en onder g), bepaling 6, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 tegenover de subverwerker afdwingen in die gevallen waarin zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen en daardoor de rechten en verplichtingen van de gegevensexporteur op zich neemt; in dat geval kunnen betrokkenen de genoemde bepalingen tegenover deze rechtsopvolger afdwingen. Deze aansprakelijkheid van de

<sup>1</sup> De partijen kunnen in deze bepaling de definities en begrippen van de Algemene Verordening Gegevensbescherming herhalen, indien zij de voorkeur geven aan een autonoom contract.

subverwerker jegens derden blijft beperkt tot de verwerkingswerkzaamheden die deze zelf heeft uitgevoerd krachtens de bepalingen.

4. De partijen verzetten zich er niet tegen dat de betrokkenen door een vereniging of andere instelling worden vertegenwoordigd, indien de betrokkenen dit uitdrukkelijk wensen en dit in het nationale recht is toegestaan.

#### *Bepaling 4*

#### **Verplichtingen van de gegevensexporteur**

De gegevensexporteur stemt ermee in en garandeert dat:

- a) de verwerking van de persoonsgegevens, met inbegrip van de doorgifte zelf, is geschied en zal blijven geschieden in overeenstemming met alle relevante bepalingen van het toepasselijke recht inzake gegevensbescherming (en, waar van toepassing, is gemeld aan de betrokken autoriteiten van de lidstaat waar de gegevensexporteur is gevestigd), en dat zij niet in strijd is met de toepasselijke bepalingen van die staat;
- b) hij de gegevensimporteur instructie heeft gegeven, en gedurende de verwerking van de persoonsgegevens zal geven, de persoonsgegevens uitsluitend namens de gegevensexporteur en in overeenstemming met het toepasselijke recht inzake gegevensbescherming en de bepalingen te verwerken;
- c) de gegevensimporteur voldoende waarborgen zal bieden ten aanzien van de technische en organisatorische beveiligingsmaatregelen die in aanhangsel 2 bij dit contract worden omschreven;
- d) deze beveiligingsmaatregelen, na een beoordeling van de vereisten van het toepasselijke recht inzake gegevensbescherming, geschikt zijn bevonden om persoonsgegevens te beschermen tegen vernietiging, hetzij bij ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens via een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking, en deze maatregelen gezien de aard van de verwerking en de aard van de te beschermen gegevens verbonden risico's een passend beveiligingsniveau waarborgen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging;
- e) hij op de naleving van deze beveiligingsmaatregelen zal toezien;
- f) in het eventuele geval van de doorgifte bijzondere categorieën gegevens betreft, de betrokkene ervan in kennis is gesteld, of vóór of zo spoedig mogelijk na de doorgifte ervan in kennis zal worden gesteld, dat zijn gegevens kunnen worden doorgegeven naar een derde land dat geen passende bescherming biedt als bedoeld in de Algemene Verordening Gegevensbescherming;
- g) hij overeenkomstig bepaling 5, onder b), en bepaling 8, lid 3, ontvangen kennisgevingen van de gegevensimporteur of een subverwerker aan de toezichthoudende autoriteit zal doorzenden, wanneer hij (dat wil zeggen de gegevensexporteur) besluit de doorgifte voort te zetten of de opschorting op te heffen;
- h) hij op verzoek een afschrift van de bepalingen ter beschikking van de betrokkene zal stellen, met uitzondering van aanhangsel 2, alsmede een beknopte beschrijving van de beveiligingsmaatregelen en een afschrift van elk contract voor subverwerkingsdiensten dat overeenkomstig de bepalingen dient te worden opgesteld; indien de bepalingen of het contract commerciële informatie bevatten, mag de gegevensexporteur deze commerciële informatie verwijderen;
- i) in geval van subverwerking de verwerkingsactiviteiten worden uitgevoerd overeenkomstig bepaling 11 door een subverwerker die ten minste hetzelfde beschermingsniveau voor de persoonsgegevens en de rechten van de betrokkenen waarborgt als de gegevensimporteur overeenkomstig deze bepalingen; en
- j) hij zal toezien op de naleving van bepaling 4, onder a) tot en met i).

**Verplichtingen van de gegevensimporteur <sup>(2)</sup>**

De gegevensimporteur stemt ermee in en garandeert dat:

- a) hij de persoonsgegevens uitsluitend namens de gegevensexporteur en in overeenstemming met diens instructies en met de bepalingen verwerkt; indien hij om welke reden dan ook daartoe niet in staat is, stemt hij ermee in de gegevensexporteur onverwijld daarvan in kennis te stellen, in welk geval de gegevensexporteur de gegevensdoorgifte mag opschorten en/of het contract mag beëindigen;
- b) hij geen reden heeft aan te nemen dat de op hem toepasselijke wetgeving hem belet de van de gegevensexporteur ontvangen instructies en zijn verplichtingen krachtens het contract na te komen, en dat hij in geval van een wijziging in deze wetgeving die in aanzienlijke mate afbreuk dreigt te doen aan de in de bepalingen opgenomen waarborgen en verplichtingen, de gegevensexporteur, zodra hij de wijziging kent, onverwijld daarvan in kennis stelt, in welk geval de gegevensexporteur de gegevensdoorgifte mag opschorten en/of het contract mag beëindigen;
- c) hij de in aanhangsel 2 omschreven technische en organisatorische beveiligingsmaatregelen vóór de verwerking van de doorgegeven persoonsgegevens heeft getroffen;
- d) hij de gegevensexporteur onverwijld ervan in kennis stelt wanneer:
  - i) een wetshandhavingsinstantie een juridisch bindend verzoek om verstrekking van persoonsgegevens heeft gedaan, tenzij deze kennisgeving anderszins is verboden, zoals een strafrechtelijk verbod dat ten doel heeft de vertrouwelijkheid van een wetshandhavingsonderzoek te bewaren;
  - ii) iemand per ongeluk of op ongeoorloofde wijze toegang tot de gegevens heeft gehad;
  - iii) hij van de betrokkenen rechtstreeks een verzoek heeft ontvangen, waarop hij niet ingaat, tenzij hem dit anderszins is toegestaan;
- e) hij alle vragen van de gegevensexporteur betreffende de door hem uitgevoerde verwerking van de doorgegeven persoonsgegevens zo spoedig mogelijk naar behoren beantwoordt en het advies van de toezichthoudende autoriteit volgt bij de verwerking van de doorgegeven gegevens;
- f) hij op verzoek van de gegevensexporteur zijn verwerkingsvoorzieningen beschikbaar stelt voor controle van de onder deze bepalingen vallende verwerkingsactiviteiten, welke wordt uitgevoerd door de gegevensexporteur of door een controleorgaan waarvan de leden onafhankelijk zijn, over de vereiste beroepskwalificaties beschikken, tot geheimhouding verplicht zijn en door de gegevensexporteur worden aangewezen, waar van toepassing in overleg met de toezichthoudende autoriteit;
- g) hij, wanneer de betrokkene geen afschrift van de gegevensexporteur kan verkrijgen, hem op verzoek een afschrift van de bepalingen alsmede eventuele subverwerkingscontracten ter beschikking stelt, met uitzondering van aanhangsel 2 dat door een beknopte beschrijving van de beveiligingsmaatregelen wordt vervangen; indien de bepalingen of contracten commerciële informatie bevatten, mag de gegevensimporteur deze commerciële informatie verwijderen;
- h) hij, wanneer subverwerking plaatsvindt, de gegevensexporteur tevoren heeft ingelicht en diens schriftelijke toestemming heeft verkregen;
- i) de verwerkdiensten van de subverwerker overeenkomstig bepaling 11 zullen worden uitgevoerd;

---

2. Vereisten van het nationale recht die op de gegevensimporteur van toepassing zijn en die niet verder gaan dan wat in een democratische samenleving noodzakelijk is op basis van een van de in artikel 46, lid 4, van de Algemene Verordening Gegevensbescherming vermelde belangen, dat wil zeggen noodzakelijke maatregelen ter vrijwaring van de veiligheid van een staat, de landsverdediging, de openbare veiligheid, het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of schendingen van de beroepscodes voor gereguleerde beroepen, een belangrijk economisch en financieel belang van een lidstaat of de bescherming van de betrokkene of van de rechten en vrijheden van anderen, zijn niet in strijd met de bepalingen. Enkele voorbeelden van dergelijke vereisten die niet verder gaan dan wat in een democratische samenleving noodzakelijk is, zijn internationaal erkende sancties, verplichtingen in verband met de belastingaangifte en verplichtingen in verband met het melden van witwaspraktijken.

- j) hij van elk subverwerkingscontract dat hij in het kader van de bepalingen aangaat, onverwijld een afschrift doet toekomen aan de gegevensexporteur.

#### *Bepaling 6*

##### **Aansprakelijkheid**

1. De partijen komen overeen dat elke betrokkene die ten gevolge van een schending van de verplichtingen bedoeld in bepaling 3 of bepaling 11 door een partij of een subverwerker schade heeft geleden, het recht heeft van de gegevensexporteur vergoeding voor de geleden schade te ontvangen.

2. Wanneer de betrokkene geen vordering tot schadevergoeding wegens niet-nakoming door de gegevensimporteur of diens subverwerker van een van de in bepaling 3 of bepaling 11 bedoelde verplichtingen, als bedoeld in lid 1, tegen de gegevensexporteur kan instellen doordat de gegevensexporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, stemt de gegevensimporteur ermee in dat de betrokkene een vordering kan instellen tegen de gegevensimporteur alsof hij de gegevensexporteur was, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen, in welk geval de betrokkene zijn rechten tegenover die rechtsopvolger kan doen gelden.

De gegevensimporteur kan zich niet aan zijn aansprakelijkheid onttrekken door zich te beroepen op niet-nakoming van verplichtingen door de subverwerker.

3. Wanneer de betrokkene de in lid 1 of 2 bedoelde vordering wegens niet-nakoming door de subverwerker van een van de in bepaling 3 of bepaling 11 bedoelde verplichtingen niet tegen de gegevensexporteur of de gegevensimporteur kan instellen doordat zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, stemt de subverwerker ermee in dat de betrokkene een vordering kan instellen tegen de subverwerker, met betrekking tot diens eigen verwerkingsactiviteiten krachtens de bepalingen, alsof deze de gegevensexporteur of de gegevensimporteur was, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen, in welk geval de betrokkene zijn rechten tegenover die rechtsopvolger kan doen gelden. De aansprakelijkheid van de subverwerker blijft beperkt tot de verwerkingsactiviteiten die deze zelf heeft uitgevoerd krachtens de bepalingen.

#### *Bepaling 7*

##### **Bemiddeling en rechtsmacht**

1. De gegevensimporteur stemt ermee in dat, indien de betrokkene tegen hem rechten ten behoeve van derden en/of vorderingen tot schadevergoeding krachtens de bepalingen inroept, de gegevensimporteur de beslissing van de betrokkene aanvaardt:

a) om het geschil te onderwerpen aan bemiddeling door een onafhankelijke persoon of, waar van toepassing, door de toezichthoudende autoriteit;

b) om het geschil voor te leggen aan een rechterlijke instantie in de lidstaat waar de gegevensexporteur is gevestigd.

2. De partijen komen overeen dat de door de betrokkene gemaakte keuze geen afbreuk doet aan diens materiële of formele rechten om op grond van andere bepalingen van nationaal of internationaal recht verhaal te zoeken.

#### *Bepaling 8*

##### **Samenwerking met de toezichthoudende autoriteiten**

1. De gegevensexporteur stemt ermee in een afschrift van dit contract bij de toezichthoudende autoriteit neer te leggen, indien deze daarom verzoekt of indien dit krachtens het toepasselijke recht inzake gegevensbescherming vereist is.

2. De partijen komen overeen dat de toezichthoudende autoriteit bevoegd is bij de gegevensimporteur en eventuele subverwerkers een controle te verrichten die dezelfde reikwijdte heeft en aan dezelfde voorwaarden is onderworpen als die welke krachtens het toepasselijke recht inzake gegevensbescherming voor haar controle van de gegevensexporteur zouden gelden.

3. Indien er wetgeving bestaat die op de gegevensimporteur of een subverwerker van toepassing is en die de uitvoering van controles als in lid 2 bedoeld op de gegevensimporteur of een subverwerker verbiedt, stelt de gegevensimporteur de gegevensexporteur daarvan onverwijld in kennis. In een dergelijk geval mag de gegevensexporteur de in bepaling 5, onder b), bedoelde maatregelen nemen.

#### *Bepaling 9*

#### **Toepasselijk recht**

Op de bepalingen is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing, te weten Nederland.

#### *Bepaling 10*

#### **Wijziging van het contract**

De partijen verbinden zich ertoe de bepalingen niet te wijzigen. Dit vormt voor de partijen geen beletsel om indien nodig bepalingen toe te voegen betreffende met de transactie verband houdende vraagstukken, mits deze niet met de modelcontractbepalingen in strijd zijn.

#### *Bepaling 11*

#### **Subverwerking**

1. De gegevensimporteur besteedt de verwerkingsactiviteiten die hij overeenkomstig de bepalingen namens de gegevensexporteur uitvoert, niet uit zonder de voorafgaande schriftelijke toestemming van de gegevensexporteur. Indien de gegevensimporteur met toestemming van de gegevensexporteur zijn verplichtingen uit hoofde van de bepalingen uitbestedt, dient hij met de subverwerker een schriftelijk contract te sluiten waarbij aan de subverwerker dezelfde verplichtingen worden opgelegd als die waaraan de gegevensimporteur uit hoofde van de bepalingen moet voldoen<sup>3</sup>. Indien de subverwerker niet voldoet aan zijn verplichtingen tot gegevensbescherming uit hoofde van dat schriftelijke contract, blijft de gegevensimporteur jegens de gegevensexporteur volledig aansprakelijk voor de uitvoering van de verplichtingen van de subverwerker uit hoofde van dat contract.

2. In het tevoren tussen de gegevensimporteur en de subverwerker te sluiten schriftelijke contract dient tevens een derdenbeding te zijn opgenomen zoals vervat in bepaling 3, dat voorziet in gevallen dat de betrokkene geen vordering tot schadevergoeding als bedoeld in bepaling 6, lid 1, kan instellen tegen de gegevensexporteur of de gegevensimporteur omdat deze feitelijk zijn verdwenen, hebben opgehouden rechtens te bestaan of insolvent zijn geworden, en er geen rechtsopvolger is die contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen. Deze aansprakelijkheid van de subverwerker jegens derden blijft beperkt tot de verwerkingswerkzaamheden die deze zelf heeft uitgevoerd krachtens de bepalingen.

3. Op de in lid 1 bedoelde bepalingen betreffende de gegevensbeschermingsaspecten van de subverwerking uit hoofde van het in lid 1 bedoelde contract is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing, te weten Nederland. De gegevensexporteur houdt een lijst bij van subverwerkingscontracten die krachtens de bepalingen zijn gesloten en door de gegevensimporteur overeenkomstig bepaling 5, onder j), zijn aangemeld, en werkt deze ten minste eenmaal per jaar bij. Deze lijst wordt ter beschikking gesteld van de toezichthoudende autoriteit voor gegevensbescherming die op de gegevensexporteur toezicht houdt.

#### *Bepaling 12*

#### **Verplichting na de beëindiging van de verwerking van persoonsgegevens**

1. De partijen komen overeen dat de gegevensimporteur en de subverwerker na het beëindigen van de verlening van de gegevensverwerkingsdiensten alle doorgegeven persoonsgegevens en kopieën daarvan aan de gegevensexporteur terugbezorgen of, indien de gegevensexporteur dat verkiest, alle persoonsgegevens vernietigen en aan de gegevensexporteur verklaren dat de vernietiging heeft plaatsgevonden, tenzij de op de gegevensimporteur toepasselijke wetgeving hem verbiedt alle of een gedeelte van de doorgegeven persoonsgegevens terug te bezorgen of te vernietigen. In dat geval garandeert de gegevensimporteur dat hij de vertrouwelijkheid van de doorgegeven persoonsgegevens zal respecteren en dat hij de doorgegeven gegevens niet verder actief zal verwerken.

2. De gegevensimporteur en de subverwerker garanderen dat zij op verzoek van de gegevensexporteur en/of de toezichthoudende autoriteit hun verwerkingsvoorzieningen voor een controle van de in lid 1 bedoelde maatregelen beschikbaar zullen stellen.

