



**Verwerkersovereenkomst  
Parkeerdata ten behoeve van  
parkeeronderzoeken  
gemeente Amsterdam  
Al 2022-0027**

Voor u ligt de standaard voor een verwerkersovereenkomst van de gemeente Amsterdam.

De gemeente Amsterdam heeft de standaard voor een verwerkersovereenkomst  
"Standaard Verwerkersovereenkomst Gemeenten, versie bijgewerkt op 4 mei 2021/ Versie 2.4"  
van de VNG overgenomen.

**Indien de "Standaard Verwerkersovereenkomst Gemeenten" van de VNG wijzigt, wordt deze standaard voor een verwerkersovereenkomst aangepast volgens de dan geldende bepalingen.**

Gemeente Amsterdam, waarvan het college van Burgemeester en Wethouders de verwerkingsverantwoordelijke is, verder te noemen Verwerkingsverantwoordelijke, hierbij rechtsgeldig vertegenwoordigd door de heer B. Rusken, directeur Parkeren

en

<Bedrijf>, gevestigd te <plaatsnaam>, KVK-nummer <nummer> verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam>, <functie>,

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwegen het volgende:

Partijen hebben op <datum> de <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: levering data parkeeronderzoeken, zowel in bestandsformaat als via een webapplicatie;

Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;

Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;

Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

## **Artikel 1 Definities**

- 1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
- 1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

## **Artikel 2 Ingangsdatum en duur**

- 2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.
- 2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven

en/of wissen van Persoonsgegevens zijn nagekomen.

### **Artikel 3 Onderwerp van deze Verwerkersovereenkomst**

3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

3.2 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.

### **Artikel 4 Inhoudelijke afspraken**

#### **4.1 Beveiligingsmaatregelen**

Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. De wijze waarop Verwerker de passende technische en organisatorische maatregelen aantoont, staat in Bijlage 2.

#### **4.2 Audits**

Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.

#### **4.3 Verwerking buiten de EER**

Verwerker mag Persoonsgegevens buiten de Europese Economische Ruimte (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan vooraf op de hoogte.

#### **4.4 Geheimhouding**

Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.

#### **4.5 Subverwerkers**

De ten tijde van het afsluiten van deze Verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1. Verwerkingsverantwoordelijke verleent hierbij algemene toestemming voor de inschakeling van subverwerkers. Verwerker houdt na de start van de werkzaamheden Verwerkingsverantwoordelijke op de hoogte van de beoogde inschakeling van nieuwe subverwerkers. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.

#### **4.6 Rechten van betrokkenen**

Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Verwerker Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.

#### **4.7 Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging**

Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

### **Artikel 5 Inbreuk in verband met Persoonsgegevens**

5.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24

uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.

5.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen.

5.3 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.

5.4 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

## **Artikel 6 Aansprakelijkheid**

6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.

## **Artikel 7 Beëindigen verwerkersovereenkomst**

7.1 Partijen moeten in de Hoofdovereenkomst afspraken maken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens.

7.2 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

## **Artikel 8 Overige bepalingen**

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

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <.....>

Gemeente Amsterdam

<Naam organisatie>

namens deze: B. Rusken, directeur Parkeren

namens deze: <naam, functie>

plaats: Amsterdam

plaats: <.....>

datum: <.....>

datum: <.....>

**Bijlage 1: Overzicht van te verwerken persoonsgegevens**

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

| Naam verwerking                           | Verwerkingsdoeleinden                          | Categorieën van Betrokkenen    | Categorieën Persoonsgegevens (waaronder bijzondere persoonsgegevens) | Bewaartermijn     | Doorgifte naar derde landen | Doorgifte-instrument | Aanvullende maatregelen (indien van toepassing) |
|-------------------------------------------|------------------------------------------------|--------------------------------|----------------------------------------------------------------------|-------------------|-----------------------------|----------------------|-------------------------------------------------|
| Verrijken scandata geparkeerde voertuigen | Vaststellen parkeerdruk en betalingsbereidheid | Voertuigeigenaren en passanten | Beeldmateriaal, kentekens                                            | Conform bijlage 3 | Nee                         | SFTP                 | Zie bijlage 4                                   |
|                                           |                                                |                                |                                                                      |                   |                             |                      |                                                 |

**Contactgegevens**

|                                                                          |                                                               |
|--------------------------------------------------------------------------|---------------------------------------------------------------|
| Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren) | Naam: <b>nog nader in te vullen</b><br>Contactgegevens:       |
| Contactpersoon Verwerker (NB: Ook buiten kantooruren)                    | Naam:<br>Contactgegevens:                                     |
| Contactgegevens IBD                                                      | telefoonnummer: 070-204 55 11<br>e-mailadres : privacy@vng.nl |

NB: Eventuele wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

**Ingeschakelde subverwerkers**

| Naam en contactgegevens subverwerker | KvK-nummer | Uitbestede verwerkingen | Toepassing |
|--------------------------------------|------------|-------------------------|------------|
|                                      |            |                         |            |
|                                      |            |                         |            |
|                                      |            |                         |            |

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|--|--|--|--|

## **Bijlage 2: Aantonen passend niveau van beveiliging**

### **Normenstelsel**

De verwerker is verplicht volgens de volgende algemeen erkende normen voor informatiebeveiliging te werken:

BIO (BBn) 2;

NEN/ISO 27001 – of dit behalen binnen 6 maanden na ingangsdatum overeenkomst;

Of een aan bovenstaande normen gelijkwaardig normenstelsel, waarbij het bewijs voor gelijkwaardigheid aan de norm wordt geleverd door een onafhankelijke derde/auditor als bedoeld in het ISO-systeem.