#### *Bepaling 13*

#### **Startdatum overeenkomst**

Deze overeenkomst heeft als ingangsdatum 25 mei 2018 ongeacht de bij ondertekening vermelde data.

---

<sup>3</sup> Aan deze eis kan worden voldaan door medeondertekening door de subverwerker van het contract tussen de gegevensexporteur en de gegevensimporteur dat krachtens dit besluit wordt gesloten.

## Bij de modelcontractbepalingen

Dit aanhangsel maakt deel uit van de bepalingen en moet door de partijen worden ingevuld en ondertekend.

De lidstaten kunnen overeenkomstig hun nationale procedures aanvullende of meer gedetailleerde gegevens voorschrijven die in dit aanhangsel moeten worden opgenomen.

### Gegevensexporteur

De gegevensexporteur is:

5.1.2.i ., van tijd tot tijd gebruikmakend van de diensten, het personeel en de infrastructuur in eigendom van, geëxploiteerd door of in dienst van de gegevensimporteur(s) om de activiteiten van de gegevensexporteur te ondersteunen.

### Gegevensimporteur

De gegevensimporteur zijn:

Elke gegevensimporteur behoort tot de 5.1.2.i groepsmaatschappijen, die van tijd tot tijd hun infrastructuur, personeel en diensten ter beschikking om de activiteiten van de gegevensexporteur te ondersteunen.

### Betrokkenen

De doorgegeven persoonsgegevens betreffen de volgende categorieën betrokkenen:

- individuele klanten, medewerkers en contractanten van de van de klanten van de gegevensexporteur;
- bestuurders en aandeelhouders van commerciële entiteiten en eenmanszaken of partners;
- derden die een commerciële relatie hebben of kunnen krijgen met de gegevensexporteur (bijvoorbeeld adverteerders, leveranciers, dienstverleners en contractanten) en hun vertegenwoordigers;

### Categorieën gegevens

De doorgegeven persoonsgegevens betreffen de volgende categorieën gegevens:

- namen, eerdere namen, geboortedata, adres, vorige adressen, e-mailadressen, mobiele telefoonnummers en andere contactinformatie;
- de persoonsgegevens gegenereerd, gedeeld en geüpload door of over personen die de diensten van de dataexporteur of de klanten van de dataexporteur of data leveranciers bezoeken, toegang hebben tot, gebruiken of er anderszins mee communiceren;
- financiële informatie;
- de persoonsgegevens van het personeel van de gegevensexporteur die zijn gegenereerd tijdens de personeelsadministratie;
- persoonsgegevens met betrekking tot of van externe derden waarmee de gegevensexporteur een commerciële relatie heeft of kan krijgen;
- andere persoonsgegevens in documenten of in elektronische vorm;
- informatie van externe partners (zoals informatie met betrekking tot gezamenlijk aangeboden diensten of gebruik van diensten van derden);
- informatie van gelieerde ondernemingen van de gegevensexporteur en bedrijven in de 5.1.2.i -groep;
- persoonsgegevens die worden gehouden op systemen die eigendom zijn van of zijn gecontracteerd door de gegevensexporteur zoals in e-mails, servers in datacentra, in de cloud, op computers en in bestandenopslag en systemen die internetverkeerinformatie bevatten;
- informatie van of over derden die commerciële afspraken hebben of kunnen maken met de gegevensexporteur (en hun vertegenwoordigers), inclusief informatie in CRM- en leveranciersbeheersystemen van de gegevensexporteur die worden ondersteund of verstrekt door de gegevensimporteur.

### Bijzondere categorieën gegevens (indien van toepassing)

- Niet van Toepassing

## **Verwerking**

De doorgegeven persoonsgegevens zullen de volgende basisverwerkingen ondergaan:

De verwerking van persoonsgegevens door de gegevensimporteurs is uitsluitend gericht op het verlenen van ondersteuning en diensten aan de gegevensexporteurs. Om ondersteuning en diensten aan te bieden wordt er persoonlijke data gehost, geopend en verwerkt door of namens de gegevensimporteurs. Afhankelijk van de ondersteuning of diensten die worden aangeboden, omvat het type verwerking dat de dataimporteur zal uitvoeren onder meer gegevensverwerking, productafhandeling, servicelevering, operationele ondersteuning, testen, onderzoek, analyse en voor algemene ondersteuningsdoeleinden.

---

**Bij de modelcontractbepalingen**

Dit aanhangsel maakt deel uit van de bepalingen en moet door de partijen worden ingevuld en ondertekend.

**Beschrijving van de technische en organisatorische beveiligingsmaatregelen die door de gegevensimporteur overeenkomstig bepaling 4, onder d), en bepaling 5, onder c), zijn getroffen (of bijgevoegd(e) document/wettelijke regeling):**

Beide partijen zullen zich houden aan het informatie en securitybeleid van 5.1.2.i dat bestaat uit vertrouwelijke en interne documenten van 5.1.2.i

---

(<sup>1</sup>) De bepaling inzake aansprakelijkheid is facultatief.

APPENDIX 3 LIJST VAN DATA EXPORTEURS

| NAME OF DATA EXPORTER | REGISTERED ADDRESS | TELEPHONE NUMBER | FAX NUMBER | EMAIL ADDRESS |
|-----------------------|--------------------|------------------|------------|---------------|
| 5.1.2.i               |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |

APPENDIX 4 LIJST VAN DATA IMPORTEURS

| NAME OF DATA IMPORTER | REGISTERED ADDRESS | TELEPHONE NUMBER | FAX NUMBER | EMAIL ADDRESS |
|-----------------------|--------------------|------------------|------------|---------------|
| <div>5.1.2.i</div>    |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |
|                       |                    |                  |            |               |

**Van:** 5.1.2.e  
**Aan:** 5.1.2.e 5.1.  
**Onderwerp:** RE: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf  
**Datum:** woensdag 10 maart 2021 15:58:58

---

Hoi,

Bedankt!

**Met vriendelijke groeten,**

5.1.2.e

**Adviseur bedrijfsvoering Staf en DRIO**

Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Doelwater 5,  
 3011AH Rotterdam

06 5.1.2.e

Vrijdag is mijn roostervrije dag

5.1.2.e

[@politie.nl](mailto:5.1.2.e@politie.nl)

---

**Van:** 5.1.2.e 5.1.2.e

**Verzonden:** woensdag 10 maart 2021 15:55

**Aan:** 5.1.2.e 5.1.2.e <[5.1.2.e@politie.nl](mailto:5.1.2.e@politie.nl)>

**Onderwerp:** RE: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

Hoi 5.1.2.e

Jazeker, het mailadres van het inkooploket is [5.1.2.i@politie.nl](mailto:5.1.2.i@politie.nl)

Met vriendelijke groet,

5.1.2.e 5.1.2.e

5.1.2.e

06 – 5.1.2.e

Werkdagen: ma, di, wo en do

Politie | PDC | Dienst Facility Management | Team Bedrijfsadministratie  
 Prins Frederik Hendrikstraat 40, 3051ES Rotterdam

Meer informatie? Kijk op [politie.nl](https://politie.nl)

5.1.2.i

[@politie.nl](mailto:5.1.2.i@politie.nl)

---

**Van:** 5.1.2.e

**Verzonden:** woensdag 10 maart 2021 15:51

**Aan:** 5.1.2.e 5.1.2.e <[5.1.2.5.1.2.e@politie.nl](mailto:5.1.2.5.1.2.e@politie.nl)>

**Onderwerp:** RE: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

Hoi,

Heb ik weer 😊 Ja klopt zo heb ik het indertijd voor RTD ook zo gedaan voor 5.1.2.i

Alleen nu is de vraag inderdaad stel dat alle rtic's dit willen dan, dus ik begrijp dat je de collega adviseert om alles wat zij landelijk willen gaan gebruiken via het inkoop loket aan te geven.

Heb jij dan een mail adres wat ik door kan geven voor de collega's in het land?

Bedankt!

Met vriendelijke groeten,

5.1.2.e

**Adviseur bedrijfsvoering Staf en DRIO**

Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Doelwater 5,  
3011AH Rotterdam

06-5.1.2.e

Vrijdag is mijn roostervrije dag

5.1.2.e

@politie.nl

---

**Van:** 5.1.2.e 5.1.2.e

**Verzonden:** woensdag 10 maart 2021 14:53

**Aan:** 5.1.2.e 5.1.2.e @politie.nl>

**Onderwerp:** RE: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

Hoi 5.1.2.e ,

Tja, dat is een lastige. Het is geen abonnement op een tijdschrift, maar op een dienst. Die vallen niet onder het contract abonnementen. Voor tijdschriften is er namelijk wel een landelijk contract: LM Information Delivery.

Omdat 5.1.2.i landelijk gebruikt wordt, zou ik adviseren dit via het Inkooploket te doen. Die zullen waarschijnlijk adviseren een regionaal contract af te sluiten omdat de jaar-spend niet boven de aanbestedingsgrens uitkomt. Voor hun is het wel handig te weten dat dit landelijk speelt en ooit een keer aanbesteed zal moeten worden.

Met vriendelijke groet,

5.1.2.e 5.1.2.e

5.1.2.e

06 – 5.1.2.e

Werkdagen: ma, di, wo en do

Politie | PDC | Dienst Facility Management | Team Bedrijfsadministratie  
Prins Frederik Hendrikstraat 40, 3051ES Rotterdam

Meer informatie? Kijk op [politie.nl](https://politie.nl)

5.1.2.i

@politie.nl

---

**Van:** 5.1.2.e

**Verzonden:** woensdag 10 maart 2021 14:08

**Aan:** 5.1.2.e 5.1.2.e <5.1.2.5.1.2.e@politie.nl>

**Onderwerp:** FW: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

Met vriendelijke groeten,

5.1.2.e

**Adviseur bedrijfsvoering Staf en DRIO**

Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Doelwater 5,  
3011AH Rotterdam

06-5.1.2.e

Vrijdag is mijn roostervrije dag

5.1.2.e

[@politie.nl](mailto:5.1.2.e@politie.nl)

---

**Van:** 5.1.2.e

**Verzonden:** dinsdag 12 januari 2021 08:56

**Aan:** 5.1.2.e ' <5.1.2.e@5.1.2.i.com>; 5.1.2.e ' <5.1.2.e@5.1.2.i.com>

5.1.2.e

**CC:** 5.1.2.e 5.1.2.e [@politie.nl](mailto:5.1.2.e@politie.nl)>

**Onderwerp:** RE: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

Goedemorgen,

Zoals vorige week afgesproken stuur ik hierbij de getekende overeenkomsten toe..  
Indien er nog vragen zijn hoor ik het graag, ik hoop dat alles hiermee weer goed geregeld is!

Prettige werkdag!

**Met vriendelijke groeten,**

5.1.2.e

**Adviseur bedrijfsvoering DRIO**

Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Doelwater 5,  
3011AH Rotterdam

06-5.1.2.e

Vrijdag is mijn roostervrije dag

5.1.2.e

[@politie.nl](mailto:5.1.2.e@politie.nl)

---

**Van:** 5.1.2.e [<mailto:5.1.2.e@5.1.2.i.com>]

**Verzonden:** donderdag 7 januari 2021 14:59

**Aan:** 5.1.2.e <5.1.2.e@politie.nl>

**Onderwerp:** RE: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

Hallo,

Natuurlijk, zie bijlage,

Met vriendelijke groet, Kind regards,

5.1.2.e

Receptionist | *Corporate Services*

Grote Marktstraat 49 | 2511 BH Den Haag | Tel - +31 70 440 4000

5.1.2.e

@5.1.2.i .com  
[www.5.1.2.i .nl](http://www.5.1.2.i.nl)

*Niet aanwezig op vrijdag*

*Out of office on Friday*

**Next annual leave:**

**Januari 12**

5.1.2.i

**From:** 5.1.2.e <5.1.2.e@politie.nl>

**Sent:** 07 January 2021 14:48

**To:** 5.1.2.e 5.1.2.e @5.1.2.i .com>

**Subject:** [EXTERNAL] RE: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

**Security First:** External email, use caution clicking links or opening attachments

Hoi,

Willen jullie nog even het telefoonnummer van 5.1.2.e aanpassen nu staat mijn nummer daar?..  
06-5.1.2.e

**Met vriendelijke groeten,**

5.1.2.e

**Adviseur bedrijfsvoering DRIO**

Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Doelwater 5,  
3011AH Rotterdam

06-5.1.2.e

Vrijdag is mijn roostervrije dag

5.1.2.e

@politie.nl

**Van:** 5.1.2.e [mailto:5.1.2.e@5.1.2.i.com]

**Verzonden:** donderdag 7 januari 2021 14:44

**Aan:** 5.1.2.e <5.1.2.e@politie.nl>; 5.1.2.e  
5.1.2.e@5.1.2.i.com>

**CC:** 5.1.2.e@politie.nl>

**Onderwerp:** RE: DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

Beste 5.1.2.e

Dank voor het mailen van de DPA verwerkersovereenkomst, deze is correct ingevuld.  
In de bijlage de aangepast PPU opdrachtbevestiging ter ondertekening.

Met vriendelijke groet, Kind regards,

5.1.2.e

Receptionist | Corporate Services

Grote Marktstraat 49 | 2511 BH Den Haag | Tel - +31 70 440 4000

5.1.2.e@experian.com  
[www.5.1.2.i.nl](http://www.5.1.2.i.nl)

*Niet aanwezig op vrijdag*

*Out of office on Friday*

**Next annual leave:**

**Januari 12**

5.1.2.i

---

**From:** 5.1.2.e ) <5.1.2.e@politie.nl>

**Sent:** 07 January 2021 13:54

**To:** 5.1.2.e 5.1.2.e@5.1.2.i.com>; 5.1.2.e  
5.1.2.e@5.1.2.i.com>

Cc: 5.1.2.e 5.1.2.e @politie.nl>

Subject: [EXTERNAL] DPA 5.1.2.i NL DUTCH with model clauses\_v05June2020 invulbare versie.pdf

**Security First:** External email, use caution clicking links or opening attachments

Zoals vanmorgen besproken met jullie collega, graag een laatste controle op deze overeenkomst. Jullie zorgen dan voor aangepast contract met de juiste gegevens, zodat ik dit kan laten tekenen door 5.1.2.e 5.1.2.e  
Hier de gevraagde gegevens.

Het KVK nummer is 5.1.2.i

Het factuuradres is:  
5.1.2.i @politie.nl

Politie  
t.a.v. team Crediteuren  
Postbus 33137  
3005 EC Rotterdam

**Met vriendelijke groeten,**

5.1.2.e  
**Adviseur bedrijfsvoering DRIO**  
Nationale Politie | Eenheid Rotterdam | Staf | Bestuursondersteuning

Doelwater 5,  
3011AH Rotterdam  
06-5.1.2.e  
Vrijdag is mijn roostervrije dag

5.1.2.e @politie.nl

----- Disclaimer -----

De informatie verzonden met dit e-mailbericht (en bijlagen) is uitsluitend bestemd voor de geadresseerde(n) en zij die van de geadresseerde(n) toestemming kregen dit bericht te lezen. Kennisneming door anderen is niet toegestaan.

De informatie in dit e-mailbericht (en bijlagen) kan vertrouwelijk van aard zijn en binnen het bereik van een geheimhoudingsplicht en/of een verschoningsrecht vallen.

Indien dit e-mailbericht niet voor u bestemd is, wordt u verzocht de afzender daarover onmiddellijk te informeren en het e-mailbericht (en bijlagen) te vernietigen.

Conform het beveiligingsbeleid van de Politie wordt e-mail van en naar de politie gecontroleerd op virussen, spam en phishing en moet deze e-mail voldoen aan de voor de overheid verplichte mailbeveiligingsstandaarden die zijn vastgesteld door het Forum Standaardisatie.

Mail die niet voldoet aan het beveiligingsbeleid kan worden geblokkeerd waardoor deze de

geadresseerde niet bereikt. De geadresseerde wordt hiervan niet in kennis gesteld.

-----  
The information sent in this E-mail message (including any attachments) is exclusively intended for the individual(s) to whom it is addressed and for the individual(s) who has/have had permission from the recipient(s) to read this message.

Access by others is not permitted.

The information in this E-mail message (including any attachments) may be of a confidential nature and may form part of the duty of confidentiality and/or the right of non-disclosure.

If you have received this E-mail message in error, please notify the sender without delay and delete the E-mail message (including any attachments).

In conformity with the security policy of the Police, E-mails from and to the Police are checked for viruses, spam and phishing and this E-mail must meet the standards of the government-imposed E-mail security as set by the Standardization Forum.

Any E-mail failing to meet said security policy may be blocked as a result of which it will not reach the intended recipient. The recipient concerned will not be notified.

=====

Information in this e-mail and any attachments is confidential, and may not be copied or used by anyone other than the addressee, nor disclosed to any third party without our permission. There is no intention to create any legally binding contract or other binding commitment through the use of this electronic communication, except where such contract or commitment has been confirmed and duly signed by an authorized representative of

5.1.2.i

Although 5.1.2.i has taken reasonable steps to ensure that this communication and any attachments are free from computer viruses, you are advised to take your own steps to ensure that they are actually virus free.

Registered name: 5.1.2.i

Registered office: 5.1.2.i

Chamber of Commerce number: 5.1.2.i

Information in this e-mail and any attachments is confidential, and may not be copied or used by anyone other than the addressee, nor disclosed to any third party without our permission. There is no intention to create any legally binding contract or other binding commitment through the use of this electronic communication unless it is issued in accordance with the 5.1.2.i standard terms and conditions of purchase or other express written agreement between 5.1.2.i and the recipient. Although 5.1.2.i has taken reasonable steps to ensure that this communication and any attachments are free from computer viruses, you are advised to take your own steps to ensure that they are actually virus free.

5.1.2.i is authorised and regulated by the Financial Conduct Authority.

Companies Act information: Registered name: 5.1.2.i. Registered office 5.1.2.i

. Place of registration: England and Wales. Registered number: 5.1.2.i

----- Disclaimer -----

De informatie verzonden met dit e-mailbericht (en bijlagen) is uitsluitend bestemd voor de geadresseerde(n) en zij die van de geadresseerde(n) toestemming kregen dit bericht te lezen. Kennisneming door anderen is niet toegestaan.

De informatie in dit e-mailbericht (en bijlagen) kan vertrouwelijk van aard zijn en binnen het bereik van een geheimhoudingsplicht en/of een verschoningsrecht vallen.

Indien dit e-mailbericht niet voor u bestemd is, wordt u verzocht de afzender daarover

onmiddellijk te informeren en het e-mailbericht (en bijlagen) te vernietigen.

Conform het beveiligingsbeleid van de Politie wordt e-mail van en naar de politie gecontroleerd op virussen, spam en phishing en moet deze e-mail voldoen aan de voor de overheid verplichte mailbeveiligingsstandaarden die zijn vastgesteld door het Forum Standaardisatie.

Mail die niet voldoet aan het beveiligingsbeleid kan worden geblokkeerd waardoor deze de geadresseerde niet bereikt. De geadresseerde wordt hiervan niet in kennis gesteld.

-----  
The information sent in this E-mail message (including any attachments) is exclusively intended for the individual(s) to whom it is addressed and for the individual(s) who has/have had permission from the recipient(s) to read this message.

Access by others is not permitted.

The information in this E-mail message (including any attachments) may be of a confidential nature and may form part of the duty of confidentiality and/or the right of non-disclosure.

If you have received this E-mail message in error, please notify the sender without delay and delete the E-mail message (including any attachments).

In conformity with the security policy of the Police, E-mails from and to the Police are checked for viruses, spam and phishing and this E-mail must meet the standards of the government-imposed E-mail security as set by the Standardization Forum.

Any E-mail failing to meet said security policy may be blocked as a result of which it will not reach the intended recipient. The recipient concerned will not be notified.

=====

Information in this e-mail and any attachments is confidential, and may not be copied or used by anyone other than the addressee, nor disclosed to any third party without our permission. There is no intention to create any legally binding contract or other binding commitment through the use of this electronic communication, except where such contract or commitment has been confirmed and duly signed by an authorized representative of

5.1.2.i

Although 5.1.2.i has taken reasonable steps to ensure that this communication and any attachments are free from computer viruses, you are advised to take your own steps to ensure that they are actually virus free.

Registered name: 5.1.2.i

Registered office: 5.1.2.i

Chamber of Commerce number: 5.1.2.i

Information in this e-mail and any attachments is confidential, and may not be copied or used by anyone other than the addressee, nor disclosed to any third party without our permission. There is no intention to create any legally binding contract or other binding commitment through the use of this electronic communication unless it is issued in accordance with the 5.1.2.i standard terms and conditions of purchase or other express written agreement between 5.1.2.i and the recipient. Although 5.1.2.i has taken reasonable steps to ensure that this communication and any attachments are free from computer viruses, you are advised to take your own steps to ensure that they are actually virus free.

5.1.2.i is authorised and regulated by the Financial Conduct Authority.

Companies Act information: Registered name: 5.1.2.i. Registered office: 5.1.2.i

. Place of registration: England and Wales. Registered number: 5.1.2.i

**Van:** 5.1.2.e 5.1.2.e  
**Aan:** 5.1.2.e  
**Cc:** 5.1.2.e 5.1.2.  
**Onderwerp:** RE: Verwerkersovereenkomst <> document meldplicht datalekken  
**Datum:** maandag 10 mei 2021 15:08:55  
**Bijlagen:** [image007.png](#)  
[image001.png](#)

---

5.1.2.e ,

5.2.1 hartelijk dank,

Hartelijke groet,

5.1.2.e  
5.1.2.e

06 – 5.1.2.e of 0900 - 8844  
 Werkdagen: ma, di, wo, do ,vrij afwezig)

Politie I PDC I ICT I [Team Tactische Bedrijfsvoering](#)  
 Bezoekadres, Zeisterweg 1, kmr D1.29b,  
 Postcode, 3984 NH, Odijk,  
 Postbus 238, 3970 AE Driebergen,  
 Meer informatie? Kijk op [politie.nl](#)



please don't print this e-mail unless you really need to  
 © 2021 Politie Nederland, all rights reserved.




---

**Van:** 5.1.2.e  
**Verzonden:** maandag 10 mei 2021 12:36  
**Aan:** 5.1.2.e 5.1.2.e 5.1.2.e ?e <5.1.2.e> politie.nl>  
**Onderwerp:** RE: Verwerkersovereenkomst <> document meldplicht datalekken

Hallo 5.1.2.e

Als het gaat over de BIO en ISMS dan mag hij gaan sparren met 5.1.2.e  
 Wat betreft Privacy en GEB's en verwerkersovereenkomsten verwijs ik hem graag naar 5.1.2.e  
 5.1.2.e . Hij is bezig om daar een afdeling op te zetten.

Grts 5.1.2.e

---

**Van:** 5.1.2.e 5.1.2.e  
**Verzonden:** zondag 9 mei 2021 23:08  
**Aan:** 5.1.2.e <5.1.2.e> @politie.nl>  
**Onderwerp:** FW: Verwerkersovereenkomst <> document meldplicht datalekken

Hallo 5.1.2.e

Sinds 1 mei is 5.1.2.e bij ons komen werken bij het Contract Management team.  
 5.1.2.e heeft super veel ervaring op gebied van BIO en Security aspecten, zou jij iemand in jouw team  
 kunnen laten sparren met 5.1.2.e om meer inzicht te verkrijgen hoe het binnen Politie werkt en waar de  
 aandachtspunten cq de afwijkingen zitten bij Politie tov de overheid brede implementaties?

Alvast bedankt,

Hartelijke groet,

5.1.2.e

5.1.2.e

06 – 5.1.2.e of 0900 - 8844  
Werkdagen: ma, di, wo, do ,vrij afwezig)

Politie | PDC | ICT | [Team Tactische Bedrijfsvoering](#)  
Bezoekadres, Zeisterweg 1, kmr D1.29b,  
Postcode, 3984 NH, Odijk,  
Postbus 238, 3970 AE Driebergen,  
Meer informatie? Kijk op [politie.nl](#)



please don't print this e-mail unless you really need to  
© 2021 Politie Nederland, all rights reserved.



---

**Van:** 5.1.2.e

**Verzonden:** vrijdag 7 mei 2021 15:14

**Aan:** 5.1.2.e 5.1.2.e 5.1.2.e <[@politie.nl](#)>

**Onderwerp:** FW: Verwerkersovereenkomst <> document meldplicht datalekken

Hallo 5.1.2.e,

Ik heb gisteravond nog op Agora gekeken en heb daarbij gezocht naar verwerkersovereenkomsten etc. Zo leerde ik onder meer dat een PIA bij de Politie een GEB heet... En ik heb in de vrijgegeven map van de audit deze opdracht doorgelezen. Daarin zag ik dat er voor de Politie een BIO (Baseline Informatiebeveiliging Overheid) addendum is; daar wist ik nog niet van en over dit BIO addendum heb ik ook niets kunnen vinden op het openbare internet en ook niet op Agora.... Ik zie zelf een addendum als iets dat extra is, extra naast de overige BIO controls. Dus meer werk...

#### *ISMS / BIO*

Ik heb ook op Agora nog gekeken naar ISMS (Information Security Management System). De oogst van documenten daarover was beperkt.

Het ISMS is heel geschikt om de BIO controls in vast te leggen en de evidence (bewijslast) bij te voegen, zie ook <https://bio-overheid.nl>.

#### *Verwerkersovereenkomsten*

Onderstaand bericht heb ik eerst maar naar mijzelf gemaild als geheugen steun. Als we met de AVG collega's gaan zitten, ben ik belangstellend hoever zij zijn met de Politie verwerkersovereenkomsten (VWO of VWO'n) en waar de Politie VWO afwijkt van de Model VWO (van 5.1.2.i - Bijlage 7). En waar de Ten aanzien van 5.1.2.i (5.1.2.i

5.2.1 . Ik heb nu nog onvoldoende kennis en inzicht om een voorkeur te kunnen uitspreken.

Mijn aantekening over het denken in type / soort informatieketen is mede ingegeven door de mogelijk verschillende bewaartermijnen van persoonsgegevens voor verschillende doelen. Als dat bij de Politie anders wordt gezien, lees dat er ander beleid voor is, dan wil ik graag leren begrijpen hoe ik het anders moet zien.

Tot zover.

Met dank en groet,

5.1.2.e

---

5.1.2.e

**Verzonden:** donderdag 6 mei 2021 21:06

**Aan:** 5.1.2.e 5.1.2.e <5.1.2.e@politie.nl>

**Onderwerp:** Verwerkersovereenkomst <> document meldplicht datalekken

5.1.2.i

Het blijkt dat in de procesbeschrijving meldplicht datalekken concrete uitspraken zijn gedaan (verwachtingen zijn geadresseerd) over wat er in een verwerkersovereenkomst moet worden / zijn opgenomen. 5.2.1

---

Met vriendelijke groet,

5.1.2.e

5.1.2.e



# Procedure en handleiding Contracten

**AVG en Wpg**

Eigenaar document, Dienst Verwerving

Definitief

Versie 1.0

Versie datum 21 mei 2021

Rubricering: Politie intern

# Documentinformatie

## Versiegeschiedenis

| Versie | Versie datum | Samenvatting van de aanpassing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Gemarkeerde wijzigingen |
|--------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| 0.1    | 24-03-2021   | Eerste opzet                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | n.v.t.                  |
| 0.2    | 30-03-2021   | Enkele tekstuele aanpassingen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | n.v.t.                  |
| 0.3    | 11-05-2021   | Aanpassingen: <ul style="list-style-type: none"> <li>- Gerelateerde documenten toegevoegd bij documentinformatie;</li> <li>- Inleiding hfst 2 toegevoegd aan hoofdstuk 1 (paragraaf 1.1.);</li> <li>- Vorige hoofdstuk 2 verwijderd. Hierdoor hoofdstuknummering aangepast;</li> <li>- Par. 2.2. (was 3.2.): RACI-tabel aangepast;</li> <li>- Par. 2.2. (was 3.2.): Rol van IV als vertegenwoordiger van de opdrachtgever;</li> <li>- Par. 2.3. (was 3.3.): Rol van de privacyfunctionaris en privacy adviseur toegevoegd;</li> <li>- Hoofdstuk 5 (was 6): Begrippen politiegegevens en privacy adviseur toegevoegd. Begrip privacyfunctionaris aangepast;</li> <li>- Bijlage 1: Diverse tekstuele aanpassingen;</li> <li>- Bijlage 2: Aanpassing proces ;</li> <li>- Tekstuele aanpassingen in het gehele document.</li> </ul> | Ja                      |
| 0.3    | 18-05-2021   | Document vastgesteld door de stuurgroep privacy. Omzetten naar definitieve versie 1.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                         |
| 1.0    | 21-05-2021   | Eigenaar document gewijzigd in Dienst Verwerving en documentinformatie bijgewerkt.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                         |

## Distributie

| Versie | Verzend datum | Naam                                                          | Afdeling / Functie                                       |
|--------|---------------|---------------------------------------------------------------|----------------------------------------------------------|
| 0.1    | 24-03-2021    | 5.1.2.e                                                       | Werkproces contracten – Programma privacy                |
| 0.2    | 30-03-2021    | 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e | Programma privacy / leden MT                             |
|        |               | 5.1.2.e                                                       | Afdeling privacy PDC/ Privacy adviseur                   |
|        |               | 5.1.2.e                                                       |                                                          |
|        | 31-03-2021    | 5.1.2.e en achterban                                          | Dienst Verwerving / sectorhoofd IV                       |
|        |               | 5.1.2.e                                                       | Dienst Communicatie / leidinggevende                     |
|        |               | 5.1.2.e                                                       | Dienst IV / Productline manager telefonie en beeldspraak |
|        |               | 5.1.2.e en achterban                                          | Dienst IV / applicatie lijnmanager ICT                   |

|     |            |                                                          |                                                       |
|-----|------------|----------------------------------------------------------|-------------------------------------------------------|
|     |            | 5.1.2.e en achterban                                     | Dienst IV / transitie manager<br>sourcingprocessen IV |
| 0.3 | 07-05-2021 | 5.1.2.e                                                  | Adviseur wet- en regelgeving,<br>Gegevensautoriteit   |
|     | 11-05-2021 | 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e en B 5.1.2.e | Stuurgroep Programma privacy                          |

#### Review commentaar

| Versie | Wanneer    | Wie                                           | Functie                                                |
|--------|------------|-----------------------------------------------|--------------------------------------------------------|
| 0.1    | 29-03-2021 | 5.1.2.e                                       | Programma privacy, medewerker<br>werkproces contracten |
| 0.2    | 01-04-2021 | 5.1.2.e                                       | Programma privacy, business<br>architect               |
|        | 21-04-2021 | 5.1.2.e                                       | Dienst Verwerving, sectorhoofd<br>IV                   |
|        | 28-04-2021 | 5.1.2.e                                       | Afdeling privacy PDC/ Privacy<br>adviseur              |
|        | 30-04-2021 | 5.1.2.e                                       | Dienst IV / applicatie lijnmanager<br>ICT              |
|        | 04-05-2021 | 5.1.2.e                                       | Programma privacy, projectleider<br>communicatie       |
| 0.3    | 19-05-2021 | 5.1.2.e                                       | Adviseur wet- en regelgeving,<br>Gegevensautoriteit    |
|        | 20-05-2021 | 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e en 5.1.2.e | Stuurgroep Programma privacy                           |

#### Gerelateerde documenten

| Documentversie en -<br>datum | Documentnaam                     | Vastgesteld door   |
|------------------------------|----------------------------------|--------------------|
| V1.0, d.d. 10-01-2020        | Privacybeleid                    | Gegevensautoriteit |
| V1.8, d.d. 31-07-2020        | Inkoopbeleid Politie             | CPO bureau         |
| V1.3, d.d. 20-06-2019        | Governance inkoopstelsel Politie | CPO bureau         |
| V1.3, d.d. 13-07-2020        | Inkoop- en bestelrichtlijn       | Dienst Verwerving  |

# Inhoudsopgave

## Inhoud

|                                                                  |    |
|------------------------------------------------------------------|----|
| Documentinformatie .....                                         | 2  |
| Inhoudsopgave.....                                               | 4  |
| 1. Inleiding .....                                               | 5  |
| 1.1. AVG en Wpg.....                                             | 5  |
| 1.2. Over dit document .....                                     | 5  |
| 1.3. Doel .....                                                  | 5  |
| 1.4. Doelgroepen .....                                           | 6  |
| 2. Procedure.....                                                | 7  |
| 2.1. Het proces .....                                            | 7  |
| 2.2. De rollen van de doelgroepen.....                           | 8  |
| 2.3. De rol van de privacyfunctionaris of privacy adviseur ..... | 9  |
| 3. Analyse van de verwerking.....                                | 11 |
| 3.1. Verplichtingen onder de AVG en Wpg .....                    | 11 |
| 3.2. Verwerkingsverantwoordelijke of verwerker? .....            | 11 |
| 3.3. De beslisboom .....                                         | 12 |
| 3.4. Misverstanden .....                                         | 13 |
| 4. De verwerkersovereenkomst .....                               | 14 |
| 4.1. Wat is een verwerkersovereenkomst? .....                    | 14 |
| 4.2. Modellen verwerkersovereenkomst .....                       | 14 |
| 4.3. Aandachtspunten voor de verwerkersovereenkomst .....        | 15 |
| 4.4. Wat te doen als er geen verwerkersrelatie is .....          | 16 |
| 5. Begrippen .....                                               | 18 |
| Bijlage 1 Voorbeelden (geen) verwerkersrelatie .....             | 21 |
| Bijlage 2 Proces .....                                           | 25 |

# 1. Inleiding

## 1.1.AVG en Wpg

Er zijn in Nederland een aantal wetten, besluiten en regelingen die de verwerking van persoonsgegevens regelen. De belangrijkste is de Algemene Verordening Gegevensbescherming (AVG) die geldt voor alle bedrijven en organisaties die persoonsgegevens vastleggen van klanten, personeel of andere personen uit de EU. Naast de AVG is er een aparte Richtlijn gegevensbescherming politie en justitie. In Nederland is deze richtlijn per 1 januari 2019 geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Voor de politie en in het kader van dit document zijn vooral de AVG en de Wpg van belang. De AVG en Wpg sluiten elkaar uit. Waar de AVG geldt, is de Wpg niet van toepassing en andersom.

De AVG is sinds 25 mei 2018 van kracht en dat betekent dat er sinds die datum dezelfde privacywetgeving geldt in de hele Europese Unie. Internationaal heet de wet General Data Protection Regulation (GDPR). De AVG is de opvolger van de Wet bescherming persoonsgegevens (Wbp) in Nederland. Het doel van de AVG is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie. In Nederland houdt de Autoriteit Persoonsgegevens (AP) toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.

De Wet politiegegevens (Wpg) is sinds 2008 van kracht. In 2018 is de wet aangepast als gevolg van Europese wetgeving. In deze wet staat beschreven op welke wijze gegevens mogen worden verwerkt voor de politietaken door onder meer de politie, de bijzondere opsporingsdiensten, de Koninklijke marechaussee, de Rijksrecherche en de buitengewoon opsporingsambtenaren (BOA's). De wet bepaalt voor welke doeleinden gegevens mogen worden gebruikt en hoe. Bijvoorbeeld voor de opsporing van daders van strafbare feiten. De gegevens die de politie in dat kader verwerkt, moeten noodzakelijk zijn om dat doel te bereiken. De Wpg geldt niet voor de verwerking van politiegegevens bij de uitvoering van de wet Administratiefrechtelijke handhaving verkeersvoorschriften. Dus bijvoorbeeld bij verkeersboetes. De wet geldt ook niet voor de uitvoering van de Vreemdelingenwet en de grensbewakingstaak. Voor deze verwerkingen geldt de AVG. De Autoriteit Persoonsgegevens houdt, net als op de AVG, ook toezicht op naleving van de Wpg.

## 1.2.Over dit document

In het privacybeleid van de politie staat beschreven wat er minimaal moet gebeuren om de geldende wet- en regelgeving op het gebied van bescherming van persoonsgegevens na te leven. Het gaat hierbij om de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

De politie maakt bij het verwerken van persoonsgegevens ook gebruik van externe leveranciers of heeft samenwerkingsverbanden met externe partijen, waarbij persoonsgegevens verwerkt worden. In al deze gevallen wordt van de politie verwacht dat zij de AVG en Wpg naleeft en dat deze zijn geborgd in de juridische verbintenissen met de externe partijen. Deze verbintenissen beperken zich daarbij niet alleen tot inkoopcontracten, maar omvatten ook inkooporders, convenanten en andere overeenkomsten waarbij persoonsgegevens verwerkt worden.

De handleiding richt zich primair op:

- het proces en de rollen en verantwoordelijkheden van de doelgroepen (hoofdstuk 2)
- de analyse van de verwerking (hoofdstuk 3)
- de verwerkersovereenkomst (hoofdstuk 4).

Voor de duidelijkheid zijn in hoofdstuk 5 de belangrijkste begrippen uit deze handleiding beschreven. Voor de leesbaarheid van dit document is het aan te bevelen om deze begrippen vooraf te lezen.

## 1.3.Doel

Het doel van deze procedure en handleiding is om de doelgroepen duidelijkheid te verschaffen over hun rol en verantwoordelijkheden in het proces, handvaten te geven voor het analyseren van de verwerking en voor het opstellen van de verwerkersovereenkomst of aanvullende privacybepalingen in de hoofdovereenkomst.

## 1.4. Doelgroepen

Deze handleiding is gericht op alle medewerkers (de doelgroepen) die betrokken zijn bij de uitvoering van het inkoopproces en een taak hebben in de borging van AVG en/of Wpg bij het tot stand komen van juridische verbintenissen met leveranciers van de politie.

Afhankelijk van de omvang of de aard van de inkoopbehoefte hebben medewerkers van verschillende disciplines een specifieke rol in het inkoopproces van de politie. De Dienst Verwerving heeft in haar beleidsdocumenten "Governance Inkoopstelsel Politie" en "Inkoop- en bestelrichtlijn" beschreven hoe er ingekocht wordt binnen de politie en welke rollen er zijn in het inkoopproces. Beide documenten besteden ook kort aandacht aan de AVG en verwerking van persoonsgegevens.

De voornaamste rollen binnen het inkoopproces en daarmee ook de doelgroepen voor deze handleiding zijn de:

- opdrachtgevers als verwerkingsverantwoordelijken en eindverantwoordelijk voor de inkoop
- vertegenwoordigers van die opdrachtgevers in het inkoopproces
- vertegenwoordigers van de Dienst Verwerving, waar onder producten- en dienstenmanagers (PDM) en inkopers.

De opdrachtgever is daarbij bijvoorbeeld een portefeuillehouder, diensthoofd, sectorhoofd of politiechef van een regionale eenheid. Opdrachtgevers kunnen zich laten vertegenwoordigen door een aanbestedingsstuurgroep, een projectleider, deskundig medewerkers, bestellers of andere Diensten.

Als er persoonsgegevens worden verwerkt bij de in te kopen diensten of in te kopen producten, dan hebben ook de privacyfunctionaris van de eenheid of de privacy adviseur van het PDC als privacy-deskundige mogelijk een rol in het inkoopproces.

## 2. Procedure

### 2.1. Het proces

Elk inkoopproces van een product of dienst begint met de behoeftestelling van een opdrachtgever ( budgethouder). Maar voordat een aanbesteding voor de inkoop van het product of dienst start, maakt de opdrachtgever in het voortraject een analyse van de mogelijke oplossingen en kijkt daarbij ook naar de verwerking van persoonsgegevens (PSbD). De analyse kan ertoe leiden dat de behoefte afgedekt kan worden met een bestaande oplossing, waarbij gekeken wordt bij welk proces en verwerking deze behoefte hoort. Of dat het product niet wordt ingekocht, maar intern ontwikkelt en geproduceerd. Bijvoorbeeld de ontwikkeling en productie van specifieke software voor de eenheden.

Besluit de opdrachtgever om het product (of dienst) in te kopen, dan wordt er in ieder geval bij aanbestedingen boven de drempel voor Europees aanbesteden door de PDM een business case opgesteld waarin de zakelijke rechtvaardiging voor de inkoop is onderbouwd. Deze zakelijke rechtvaardiging betreft o.a. de afweging tussen geschatte opbrengsten en kosten, het besparingspotentieel, diverse scenario's en de onderbouwing van strategische keuzes, de verwachte voordelen, de risico's, maar ook de te nemen acties bij verwerking van persoonsgegevens.

Worden er in het nieuwe product of bij de uitvoering van de in te kopen dienst ook persoonsgegevens verwerkt, dan moet de opdrachtgever, voordat de business case opgesteld wordt, ook de volgende acties nemen:

- ontwerpen van een soll-proces met verwerking persoonsgegevens als onderdeel daarvan, met taken en categorieën persoonsgegevens, benodigde rechtsgrond en het gerechtvaardigde doel
- registratie van de verwerking in het verwerkingsregister Smart PIA, als het een nieuwe verwerking of een wijziging op een bestaande verwerking betreft
- uitvoeren van een quickscan en bepalen vervolgstappen
- uitvoeren van een GEB (gegevensbeschermingseffectbeoordeling) bij een hoog risico verwerking of een risicoanalyse (bij een laag risico verwerking)
- Voor zover mogelijk, onderzoeken of er een verwerkersrelatie is en een verwerkersovereenkomst nodig is (zie hoofdstuk 4).

Na goedkeuring van de business case wordt de aanbesteding op de politie aanbestedingskalender (PAK) gezet en uitgevoerd zodra hiervoor budget gereserveerd is.

Buiten het proces voor het uitvoeren van aanbestedingen boven het drempelbedrag (€ 139.000 in 2021 voor leveringen en diensten) voor Europese aanbestedingen, zijn er ook regels voor inkopen onder de aanbestedingsgrens. Boven de € 50.000 wordt tot de aanbestedingsgrens meervoudig onderhands (meerdere offertes) aanbesteed. Onder de €50.000 wordt enkelvoudig onderhands (1 offerte) aanbesteed. De meervoudig onderhandse aanbestedingen voert een inkoper van Dienst Verwerving uit. De enkelvoudig onderhandse aanbestedingen kan de opdrachtgever zelf uitvoeren.

Bij een opdrachtwaarde boven de € 20.000 vraagt de opdrachtgever bij het Inkooploket van Dienst Verwerving een inkoopadvies aan. Op het inkoopadviesformulier geeft de opdrachtgever ook aan of er bij de opdracht persoonsgegevens worden verwerkt en of de AVG (of Wpg) van toepassing is. Onder de € 20.000 is een inkoopadvies niet noodzakelijk en kan de opdrachtgever zonder advies van Dienst Verwerving inkopen.

Als er bij de opdracht persoonsgegevens verwerkt worden en een of beide wetten van toepassing zijn, dan voert de opdrachtgever de hiervoor genoemde acties uit, te weten registratie van de verwerking in SmartPIA bij een nieuwe verwerking of een wijziging op een bestaande verwerking, uitvoeren van een quickscan, uitvoeren van een GEB of een risicoanalyse en onderzoeken of een verwerkersovereenkomst nodig is.

Als er is vastgesteld dat er persoonsgegevens verwerkt worden bij gebruik van het nieuwe product (meestal bij software) of bij de uitvoering van de in te kopen dienst, dan moet hier tijdens (de voorbereiding op) de aanbesteding verder aandacht aan besteed worden. Er worden mogelijk eisen in het Programma van Eisen gesteld die betrekking hebben op de verwerking van persoonsgegevens of er worden extra voorwaarden in de overeenkomst gesteld waaraan de leverancier moet voldoen. Ook als de leverancier zelf verwerkingsverantwoordelijk is. Als de leverancier verwerker is dan is een verwerkersovereenkomst nodig (zie hoofdstuk 4).

In bijlage 2 is het hiervoor beschreven proces schematisch op kaart gezet.

## 2.2. De rollen van de doelgroepen

In paragraaf 1.3. zijn kort de doelgroepen genoemd die een rol spelen in het inkoopproces en bij het borgen van de verplichtingen die volgen uit de AVG en de Wpg. In de vorige paragraaf is hier dieper op ingegaan. In deze paragraaf worden de rollen, met behulp van het RACI model, verder uitgediept.

### RACI-model

Het RACI-model is een matrix die we hanteren om de rollen en verantwoordelijkheden van de personen die bij het proces betrokken zijn weer te geven.

Het RACI-model kent 4 rollen:

- (R)esponsible: Degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die accountable is
- (A)ccountable: Degene die eindverantwoordelijk, bevoegd is en goedkeuring geeft aan het resultaat. Als het erom gaat, moet hij/zij het eindoordeel kunnen vellen. Er is slechts één persoon Accountable
- (C)onsulted: Deze persoon geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan beslissingen of acties (verplicht) geraadpleegd. Dit is tweerichtingscommunicatie
- (I)nformed: Iemand die geïnformeerd wordt over de beslissingen, over de voortgang, bereikte resultaten enz. Dit is eenrichtingscommunicatie.

Het RACI-model voor het inkoopproces met daarbij de nadruk op de AVG- en Wpg-verplichtingen ziet er als volgt uit.

| Proces taken                                                     | Opdrachtgever | Vertegenwoordiger opdrachtgever | BA & IV Architect | IB-specialist | Producten- en dienstenmanager | Inkoper     | Privacyfunctionaris / privacyadviseur |
|------------------------------------------------------------------|---------------|---------------------------------|-------------------|---------------|-------------------------------|-------------|---------------------------------------|
| <b>Vaststellen behoefte</b>                                      |               |                                 |                   |               |                               |             |                                       |
| Analyse mogelijke oplossingen                                    | Accountable   | Responsible                     | Responsible       |               |                               |             |                                       |
| Ontwerp en PSdB                                                  | Accountable   | Responsible                     | Responsible       | Consulted     |                               |             | Consulted                             |
| Registratie SmartPIA                                             | Accountable   | Responsible                     |                   |               | Informed                      |             | Consulted                             |
| Uitvoeren Quicksan                                               | Accountable   | Responsible                     |                   |               | Informed                      |             | Consulted                             |
| Uitvoeren GEB of risicoanalyse                                   | Accountable   | Responsible                     |                   | Consulted     | Informed                      |             | Consulted                             |
| Make or buy beslissing                                           | Accountable   | Responsible                     |                   |               | Informed                      | Informed    |                                       |
| <b>Voorbereiding aanbesteding</b>                                |               |                                 |                   |               |                               |             |                                       |
| Bepalen inkooptraject en inkoopwaarde                            | Accountable   | Responsible                     |                   |               |                               |             |                                       |
| Opstellen business case (Europese aanbestedingen)                | Accountable   | Consulted                       |                   |               | Responsible                   | Informed    | Consulted                             |
| Aanvragen inkoopadvies (inkoopadviesformulier)                   | Accountable   | Responsible                     |                   |               |                               | Consulted   | Consulted                             |
| <b>Aanbesteding</b>                                              |               |                                 |                   |               |                               |             |                                       |
| PvE: opstellen privacy-eisen en privacy-voorwaarden overeenkomst | Accountable   | Responsible                     | Consulted         | Consulted     |                               | Consulted   | Consulted                             |
| Uitvoeren analyse verwerkersrelatie                              | Accountable   | Responsible                     |                   |               |                               | Consulted   | Consulted                             |
| Selectie leverancier (voldoen aan privacy-eisen en -voorwaarden) | Accountable   | Responsible                     |                   |               | Informed                      | Responsible | Consulted                             |
| Opstellen en sluiten overeenkomst                                | Accountable   | Responsible                     |                   | Consulted     | Informed                      | Responsible | Consulted                             |
| Opstellen en sluiten verwerkersovereenkomst                      | Accountable   | Responsible                     |                   | Consulted     | Informed                      | Responsible | Consulted                             |
| <b>Uitvoeren contract</b>                                        |               |                                 |                   |               |                               |             |                                       |
| Contractmanagement: implementatie privacy-eisen                  | Accountable   | Responsible                     |                   | Informed      | Consulted                     |             | Consulted                             |
| Contractmanagement: monitoren privacy-eisen en -voorwaarden      | Accountable   | Responsible                     |                   | Informed      | Consulted                     |             | Consulted                             |

Uit het RACI-model blijkt dat de opdrachtgever eindverantwoordelijk is voor alle processtappen die te maken hebben met de verplichtingen die volgen uit de AVG en Wpg en met de verwerking van persoonsgegevens bij het in te kopen product of de in te kopen dienst. De opdrachtgever voert de werkzaamheden in de meeste gevallen niet zelf uit en wordt bij de daadwerkelijke uitvoering vertegenwoordigd door specialisten, zoals productspecialisten en projectleiders. Die specialisten worden bijgestaan door andere specialisten uit de organisatie, zoals architecten, IB-adviseurs, PDM's, inkopers en privacyfunctionarissen of privacy adviseurs. Deze specialisten zijn echt noodzakelijk, zodra de expertise van de opdrachtgevers en haar vertegenwoordigers tekort schiet.

Bij de inkoop van ICT-producten, zoals software wordt de opdrachtgever c.q. behoeftesteller tijdens de aanbesteding en de uitvoering van het contract vertegenwoordigd door medewerkers van IV. IV wordt dan feitelijk opdrachtgever, budgethouder en contracteigenaar als het gaat om software-applicaties.

### 2.3. De rol van de privacyfunctionaris of privacy adviseur

Wat is de rol van de privacyfunctionaris of de privacy adviseur? Daarbij zijn drie vragen te beantwoorden:

1. Welke privacyfunctionaris c.q. privacy adviseur wordt bij het inkoopproces betrokken?
2. Wanneer wordt de privacyfunctionaris of privacy adviseur betrokken?
3. Wat doet de privacyfunctionaris of privacy adviseur?

#### 1. Welke privacyfunctionaris of privacy adviseur?

Om deze vraag te beantwoorden kijken we wat de inkoopbehoefte is, wie de behoeftesteller is en wie als opdrachtgever de aanbesteding initieert. Als de inkoopbehoefte een ICT-dienst of -product (meestal softwareapplicatie) betreft dan wordt altijd IV betrokken en initieert IV de aanbesteding als opdrachtgever. Is de inkoopbehoefte geen ICT-product of ICT-dienst, dan is dat in de meeste gevallen de behoeftesteller zelf.

##### **A. Inkoopbehoefte betreft een ICT-dienst of –product**

Persoonsgegevens worden veelal verwerkt in softwareapplicaties. Deze worden ingekocht of zelf ontwikkeld. Het vaststellen van de behoefte van de gebruiker (de behoeftesteller) wordt voorbereid en ondersteund door Dienst IV (ICT/IM). Het ontwikkelen of inkopen van de software wordt uitgevoerd door Dienst IV. Zij zijn daarbij opdrachtgever en budgethouder. Dienst IV heeft in samenwerking met Dienst Verwerving raamovereenkomsten gesloten voor de inkoop van standaard software en voor de ondersteuning bij het ontwikkelen van applicaties door de politie zelf (applicatiediensten). De software en de applicatiediensten worden ingekocht via minicompenties onder de raamcontractanten. Voor de inkoop van andere ICT-producten en –diensten worden aparte aanbestedingen gehouden.

Dienst IV betreft als opdrachtgever de privacy adviseur van de afdeling privacy van het PDC, als er bij de opdracht ook persoonsgegevens verwerkt worden.

##### **B. Inkoopbehoefte betreft geen ICT-dienst of -product**

De behoeftesteller is tevens opdrachtgever. Het vaststellen van de behoefte wordt voorbereid en ondersteund door producten- en dienstenmanager(s) van PDM, als het aanbestedingen boven de aanbestedingsdrempel betreffen. Onder de drempel is de PDM meestal niet betrokken.

Als er persoonsgegevens bij de opdracht worden verwerkt, dan wordt er ondersteuning geboden door de privacyfunctionaris van de opdrachtgever.

- opdrachtgever is portefeuillehouder: privacyfunctionaris van de betreffende portefeuillehouder
- opdrachtgever is een eenheid: privacyfunctionaris van de eenheid
- opdrachtgever is de politieacademie: privacyfunctionaris van de PA
- opdrachtgever is LMS: privacyfunctionaris van LMS
- opdrachtgever is een Dienst van het PDC: privacy adviseur van de afdeling privacy PDC.

#### 2. Wanneer wordt de privacyfunctionaris of privacy adviseur betrokken?

Als persoonsgegevens verwerkt worden bij een ingekocht product of dienst, dan is het aan te bevelen om de juiste experts te betrekken bij het inkoopproces. De opdrachtgever is ervoor verantwoordelijk dat bij het verwerken van persoonsgegevens wordt voldaan aan de AVG en/of Wpg. Hij heeft in elke fase van het inkoopproces, van het vaststellen van de inkoopbehoefte tot de uitvoering van het contract, de juiste expertise nodig om de privacywetgeving te borgen. Deze expertise wordt geleverd door de privacyfunctionaris of privacy adviseur.

Om er zeker van te zijn dat privacy op de juiste wijze geborgd wordt bij het tot stand komen van een overeenkomst met een derde, is het aan te bevelen dat de privacyfunctionaris of privacy adviseur in ieder geval gedurende de aanbesteding en het tot stand komen van de overeenkomst wordt betrokken. Op deze manier wordt geborgd dat het Programma van Eisen, de overeenkomst en eventuele verwerkersovereenkomst voldoen aan de eisen van AVG en/of Wpg. De privacyfunctionaris of privacy adviseur is niet zelf verantwoordelijk voor het opstellen van deze documenten, maar beoordeelt de stukken die zijn opgesteld door het aanbestedingsteam.

Ook bij het vaststellen van de behoefte, de voorbereiding van de aanbesteding of zelfs bij de uitvoering van het contract is betrokkenheid van de privacyfunctionaris of privacy adviseur wellicht gewenst.

### 3. Wat doet de privacyfunctionaris of privacy adviseur?

De privacyfunctionaris of privacy adviseur adviseert

voor de aanbesteding bij:

- raadplegen verwerkingsregister, GEB, privacy risico analyses en status geïdentificeerde risico's en maatregelen (bestaande verwerking)
- uitvoeren quickscan, start GEB (i.g.v. hoog risico), start vastlegging verwerkingsregister (nieuwe verwerking).

tijdens het aanbestedingsproces bij:

- de analyse of er een verwerkersrelatie is en een verwerkersovereenkomst gesloten moet worden;
- het opstellen van het Programma van Eisen ten aanzien van privacyaspecten
- het opstellen van eventuele aanvullende privacybepalingen voor de overeenkomst
- het beantwoorden van vragen over privacyaspecten voor de nota van inlichtingen
- het opstellen van de verwerkersovereenkomst waaronder, i.s.m. IB-kwartier, het vaststellen van de IB vereisten.

na het aanbestedingsproces:

- in het geval van een bestaande verwerking
  - bij het actualiseren van de GEB (als van toepassing)
  - bij het actualiseren van het verwerkingsregister
  - bij het actualiseren van de risico log.
- in het geval van een nieuwe verwerking:
  - bij het afronden van de quickscan
  - en in het geval van een hoog risico verwerking, bij het afronden van de GEB
  - bij het afronden van vastlegging in het verwerkingsregister.

## 3. Analyse van de verwerking

### 3.1. Verplichtingen onder de AVG en Wpg

Zoals in paragraaf 1.1. al is aangegeven, gaat het in de AVG over het verwerken van persoonsgegevens door organisaties. De AVG en ook de Wpg maken daarbij onderscheid tussen een organisatie die te beschouwen is als verwerkingsverantwoordelijke en de organisatie die de rol krijgt van verwerker. Elke verwerking van persoonsgegevens heeft een verwerkingsverantwoordelijke. Deze verwerkingsverantwoordelijke heeft onder de AVG en Wpg een aantal verplichtingen. Soms maakt een verwerkingsverantwoordelijke voor het verwerken van persoonsgegevens gebruik van een externe partij. Die externe partij is daarbij zelf verwerkingsverantwoordelijk of verwerker. Is de externe verwerkingsverantwoordelijk, dan gelden voor deze partij dezelfde verplichtingen als voor de opdrachtgever. Is de externe partij daarentegen verwerker dan gelden er specifieke verplichtingen als verwerker. Er is dan sprake van een zogenaamde verwerkersrelatie tussen de verwerkingsverantwoordelijke en de verwerker en beide partijen dienen met elkaar een verwerkersovereenkomst te sluiten. In de volgende paragraaf wordt hier nader op ingegaan en wordt uitgelegd wanneer een externe partij verwerkingsverantwoordelijke of verwerker is.

### 3.2. Verwerkingsverantwoordelijke of verwerker?

In paragraaf 3.1. is vastgesteld dat een verwerkingsverantwoordelijke (de opdrachtgever) bij het verwerken van persoonsgegevens door een externe partij (de opdrachtnemer) mogelijk een verwerkersovereenkomst met die partij moet sluiten. Een verwerkersovereenkomst is alleen nodig als de externe partij wordt aangemerkt als verwerker. Is de externe partij zelf ook verwerkingsverantwoordelijk dan is een verwerkersovereenkomst niet noodzakelijk en eigenlijk zelfs niet gewenst. Hierover later meer.

Wanneer is een opdrachtnemer nu verwerker en wanneer is deze dat niet, maar zelf verwerkingsverantwoordelijk? Een opdrachtnemer is verwerker, als hij de verwerking uitvoert ten behoeve van de opdrachtgever die daarbij het doel en de middelen bepaalt en waarbij de opdrachtnemer niet onderworpen is aan rechtstreeks gezag en er geen hiërarchische verhouding bestaat tussen de opdrachtgever en opdrachtnemer. De relatie tussen de opdrachtgever, de verwerkingsverantwoordelijke en de opdrachtnemer, de verwerker noemt men ook wel een verwerkersrelatie. Er is dan een verwerkersovereenkomst nodig.

Alleen het beschikken over of verkrijgen van persoonsgegevens van een verwerkingsverantwoordelijke maakt een opdrachtnemer nog geen verwerker. Er moet verwerking zijn 'ten behoeve van' die opdrachtgever of verwerkingsverantwoordelijke, wat onder meer betekent dat de opdracht primair gericht moet zijn op verwerking van persoonsgegevens. Komt er verwerking bij kijken maar heeft de opdracht betrekking op een andere dienstverlening dan ontstaat er nog geen verwerkersrelatie.

Anders gesteld: Is het (administratieve of organisatorische) proces van de opdrachtgever gediend met de verwerking, dan wijst dat op een verwerkersrelatie ('ten behoeve van'). Dient de verwerking het (administratieve of organisatorische) proces van de opdrachtnemer dan is er eerder geen verwerkersrelatie. In dat geval is de opdrachtnemer zelf verwerkingsverantwoordelijk. Bijvoorbeeld de bloemist die een adres nodig heeft om zijn bloemen te kunnen bezorgen. De opdracht is primair gericht op het bezorgen van bloemen. Niet op het verwerken van de adresgegevens van de persoon die de bloemen moet ontvangen. De bloemist heeft de adresgegevens bovendien nodig voor zijn eigen administratieve en organisatorische proces. Niet voor dat van de opdrachtgever.

#### Rapportages

Geregeld worden er in overeenkomsten door de politie, ten behoeve van het contractmanagement, rapportages verlangd waarin door de opdrachtnemer persoonsgegevens worden opgenomen. Het gaat dan niet langer om persoonsgegevens die de opdrachtnemer nodig heeft voor zijn eigen administratieve proces, maar voor dat van de opdrachtgever, de politie. In dat geval bepaalt de politie doel en middelen en ontstaat er een verwerkersrelatie. Er is dan voor dit deel van de opdracht een verwerkersovereenkomst nodig. Om te voorkomen dat er onnodig een verwerkersovereenkomst gesloten wordt, is het aan te bevelen om bij rapportages goed te kijken of het rapporteren van persoonsgegevens echt nodig is voor het uitvoeren van de opdracht.

#### Voorbeelden

Vaststellen of een organisatie verwerker of verwerkingsverantwoordelijke is, is niet altijd eenvoudig. Niet zelden moet bij een analyse een collega worden geraadpleegd om dat te kunnen bepalen. Ter ondersteuning zijn daarom in bijlage 1 alvast een aantal situaties beschreven van een verwerkersrelatie of het ontbreken daarvan.

### Waarom geen verwerkersovereenkomst als er geen verwerkersrelatie is?

Het is af te raden, zowel voor verwerkingsverantwoordelijken als voor verwerkers om een verwerkersovereenkomst aan te gaan als er geen sprake is van een verwerkersrelatie. Ten eerste omdat er een juridische schijnwerkelijkheid ontstaat en partijen denken volgens de AVG te handelen maar dat niet blijken te doen. Dat is vooral een risico voor de verwerkingsverantwoordelijke die wellicht denkt beveiligingsrisico's uit te besteden (en dus zelf minder hoeft te doen), om vervolgens aangesproken te worden op tekortschieten als verwerkingsverantwoordelijke omdat hijzelf maatregelen had moeten treffen.

Ten tweede omdat de verwerkersovereenkomst rechten en verplichtingen met zich meebrengt en partijen zich daaraan moeten houden. Dat is meer relevant voor de verwerker, die bijvoorbeeld moet investeren in beveiligingsoplossingen, bedrijfsprocessen moet herinrichten, audits moet toelaten, enz. Zodra hij persoonsgegevens verwerkt, moet hij dat toch, maar wellicht met andere processen en technische middelen.

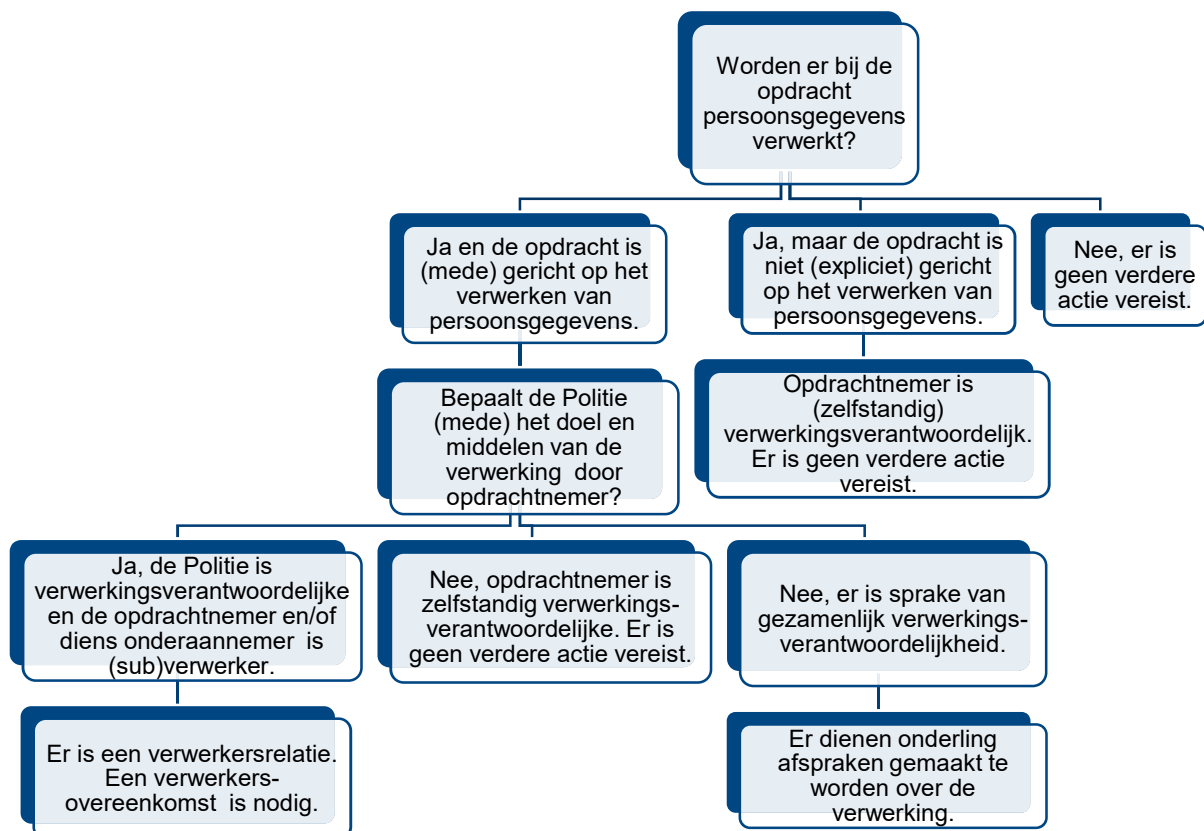
Ten derde omdat de opdrachtnemer ten onrechte in de veronderstelling verkeert zich te kunnen beroepen op de opdrachtgever als verwerkingsverantwoordelijke. Anders dan de verwerker moet de verwerkingsverantwoordelijke instaan voor de rechtmatigheid van de verwerking, de borging van de rechten van de betrokkenen, de eventueel noodzakelijke GEB's, enz. Als de opdrachtnemer geen verwerker is maar wel persoonsgegevens ontvangt en verwerkt is hij verwerkingsverantwoordelijke met alles wat daarbij komt kijken.

### Gezamenlijke verwerkingsverantwoordelijkheid

Als een organisatie persoonsgegevens verwerkt voor haar eigen doeleinden en deze gegevens deelt met een andere organisatie die de persoonsgegevens voor haar eigen doelen gebruikt, dan is sprake van twee zelfstandige verwerkingsverantwoordelijken. Van gezamenlijke verwerkingsverantwoordelijkheid in de zin van artikel 26 AVG is sprake als twee of meerdere verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen. Wanneer er sprake is van gezamenlijke verwerkingsverantwoordelijkheid dan is het voorgeschreven dat beide partijen onderling afspraken maken over de invulling van de verplichtingen uit de AVG.

### 3.3.De beslisboom

Als hulpmiddel voor het vaststellen welke acties de politie in het kader van de AVG en/of Wpg moet nemen is er een beslisboom gemaakt. Stel eerst vast of het verwerken van persoonsgegevens plaats vindt of niet. Bepaal vervolgens welke partij(en) hierbij de verwerkingsverantwoordelijke is/zijn en of er sprake is van een verwerkersrelatie.



### **3.4.Misverstanden**

In het inkoopproces zijn er, als het gaat om het verwerken van persoonsgegevens, nog wel eens misverstanden die leiden tot verkeerde keuzes. De meest voor de hand liggende is de aanname dat er bij het verwerken van persoonsgegevens door een leverancier altijd een verwerkersovereenkomst nodig is. Dat is, zoals we hiervoor gezien hebben, niet altijd het geval.

Een ander misverstand is dat er vaak wordt aangenomen, dat er na het uitvoeren van een GEB ook altijd een verwerkersovereenkomst moet worden gesloten als er sprake is van het verwerken van persoonsgegevens door een externe. Ook dat is niet altijd het geval. Een hoog risico verwerking leidt niet automatisch tot een verwerkersovereenkomst.

Uiteraard is het wel aan te bevelen om in het selectieproces een leverancier te kiezen die in staat en bereid is om de juiste technische en organisatorische maatregelen te nemen die leiden tot een goede beveiliging van de (persoons)gegevens van de politie. Ook al is die leverancier zelf verwerkingsverantwoordelijk. Bij het opstellen van een Programma van Eisen en de overeenkomst worden hieraan eisen of voorwaarden gesteld.

## 4. De verwerkersovereenkomst

### 4.1. Wat is een verwerkersovereenkomst?

Een verwerkersovereenkomst is een specifieke overeenkomst tussen een verwerkingsverantwoordelijke en een verwerker. Hierin wordt vastgelegd hoe de verwerker met de persoonsgegevens van de verwerkingsverantwoordelijke omgaat. Het gaat daarbij om schriftelijke en in rechte afdwingbare afspraken, waarvoor beide partijen tekenen. De AVG spreekt niet over een separate verwerkersovereenkomst. Artikel 28 van de AVG benoemt welke bepalingen de overeenkomst in ieder geval moet bevatten.

Ook in de Wpg is sprake van een overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker. In de wet staat dat er bij of krachtens algemene maatregel van bestuur nadere regels gesteld worden over de inhoud van die overeenkomst of rechtshandeling.

#### Eisen aan de verwerkersovereenkomst

In een verwerkersovereenkomst horen in ieder geval de volgende onderwerpen te staan:

- het onderwerp en de duur van de verwerking
- de aard en het doel van de verwerking
- het soort persoonsgegevens en de categorieën van betrokkenen
- de rechten en verplichtingen van de verwerkingsverantwoordelijke
- de verplichting van de verwerker om de persoonsgegevens alleen ten behoeve van de verwerkingsverantwoordelijke te verwerken (dus niet voor eigen doeleinden van de verwerker). De verwerker verwerkt de persoonsgegevens alleen onder de schriftelijke instructies van de verwerkingsverantwoordelijke, onder andere voor de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (tenzij deze daartoe wettelijk is verplicht)
- de technische en organisatorische beveiligingsmaatregelen die de verwerker neemt ter beveiliging van de persoonsgegevens van minimaal hetzelfde niveau van beveiliging als de verwerkingsverantwoordelijke;
- hoe de verwerker behoort te handelen in geval van een datalek
- de verwerker waarborgt dat de toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting
- afspraken met sub-verwerkers over uitbesteding van (delen van) de verwerking. Hierbij is voorafgaande toestemming nodig van de verwerkingsverantwoordelijke
- de verwerker stelt aan de sub-verwerker dezelfde eisen als de eisen die aan de verwerker zelf zijn gesteld;
- na beëindiging van de overeenkomst wist de verwerker de verwerkte persoonsgegevens of geeft deze aan de verwerkingsverantwoordelijke terug en verwijdert bestaande kopieën
- de verwerker biedt de verwerkingsverantwoordelijke alle mogelijke ondersteuning bij het nakomen van diens verplichtingen met het oog op de beantwoording van verzoeken rondom de rechten van betrokkenen;
- de verwerker staat de verwerkingsverantwoordelijke bij, bij het nakomen van diens verplichtingen op het gebied van de beveiliging van persoonsgegevens en de meldplicht datalekken
- het recht van audits of andere afspraken van de verwerkingsverantwoordelijke om aantoonbaar te maken dat de verwerker voldoet aan de verplichtingen uit de verwerkersovereenkomst en de AVG.

Strikt genomen hoeven deze bepalingen niet in een separate overeenkomst te staan. Zij mogen ook deel zijn van de algemene voorwaarden of van de hoofdovereenkomst. Het heeft de voorkeur om met de verwerker een separate overeenkomst te sluiten. Zeker voor de politie, omdat die zowel met AVG als met Wpg te maken heeft. De politie hanteert daarom ook aparte modelovereenkomsten die zowel op de AVG als op de Wpg zijn afgestemd (zie paragraaf 4.2).

### 4.2. Modellen verwerkersovereenkomst

De politie werkt met eigen modellen van verwerkersovereenkomsten. Dit zijn standaarden met een beperkt aantal variabelen / gegevens die ingevuld moeten worden. De volgende modellen zijn beschikbaar en staan in het handboek van Dienst Verwerving:

- a. Verwerkersovereenkomst Politie ARVODI-2018, versie 2.3
- b. Verwerkersovereenkomst Politie ARBIT-2018, versie 2.3
- c. Verwerkersovereenkomst Politie ARIV-2018, versie 2.3
- d. Verwerkersovereenkomst Politie 2018 (niet ARVODI of ARBIT), versie 0.1.

De verwerkersovereenkomsten a t/m c sluiten aan bij de Rijksinkoopvoorwaarden voor respectievelijk diensten (ARVODI), ICT (ARBIT) en levering (ARIV). Inhoudelijk zijn deze verwerkersovereenkomsten identiek; het verschil zijn verwijzingen naar bepalingen in de Rijksinkoopvoorwaarden. Het laatste model wordt altijd in combinatie met een hoofdovereenkomst gesloten.

Een verwerkersovereenkomst staat niet op zichzelf, maar is samen met o.a. een hoofdovereenkomst en overige voorwaarden, zoals gesteld in de uitvraag en het Programma van Eisen, onderdeel van een contractenset. Daarbij dienen inhoud en formulering van de documenten op elkaar aan te sluiten. Een verwerkersovereenkomst is altijd gekoppeld aan een hoofdovereenkomst en loopt in de meeste gevallen op hetzelfde moment af als de hoofdovereenkomst. Indien de uitvoering van de hoofdovereenkomst dit vereist, dan kan een verwerkersovereenkomst eventueel langer doorlopen.

De politie werkt, als verwerkingsverantwoordelijke, met haar eigen standaard verwerkersovereenkomsten en tekent in principe geen verwerkersovereenkomsten van andere partijen. De politie wil immers als verantwoordelijke voor de persoonsgegevens zelf controle hebben over de manier waarop de verwerker om gaat met de data. Het is niet aan de verwerker om dat te bepalen. In uitzonderlijke gevallen is het mogelijk hiervan af te wijken. Hiervoor is toestemming van de Gegevensautoriteit (GA) nodig. Soms treedt de politie zelf op als verwerker. In die gevallen kan de verwerkersovereenkomst van de verwerkingsverantwoordelijke partij gebruikt worden.

De politie ondertekent in geen geval een privacyverklaring van een leverancier! Een privacyverklaring geeft informatie over hoe wordt omgegaan met persoonsgegevens, maar staat los van de specifieke afspraken die je als verwerkingsverantwoordelijke maakt met de verwerker. Een privacyverklaring is geen overeenkomst.

### 4.3.Aandachtspunten voor de verwerkersovereenkomst

In de modellen van de politie zijn de meeste eisen die aan de verwerkersovereenkomst gesteld worden in de standaardbepalingen verwerkt.

De verwerkersovereenkomst wordt nog aangevuld met de gegevens waar het uiteindelijk om draait. Namelijk de categorieën van betrokkenen, het soort persoonsgegevens en aard en het doel van de verwerking. Categorieën van betrokkenen zijn bijvoorbeeld: medewerkers politie, gepensioneerden politie, studenten PA, docenten PA, gebruikers van een bepaalde dienst of applicatie, burgers (Wpg), etc. Soort persoonsgegevens zijn bijvoorbeeld: voornaam, achternaam, geboortedatum, personeelsnummer, functie, afdeling, inloggegevens, e-mailadres, telefoonnummer, diploma's, opleidingsgegevens, gepseudonimiseerde persoonsgegevens, etc.

In de verwerkersovereenkomst wordt ook vermeld hoe lang de verwerking duurt en hoe lang de persoonsgegevens bewaard mogen worden. De duur van de verwerking is in de meeste gevallen gelijk aan de duur van de hoofdovereenkomst.

Geef in de verwerkersovereenkomst ook aan van welke sub-verwerkers de verwerker eventueel gebruik maakt. De politie dient expliciet toestemming te geven voor gebruik van deze sub-verwerkers.

Aan het model verwerkersovereenkomst zijn twee bijlagen toegevoegd. De tweede bijlage gebruikt de verwerker in het geval er sprake is van een datalek. De eerste bijlage is bedoeld voor het invullen van de hiervoor genoemde gegevens. Deze gegevens worden aangevuld met de contactgegevens van de verwerker en met functiegegevens van het personeel van de verwerker dat bij de verwerking betrokken is.

Tot slot vermeldt bijlage 1 van de verwerkersovereenkomst welke technische en organisatorische maatregelen de verwerker dient te nemen ter beveiliging van de persoonsgegevens van de politie of van de politiegegevens. Denk hierover al na tijdens het vaststellen van de behoefte, de voorbereiding van de aanbesteding of verlenging van een overeenkomst. In ieder geval is bij het opstellen van het Programma van Eisen duidelijk welke technische en organisatorische maatregelen de verwerker behoort te nemen. Welke eisen worden er bijvoorbeeld aan het beveiligingsbeleid en de kwaliteitsborging gesteld? Is de verwerker of sub-verwerker hiervoor gecertificeerd of kan de verwerker dat op een andere wijze aantonen?

Organisaties moeten moderne technieken gebruiken om persoonsgegevens adequaat te beveiligen. Welke technische maatregelen kan de verwerker o.a. nemen om de persoonsgegevens (en mogelijk andere gegevens) van de politie te beveiligen?

- toegangscontrole voor bepaalde ruimtes
- encryptie (pseudonimisering)
- wachtwoordbeleid
- twee factor authenticatie
- complete documentatie
- goede back-ups
- recovery plan wanneer de verwerker wordt getroffen

- slimme firewall met licenties om datalekken te voorkomen
- gescheiden en veilige IT-netwerken om inbreuk te voorkomen
- centraliseren toegang en het beheer van de gebruikersaccounts
- frequent werkplek en update beheer
- monitoren en registratie van incidenten
- regelmatige controle op het juist functioneren van bovenstaande maatregelen.

Welke organisatorische maatregelen kan de verwerker nemen?

- richtlijnen over het verwerken van persoonsgegevens
- privacy-bewustzijn binnen de organisatie creëren door middel van trainingen
- autorisaties van gebruikers beperken tot bepaalde taken
- jaarlijkse evaluatie van technische en organisatorische maatregelen inzake effectiviteit en plausibiliteit.

Afhankelijk van het risico, worden de juiste technische en organisatorische maatregelen gekozen. Raadpleeg hiervoor ook een Informatiebeveiligingsdeskundige.

#### 4.4. Wat te doen als er geen verwerkersrelatie is

Als er geen verwerkersrelatie is en er geen verwerkersovereenkomst gesloten wordt, maak dan met de opdrachtnemer, als deze zelfstandig verwerkingsverantwoordelijk is, contractuele afspraken over de veilige uitwisseling, opslag en vernietiging van persoonsgegevens. Bijvoorbeeld met de bloemist die een adres ontvangt voor het bezorgen van een bos bloemen aan een zieke medewerker.

De onderwerpen waarover in ieder geval afspraken gemaakt worden betreffen:

1. geheimhouding
2. informatiebeveiliging
3. datalekken;
4. vernietigen of terugbezorgen van gegevens.

De politie hanteert standaard de Rijksinkoopvoorwaarden ARIV, ARVODI of ARBIT als onderliggende voorwaarden bij het aangaan van inkoopverplichtingen met derden. Deze inkoopvoorwaarden bevatten in meer of mindere mate bepalingen die betrekking hebben op de behandeling van (persoons)gegevens van de politie door opdrachtnemers.

##### 1. Geheimhouding

In de Rijksinkoopvoorwaarden is een bepaling opgenomen over geheimhouding. In de ARIV 2018 is dat artikel 8, in de ARVODI 2018 betreft het artikel 13 en in de ARBIT 2018, artikel 17.

##### 2. Informatiebeveiliging

Dit betreft de technische en organisatorische beveiligingsmaatregelen die de opdrachtnemer neemt ter beveiliging van de persoonsgegevens van de politie of politiegegevens. In de meest recente versies van de Rijksinkoopvoorwaarden uit 2018 is hierover geen specifieke bepaling opgenomen in geval de opdrachtnemer zelf verwerkingsverantwoordelijk is. Wel is er een bepaling in elk van de Rijksinkoopvoorwaarden over het verwerken van persoonsgegevens en de verplichting tot beveiliging daarvan, als de opdrachtnemer verwerker is.

Neem daarom om in de overeenkomst met de opdrachtnemer een aparte bepaling op over beveiliging van de verkregen informatie van de politie.

##### 3. Datalekken

Hoe de opdrachtnemer als verwerkingsverantwoordelijke handelt als er een datalek is, is vastgelegd in de AVG. Deze meldt binnen 72 uur het datalek bij de Autoriteit Persoonsgegevens. Ook de politie zal hierover graag binnen een bepaald tijdsbestek geïnformeerd willen worden. In de algemene inkoopvoorwaarden ARIV, ARVODI en ARBIT is geen specifieke bepaling opgenomen over het melden van datalekken.

Neem daarom in de overeenkomst met de opdrachtnemer een aparte bepaling op over het melden van datalekken aan de politie.

##### 4. Vernietigen of terugbezorgen van gegevens

Voor zover de opdrachtnemer niet te maken heeft met wettelijke bewaartermijnen, is het zinvol om hierover in de overeenkomst met de opdrachtnemer een bepaling op te nemen. In artikel 13 van de ARVODI 2018 en in artikel 17 van de ARBIT 2018 is het een en ander bepaald over het terugbezorgen van gegevens in het algemeen. Een aanvullende bepaling in de overeenkomst over vernietiging of terugbezorgen van persoonsgegevens is noodzakelijk.

De politie heeft in haar model raamovereenkomsten voor diensten, leveringen en ICT een bepaling opgenomen over de verwerking van persoonsgegevens. Hierin is ten aanzien van het melden van datalekken en het bewaren en vernietigen van persoonsgegevens geregeld wat de opdrachtnemer doet in geval deze zelf verwerkingsverantwoordelijk is.

**Gezamenlijke verwerkingsverantwoordelijkheid**

Ook in geval van gezamenlijke verwerkingsverantwoordelijkheid (zie 3.2.) maken beide partijen onderling afspraken over de omgang en beveiliging van de persoonsgegevens.

## 5. Begrippen

Dit hoofdstuk bevat een aantal begrippen. Voor de leesbaarheid van de handleiding is het van belang om kennis van deze begrippen te hebben.

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aanbesteding</b>            | Aanbesteden is een manier om in te kopen. Kenmerkend voor deze wijze van inkopen is het gelijktijdig, onder dezelfde condities, voorwaarden en procedureregels in concurrentie op de markt brengen van de opdracht. De aanbesteding bestaat uit drie fases specificeren, selecteren en contracteren.                                                                                                                                                                           |
| <b>Anonimiseren</b>            | Versleuteling van gegevens die niet omkeerbaar is. Als persoonsgegevens eenmaal zijn ontdaan van identificerende data, is het niet meer mogelijk om deze later weer met personen in verband te brengen. De AVG is niet van toepassing op volledig geanonimiseerde data.                                                                                                                                                                                                        |
| <b>ARBIT</b>                   | Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten. Dit zijn algemene inkoopvoorwaarden die zijn opgesteld door en voor de rijksoverheid voor gebruik bij kleine en middelgrote IT-inkopen tussen de rijksoverheid en derden.                                                                                                                                                                                                                                               |
| <b>ARIV</b>                    | Algemene Rijksinkoopvoorwaarden. Dit zijn algemene inkoopvoorwaarden die zijn opgesteld door en voor de rijksoverheid voor gebruik bij koop- en leveringsovereenkomsten tussen de rijksoverheid en derden. De voorwaarden zijn uitdrukkelijk niet bedoeld voor IT-inkopen en de inkoop van diensten.                                                                                                                                                                           |
| <b>ARVODI</b>                  | Algemene Rijksinkoopvoorwaarden voor diensten. Dit zijn algemene inkoopvoorwaarden die zijn opgesteld door en voor de rijksoverheid voor gebruik bij de uitvoering van diensten voor de rijksoverheid door derden                                                                                                                                                                                                                                                              |
| <b>AVG</b>                     | Algemene Verordening Gegevensbescherming. Deze wet regelt wat er allemaal wel en niet mag met de persoonsgegevens van mensen. Bij elk gebruik van persoonsgegevens geldt dat de privacy inbreuk zo klein mogelijk moet zijn. De Engelse benaming voor AVG is General Data Protection Regulation (GDPR).                                                                                                                                                                        |
| <b>Categorieën betrokkenen</b> | Soorten van groepen betrokkenen, waarbij de betrokkene de geïdentificeerde of identificeerbare natuurlijk persoon is op wie de verwerkte en/of de te verwerken persoonsgegevens betrekking hebben.                                                                                                                                                                                                                                                                             |
| <b>Datalek</b>                 | Met een datalek wordt in het kader van de AVG gesproken over een inbreuk in verband met de persoonsgegevens. Hiermee wordt volgens artikel 4 van de AVG een inbreuk op de beveiliging bedoeld 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.                                                   |
| <b>GEB</b>                     | Gegevensbeschermingseffectbeoordeling, ook wel een data protection impact assessment (DPIA) genoemd. Hiermee wordt een beoordeling bedoeld van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.                                                                                                                                                                                                                                       |
| <b>ISO 27001</b>               | Een wereldwijd erkende norm op het gebied van informatiebeveiliging. De norm beschrijft hoe een organisatie procesmatig met het beveiligen van informatie kan omgaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen de organisatie zeker te stellen. Denk hierbij aan het beschermen van persoons- en/of bedrijfsgegevens, bescherming tegen hackers en inbraak.                                                                  |
| <b>ISO 9001</b>                | De wereldwijde norm voor het ontwikkelen, invoeren en verbeteren van de doeltreffendheid van een kwaliteitsmanagementsysteem van een organisatie. Deze norm geeft de eisen weer om processen te borgen en te verbeteren die belangrijk zijn voor het verhogen van klanttevredenheid. ISO 9001 kan door interne en externe partijen (waaronder certificerende instellingen) worden gebruikt om te beoordelen of een goed functionerend kwaliteitsmanagementsysteem aanwezig is. |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>On premises</b>            | Software en gegevens draaien op eigen servers en computers en zijn compleet in eigen beheer.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Persoonsgegevens</b>       | Betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Bijvoorbeeld naam, identificatienummer, locatie, IP-adres, fysieke en sociale kenmerken.                                                                                                                                                                                                                                          |
| <b>Politiegegevens</b>        | Een politiegevegeven is een gegeven dat te herleiden is tot een geïdentificeerd of identificeerbaar natuurlijk persoon en dat verwerkt wordt in het kader van de politietaak.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Privacy adviseur</b>       | Een expert op het gebied van AVG die werkzaam is op de afdeling privacy van het PDC.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Privacyfunctionaris</b>    | Een expert op het gebied van Wpg. Elke eenheid heeft tenminste één privacyfunctionaris aangesteld.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>PSbD</b>                   | Privacy en Security by Design (PSbD) betekent dat al in het stadium van het maken van ontwerpkeuzes en tijdens het ontwikkelen van de informatievoorzieningen mechanismen worden ingebouwd voor informatiebeveiliging en de bescherming van persoonsgegevens. Dit vereist dat er in een zo vroeg mogelijk stadium wordt nagedacht over het gebruik van persoonsgegevens binnen de organisatie, over de noodzaak van het gebruik van gegevens en over de bescherming ervan.                                                       |
| <b>Pseudonimiseren</b>        | Versleuteling van gegevens die omkeerbaar is. Bij pseudonimisering kunnen anonieme gegevens met de juiste sleutel inzichtelijk gemaakt worden, waardoor herleiding naar natuurlijke personen weer mogelijk is. De regels van de AVG zijn, in tegenstelling tot anonimiseren, wel van toepassing op pseudonimiseren.                                                                                                                                                                                                              |
| <b>SmartPIA</b>               | Het verwerkingsregister van de politie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Verwerker</b>              | Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkings-verantwoordelijke persoonsgegevens verwerkt en: <ul style="list-style-type: none"> <li>▪ daarbij geen zeggenschap over de gegevensverwerking heeft;</li> <li>▪ handelt naar de instructies en onder verantwoordelijkheid en toezicht van de verwerkingsverantwoordelijke</li> <li>▪ en niet aan het rechtstreeks gezag van de verwerkingsverantwoordelijke onderworpen is.</li> </ul>    |
| <b>Verwerkersovereenkomst</b> | Een overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker waarin wordt vastgelegd hoe de verwerker met de persoonsgegevens van de verwerkingsverantwoordelijke dient om te gaan. Hierin staat in ieder geval: <ul style="list-style-type: none"> <li>▪ het onderwerp en de duur van de verwerking</li> <li>▪ de aard en het doel van de verwerking</li> <li>▪ het soort persoonsgegevens en de categorieën van betrokkenen</li> <li>▪ de rechten en verplichtingen van de verwerkingsverantwoordelijke.</li> </ul> |
| <b>Verwerkersrelatie</b>      | De relatie tussen een opdrachtgever (verwerkingsverantwoordelijke) en opdrachtnemer (de verwerker) met betrekking tot de verwerking van persoonsgegevens door de opdrachtnemer ten behoeve van de opdrachtgever, waarbij de opdracht primair gericht is op het verwerken van persoonsgegevens en de opdrachtnemer niet onderworpen is aan rechtstreeks gezag van de opdrachtgever of geen hiërarchische verhouding heeft met de opdrachtgever.                                                                                   |
| <b>Verwerking</b>             | Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.                                                    |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Verwerkingsregister</b>          | <p>Het register van verwerkingsactiviteiten. Dit register bevat informatie over de persoonsgegevens die de verwerkingsverantwoordelijke verwerkt. De AVG schrijft voor welke informatie de verwerkingsverantwoordelijke in het verwerkingsregister moet zetten. Dat betreft:</p> <ul style="list-style-type: none"> <li>▪ de naam en de contactgegevens van de verwerkingsverantwoordelijke van de politie en van eventuele andere organisaties met wie politie gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld, de naam en contactgegevens van de functionaris gegevensbescherming (FG), als die is aangesteld en naam en contactgegevens van eventuele internationale organisaties waar politie persoonsgegevens mee deelt</li> <li>▪ de doelen waarvoor de persoonsgegevens worden verwerkt</li> <li>▪ een beschrijving van de categorieën van betrokken personen waarvan de persoonsgegevens worden verwerkt</li> <li>▪ een beschrijving van de categorieën van persoonsgegevens die worden verwerkt</li> <li>▪ de categorieën van ontvangers aan wie de persoonsgegevens worden verstrekt</li> <li>▪ als van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie buiten de EU</li> <li>▪ als mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist</li> <li>▪ een algemene beschrijving van de technische en organisatorische maatregelen die zijn genomen om de persoonsgegevens die worden verwerkt te beveiligen.</li> </ul> <p>Ook de verwerker dient een verwerkingsregister op te stellen.</p> |
| <b>Verwerkingsverantwoordelijke</b> | <p>Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen:</p> <ul style="list-style-type: none"> <li>▪ bepaalt waarom en welke gegevens moeten worden verwerkt (doel)</li> <li>▪ bepaalt hoe gegevens moeten worden verwerkt (middelen)</li> <li>▪ duidelijke instructies geeft over de verwerking.</li> </ul> <p>De verwerkingsverantwoordelijkheid kan ook voortvloeien uit specifieke wettelijke taken (bijv. taken op het gebied van sociale zekerheid, verwerken van medische gegevens, etc).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Wpg</b>                          | <p>Wet politiegegevens is de wet die de rechten en de plichten van de politie zelf, maar ook die van de burger regelt, voor wat betreft het verwerken van politiegegevens. Politiegegevens zijn persoonsgegevens die in het kader van de politietaken worden verwerkt.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

# Bijlage 1 Voorbeelden (geen) verwerkersrelatie

Deze bijlage bevat een aantal voorbeelden van een verwerkersrelatie of juist het ontbreken daarvan. De voorbeelden zijn onderverdeeld per dienst (Communicatie, Financiën, FM, HRM en IV).

## Algemeen

### Verwerken van contactgegevens door een leverancier

Een leverancier neemt persoonsgegevens van enkele medewerkers van de politie (contactpersonen) op in haar eigen CRM-systeem. De leverancier gebruikt deze gegevens om contact te zoeken, informatie op te sturen etc. De leverancier gebruikt de gegevens voor zijn eigen administratieve proces. De politie bepaalt geen doel en middelen. Deze verwerking van persoonsgegevens is niet een primaire opdracht vanuit de politie. Er is geen verwerkersrelatie en een verwerkersovereenkomst is niet nodig.

### Adviesdiensten door advocaten en juristen

De primaire opdracht van advocaten is niet gericht op het verwerken van persoonsgegevens, maar op het geven van juridisch advies en procederen. Verwerking van persoonsgegevens is een uitvloeisel van de dienstverlening. Advocaten en juristen zijn dan ook geen verwerkers, maar zelf verwerkingsverantwoordelijken. Er is geen verwerkersrelatie en een verwerkersovereenkomst is niet nodig.

## Dienst Communicatie

### Versturen van drukwerk

Als de politie een adresbestand verstrekt aan een drukkerij om medewerkers informatie te sturen dan is er geen sprake van gebruik voor eigen doeleinden door de drukker. De politie bepaalt waarvoor de gegevens gebruikt worden, wat er na afloop mee moet gebeuren en hoe de gegevens verwerkt moeten worden (bijvoorbeeld op een transparante folie). De politie bepaalt doel en middelen en niet de drukker. De drukker heeft de persoonsgegevens uit dit bestand niet nodig voor zijn eigen administratieve proces (zoals factureren). De drukker is daarmee verwerker en er dient een verwerkersovereenkomst met de drukker gesloten te worden.

## Dienst Financiën

### Accountantsdiensten

De primaire opdracht aan de accountant is het opstellen en controleren van de jaarrekening. De accountant is hiervoor verwerkingsverantwoordelijke. De verwerking van persoonsgegevens vloeit voort uit de primaire opdracht. De accountant bepaalt immers zelf welke (persoons)gegevens nodig zijn, welke analyses hij gaat uitvoeren en welke middelen hij daarvoor gebruikt. Omdat de accountant zelf verwerkingsverantwoordelijke is, is er geen verwerkersrelatie en is een verwerkersovereenkomst niet nodig.

Een ander voorbeeld. De politie huurt een accountant in om de salarissen te administreren. In dat geval huurt de politie de accountant niet in voor accountantswerkzaamheden, maar voor salarisadministratiewerkzaamheden. De nadruk ligt - net als bij een salarisadministratiekantoor - op het verwerken van persoonsgegevens en daarbij bepaalt de politie als werkgever ook het doel en middelen van de verwerking. Daarmee is de accountant (in de rol van salarisadministrateur) in dit geval een verwerker. Er is een verwerkersrelatie en een verwerkersovereenkomst is nodig.

### Banken en andere financiële dienstverleners

De primaire opdracht van financiële dienstverleners zoals banken is niet gericht op het verwerken van persoonsgegevens, maar op het leveren van de financiële dienst. Verwerking van persoonsgegevens is slechts een uitvloeisel van de dienstverlening. Zij zijn dan ook geen verwerker, maar zelf verwerkingsverantwoordelijke. Er is geen verwerkersrelatie en een verwerkersovereenkomst is derhalve niet nodig.

### Facturen

Het opnemen van persoonsgegevens op een factuur van een leverancier vloeit voort uit de primaire opdracht (levering product of dienstverlening) en is deel van het administratieve proces van de leverancier. Deze persoonsgegevens staan op de factuur ten behoeve van controlewerkzaamheden door de opdrachtgever. De leverancier is geen verwerker, er is geen verwerkersrelatie en een verwerkersovereenkomst is niet nodig.

NB: Beoordeel wel of het echt noodzakelijk is om persoonsgegevens op een factuur te vermelden. Beperk het gebruik van persoonsgegevens op facturen zo veel als mogelijk. Bijzondere persoonsgegevens, zoals bijvoorbeeld medische gegevens moeten in ieder geval vermeden worden.

## **Dienst FM**

### **Levering van politie-uitrusting**

Bij het fabriceren en leveren van een kleding of schoeisel voor de agenten is de opdracht primair gericht op het leveren van de uitrusting en niet op het verwerken van persoonsgegevens. Er is geen verwerkersrelatie en een verwerkersovereenkomst is niet nodig. Vraag is of het echter nodig is dat de partij die de politie-uitrusting maakt, ook weet voor welke agent dat is? Hierdoor kan een privacy risico ontstaan. Is het nodig om persoonsgegevens te koppelen aan schoen- of kledingmaten?

Als de politie de leverancier daarentegen ook opdracht geeft om rapportages met persoonsgegevens op te leveren, dan is voor dit deel van de opdracht wel een verwerkersovereenkomst nodig. Het gaat dan niet langer om persoonsgegevens die de leverancier nodig heeft voor zijn eigen bedrijfsvoering. De Politie bepaalt het doel van de gegevensverwerking.

### **Postbezorgdiensten**

Een postbezorgdienst wordt ingeschakeld om brieven of pakketjes op een bepaald adres ten behoeve van een bedrijf of privé persoon te leveren. Deze brieven of pakketten kunnen persoonsgegevens bevatten. De postverwerker heeft, door het briefgeheim, geen toegang en controle tot de eventuele persoonsgegevens, maar verplaatst alleen pakketten van de ene naar de andere locatie. Bovendien heeft de postbezorger ook briefgeheim. De postbezorger is dus geen verwerker.

Een postverwerker verwerkt de NAW-gegevens om de pakketten te bezorgen, maar dit is slechts een uitvloeisel van de dienst die ze leveren, namelijk het leveren van pakketten. De postverwerker is hiervoor dan ook geen verwerker, maar is zelf verwerkingsverantwoordelijk. Er is geen verwerkersrelatie en een verwerkersovereenkomst is niet nodig.

## **Dienst HRM**

### **Inhuur van personeel**

De politie huurt een zzp'er in om een van de medewerkers te vervangen tijdens zwangerschapsverlof. De zzp'er werkt binnen de beveiligde (online) werkomgeving van de politie, is gescreend en heeft een geheimhoudingverklaring getekend. De zzp'er valt onder het rechtstreekse gezag van de politie en is daarom geen verwerker. Hij maakt tijdelijk deel uit van de politieorganisatie, waardoor er sprake is van intern beheer. Politie blijft natuurlijk wel verantwoordelijk voor de persoonsgegevens die zij zelf verwerkt. De politie is verwerkingsverantwoordelijke. De ingehuurde zzp'er is geen verwerker en geen verwerkingsverantwoordelijke. Een verwerkersovereenkomst is niet nodig.

### **Salarisadministratie**

Politie besteedt het verwerken van de salarisadministratie uit aan een externe verwerker. Daarbij verstrekt de politie persoonsgegevens van haar medewerkers. Het primaire doel van de opdracht is het verwerken van het salaris van die medewerkers en dus persoonsgegevens. Politie bepaalt hier doel en middelen. De salarisadministrateur verwerkt de persoonsgegevens niet voor haar eigen administratieve proces, maar voor dat van de politie. De salarisadministrateur is verwerker en er is een verwerkersrelatie. Er dient een verwerkersovereenkomst gesloten te worden.

### **Uitvoeren van opleidingen**

De Politie verstrekt contactgegevens van medewerkers aan een opleidingsinstituut. De primaire opdracht is het opleiden van medewerkers. Het verwerken van de persoonsgegevens vloeit daaruit voort. Het opleidingsinstituut bepaalt zelf doel en middelen voor de verwerking. Deze persoonsgegevens worden gebruikt voor het versturen van berichten met opleidingsmateriaal, data van de opleidingen, aanmaken van een account, etc. Er is geen verwerkersrelatie tussen het opleidingsinstituut en de opdrachtgever. Een verwerkersovereenkomst is daarom niet van toepassing.

NB: Van belang is om je af te vragen of het verstrekken van gegevens nodig is. Is het bijvoorbeeld mogelijk dat medewerkers zich zelf aanmelden of via de leeromgeving van de politieacademie? In dat geval verstrekt de Politie geen gegevens aan het opleidingsinstituut en speelt de vraag of een verwerkersovereenkomst nodig is niet.

Het opleidingsinstituut mag - ook als de kandidaat zich zelf aanmeldt - niet méér persoonsgegevens verzamelen dan nodig is voor het uitvoeren van haar taak. Zo zal een geboortedatum waarschijnlijk alleen nodig zijn als deze op een diploma of certificaat komt te staan. Het is ook aan de politie om er alert op te zijn dat alleen de noodzakelijke gegevens verstrekt worden. Vraag zo nodig om een gedegen onderbouwing.

Wordt er echter méér informatie uitgewisseld tussen de politie en het opleidingsinstituut, bijvoorbeeld een rapportage over examenresultaten of over hoe de ontwikkeling verloopt, dan zal een verwerkersovereenkomst wel nodig zijn. Ter verduidelijking:

- Opleidingen die verplicht worden door de politie voor bepaalde functies. Hierbij wil de politie geïnformeerd worden over de voortgang en resultaten om daar eventueel consequenties aan te kunnen verbinden. De Politie bepaalt in dit geval het doel voor het verwerken van de betreffende persoonsgegevens. Er is dus sprake van een verwerkersrelatie
- Opleidingen waarvoor elke politiemedewerker zich zelf kan inschrijven. Er is wel toestemming nodig van de leidinggevende en de politiemedewerker kan het certificaat dat hij ontvangt laten opslaan in zijn personeelsdossier. Het opleidingsinstituut verwerkt de persoonsgegevens voor de eigen bedrijfsvoering. In dit geval is er geen verwerkersrelatie.

#### **Afsluiten van een collectieve verzekering**

De politie sluit een verzekeringscontract af voor zijn medewerkers en verstrekt in dat kader persoonsgegevens aan de verzekeraar. In dat geval is er géén sprake van uitbesteding, maar van het afnemen van een dienst door de politie. De verzekeraar bepaalt zelf doel en middelen en welke persoonsgegevens nodig zijn om de contracten te kunnen uitvoeren. De verzekeraar is zelf verwerkingsverantwoordelijke. Gezien de hoeveelheden (gevoelige) data die worden uitgewisseld is het wel zinvol om afspraken te maken over veilige uitwisseling van gegevens.

Ook hier kan wel sprake zijn van een verwerkersrelatie als de verzekeraar tevens de rol van administratiekantoor ten behoeve van de politie vervult.

## **Dienst IV**

### **Softwareontwikkeling**

Een leverancier krijgt de opdracht om specifieke software voor de politie te ontwikkelen waarin ook persoonsgegevens worden verwerkt. De vraag of er een verwerkersrelatie ontstaat tussen de politie en de leverancier hangt af van een aantal zaken. Daarbij is van belang om vast te stellen wat de opdracht precies inhoudt.

- Gaat het alleen om de softwareontwikkeling of heeft de leverancier een rol bij de implementatie of het beheer van de software en in dat kader toegang tot persoonsgegevens?
- Waar vindt opslag van de persoonsgegevens plaats? Draait de software op de politieomgeving (on premises) of bijvoorbeeld in de cloud of op de server van de leverancier?
- Hoe heeft de leverancier toegang tot de persoonsgegevens van de politie? Via een politie-account of via eigen apparatuur?
- Zijn de persoonsgegevens versleuteld (geanonimiseerd of gepseudonimiseerd (zie begrippen))?

Heeft de leverancier geen toegang tot de persoonsgegevens, dan is er uiteraard geen sprake van een verwerking door de leverancier en is er geen verwerkersrelatie. Een verwerkersovereenkomst is niet nodig.

Heeft de leverancier wel toegang tot de persoonsgegevens, dan zijn er diverse situaties mogelijk.

1. De persoonsgegevens zijn extern (cloud, server leverancier) opgeslagen en niet versleuteld of slechts gepseudonimiseerd. De leverancier is verwerker en er is een verwerkersovereenkomst nodig
2. De persoonsgegevens zijn on premises opgeslagen en niet versleuteld of gepseudonimiseerd. De leverancier logt met eigen apparatuur in. De leverancier is verwerker en er is een verwerkersovereenkomst nodig
3. De persoonsgegevens zijn on premises opgeslagen en niet versleuteld of gepseudonimiseerd. De leverancier logt in via een account van de politie en dus onder toezicht van de politie (bijvoorbeeld als ingehuurd medewerker). De leverancier is geen verwerker en er is geen verwerkersovereenkomst nodig
4. De persoonsgegevens zijn geanonimiseerd en extern of on premises opgeslagen. De leverancier is geen verwerker en er is geen verwerkersovereenkomst nodig.

Als de toegang tot persoonsgegevens door de leverancier de contactgegevens van contactpersonen van de politie betreffen dan is een verwerkersovereenkomst niet nodig.

### **Externe helpdesk**

Als de externe helpdesk van een opdrachtnemer van buiten de politieomgeving persoonsgegevens kan inzien, dan is er een verwerkersrelatie en is een verwerkersovereenkomst nodig. De politie heeft deze taak – die onderdeel is van

de bedrijfsvoering van de politie – uitbesteed, wat betekent dat de politie de verwerkingsverantwoordelijke blijft voor deze gegevens. De externe helpdesk mag de persoonsgegevens niet voor eigen doeleinden gebruiken. Als de toegang tot persoonsgegevens door de helpdesk van de leverancier alleen de contactgegevens van contactpersonen van de politie betreffen dan is een verwerkersovereenkomst niet nodig.

### **Persoonsgegevens opslaan in de cloud**

Bij het gebruik van cloudopslag van persoonsgegevens door een externe partij is de politie de partij die het doel bepaalt. Het doel is het opslaan van de persoonsgegevens, de politie bepaalt ook de duur van de opslag, etc. De externe partij heeft geen zeggenschap over deze gegevens. De externe partij is een verwerker en er is een verwerkersrelatie met de politie. Dit betekent dat een verwerkersovereenkomst nodig is.

Het is alleen toegestaan om gegevens op te slaan op servers die in de EER staan. De AVG geldt in de gehele Europese Unie, plus in Noorwegen, Liechtenstein en IJsland – samen de Europese Economische Ruimte of EER geheten. Check bij Informatie Beveiliging (IB) of voor bepaalde gegevens nog striktere eisen gelden, bijvoorbeeld alleen opslaan op servers in Nederland. Afwijkingen van deze hoofdregel om gegevens alleen binnen de EER op te slaan kan uitsluitend na toestemming van de Gegevensautoriteit (GA).

Bovenstaande klinkt eenvoudiger dan het is. Veelal is de ene cloud verbonden met een andere cloud (om meer opslagruimte te verkrijgen en om bepaalde verwerkingen mogelijk te maken). Een cloud die onder EER regime valt kan daarmee toch verbonden zijn met bijvoorbeeld een Microsoft of Amazon cloud die onder het regime van de V.S. vallen. Daarnaast hoeft een cloud niet louter voor opslag te worden gebruikt. Een cloud kan bijvoorbeeld ook gebruikt worden om meer functionaliteiten aan een bepaald opgeslagen bestand toe te voegen, bijvoorbeeld om mogelijk te maken dat een bestand zowel op een laptop als op een smartphone uitleesbaar en bewerkbaar is. Het kan dan voorkomen dat een deel van de functionaliteiten slechts in een Amerikaanse cloud mogelijk zijn.

### **IT services en beheer**

IT-beheer, Applicatiebeheer en -onderhoud en Infrastructuurbeheer en -onderhoud (hosting) zijn vormen van IT-dienstverlening waarbij de opdrachtnemer in beginsel altijd een verwerker zal zijn, als de opdrachtnemer toegang heeft tot persoonsgegevens. Er is dan sprake van verwerking van persoonsgegevens. Een verwerkersovereenkomst is nodig.

Bij elke IT-dienstverlening waar het de opdracht is om een systeem of applicatie te leveren en hierbij service te verlenen – bijvoorbeeld onderhoud of ondersteuning – is de opdracht (mede) gericht op het verwerken van persoonsgegevens. Bovendien is er sprake van een uitbesteding van werkzaamheden en heeft de IT-dienstverlener geen zeggenschap over de gegevensverwerking, maar handelt naar de instructies en onder verantwoordelijkheid van de verwerkingsverantwoordelijke. Het feit dat de IT-dienstverlener zelf tot op bepaalde hoogte invulling geeft aan de precieze technische middelen die gebruikt worden, maakt hierbij niet uit. Dit is precies waarvoor IT-dienstverleners worden ingeschakeld en maakt hen nog geen verwerkingsverantwoordelijke.

Wanneer alleen een IT-product wordt afgenomen en daarbij geen service wordt geleverd/geen toegang tot (persoons)gegevens is, is de leverancier van het IT-product geen verwerker. Dit is bijvoorbeeld het geval bij het simpelweg aanschaffen van software.

### **Aanschaf van software via een wederverkoper (reseller)**

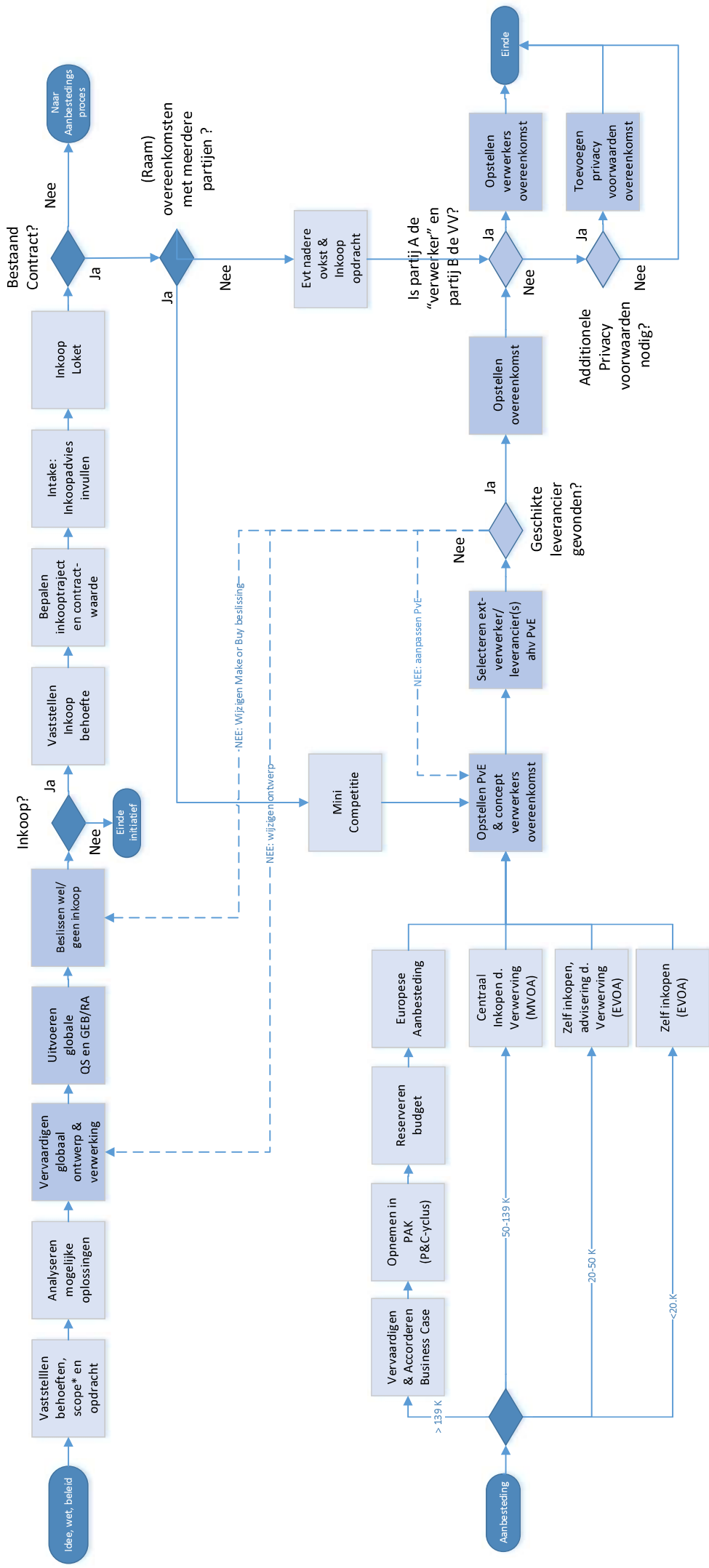
De politie koopt regelmatig software via een reseller. Met de reseller is een raamovereenkomst gesloten. Er is sprake van doorlevering van licenties van de producent van de software (licentieverstrekker) via de reseller, waarvoor met de reseller een nadere overeenkomst wordt gesloten. De reseller treedt slechts op als bemiddelaar (tussenpersoon) bij de totstandkoming van de rechtstreekse verbintenis tussen de licentieverstrekker en de politie en heeft zelf geen toegang tot de software en de gegevens die daarin verwerkt worden.

Aan de hand van de feitelijke omstandigheden moet bepaald worden of de licentieverstrekker persoonsgegevens verwerkt (of anderszins toegang heeft tot de persoonsgegevens) waarvoor de politie verwerkingsverantwoordelijke is. Bepaalt de politie doel en middelen van de verwerking van de persoonsgegevens, dan is de licentieverstrekker een verwerker en is een verwerkersovereenkomst nodig. Een verwerkersovereenkomst is altijd gekoppeld aan een hoofdovereenkomst. Bij licenties zal dat de EULA (End User Licence Agreement) zijn die de politie en de licentieverstrekker doorgaans overeenkomen.

## Bijlage 2 Proces



Inkoopproces en  
PSbD versie 10.pdf



#### Legenda:

QS= Quick Scan

GEB = GegevensbeschermingsEffect Beoordeling

RA = Risko Analyse

PAK = Politie AanbestedingsKalender

P&C = Planning & Control

MVOA = Meervoudig Onderhandse Aanbesteding

EVOA = Enkelvoudig Onderhandse Aanbesteding

PvE = Programma van Eisen

VV = Verwerkingsverantwoordelijke