### **Toereikendheid**

Bij uitbesteding van beheer en exploitatie van informatiesystemen (dus ook SAAS-toepassingen) moet de toereikendheid van de informatiebeveiliging worden vastgesteld door de volgende op te leveren documenten. 1) en 2) zijn verplicht; 3) is verplicht bij webapplicaties en SAAS-toepassingen.

Verwerker is verplicht om jaarlijks aan Verwerkingsverantwoordelijke te overleggen:

Certificering van het verplichte normenstelsel en verklaring van toepasselijkheid (VVT)

2) Een assurance-rapport (TPM, bijvoorbeeld ISAE3402 of SOC type 2) van een onafhankelijke derde/auditor die ter zake aantoonbaar deskundig is;

3) Rapportages van pen/hacktesten bij webapplicaties en SAAS-toepassingen van een onafhankelijke derde/auditor die ter zake aantoonbaar deskundig is.

Uit de certificering -waarbij de geschiktheid van de leverancier wordt aangetoond-, het assurance-rapport en de pen-en hacktesten en -indien omstandigheden volgens Verwerkingsverantwoordelijke daartoe aanleiding geven- periodieke externe audits blijkt of kan worden afgeleid dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.

**Bijlage 3 – Bewaartermijnen**

| Onderdeel                                          | Beschikbaar<br>vanaf (wkn) | Beschikbaar<br>tot (wkn) | Vernietigd<br>na (wkn) | Opmerking                                                   |
|----------------------------------------------------|----------------------------|--------------------------|------------------------|-------------------------------------------------------------|
| Ongecontroleerde waarneming (bron materiaal)       | 2                          | 4                        | 5                      | alleen beschikbaar voor auditor cq controle proceskwaliteit |
| Gecontroleerde waarneming (bron materiaal)         | 2                          | 4                        | 5                      | alleen beschikbaar voor auditor cq controle proceskwaliteit |
| Gecontroleerde waarneming (geanonimiseerd)         | 2                          | 26                       | 28                     | levering cq beschikbaar voor ETL-proces                     |
| Metadata                                           | 2                          | 26                       | 28                     | levering cq beschikbaar voor ETL-proces                     |
| Maandrapportage                                    | 2                          | 52                       | nvt                    | op te stellen door Opdrachtnemer                            |
| Meetprogramma (jaarprogramma)                      | -4                         | nvt                      | nvt                    | op te stellen door Opdrachtgever                            |
| Meetprogramma op maand/weekniveau                  | -4                         | nvt                      | nvt                    | op te stellen door Opdrachtgever                            |
| Rittenplanning                                     | 0                          | 52                       | nvt                    | op te stellen door Opdrachtnemer                            |
| Ritgegevens                                        | 2                          | 26                       | nvt                    | levering cq beschikbaar voor ETL-proces                     |
| Applicatie (eis 3.2)                               | 8                          | einde+26                 | nvt                    |                                                             |
| Metingen en meetresultaten zichtbaar in applicatie | 2                          | 26                       | 28                     | historie is na 26 weken niet meer in te zien                |

De *geanonimiseerde* foto's worden a) meegeleverd en blijven b) een half jaar bewaard voor tonen in webapp en voor opnieuw leveren. Geanonimiseerd wil zeggen dat kentekens onleesbaar en gezichten onherkenbaar zijn gemaakt.

## **BIJLAGE 4**

### **PRIVACY EN SECURITY EISEN PARKEERONDERZOEKEN**

## Privacy en Security eisen Parkeeronderzoeken

14-09-2021

### Inhoud

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| <a href="#">1.1 Personeel en geheimhouding</a>                                 | 11 |
| <a href="#">1.2 Naleven standaarden</a>                                        | 2  |
| <a href="#">1.3 Beveiliging tegen dataverlies</a>                              | 2  |
| <a href="#">1.4 Bedreigingen en incidenten</a>                                 | 2  |
| <a href="#">1.5 Verwijdering van gegevens</a>                                  | 2  |
| <a href="#">1.6 Data portabiliteit</a>                                         | 2  |
| <a href="#">1.7 Bewaartermijnen</a>                                            | 2  |
| <a href="#">1.8 Exit strategie</a>                                             | 2  |
| <a href="#">1.9 Privacy, rechten van betrokkenen</a>                           | 2  |
| <a href="#">1.10 Privacy, verwerkersovereenkomst</a>                           | 2  |
| <a href="#">1.11 Privacy, beveiligingsmaatregelen</a>                          | 2  |
| <a href="#">1.12 Privacy, verwerkingslocatie</a>                               | 2  |
| <a href="#">1.13 Privacy, impact analyse</a>                                   | 2  |
| <a href="#">1.14 Privacy, Subcontractors</a>                                   | 2  |
| <a href="#">1.15 Autorisaties</a>                                              | 2  |
| <a href="#">1.16 Authenticatie</a>                                             | 2  |
| <a href="#">1.17 Procedure toegangsverlening</a>                               | 2  |
| <a href="#">1.18 Audit</a>                                                     | 2  |
| <a href="#">1.19 Logging en audit trail</a>                                    | 2  |
| <a href="#">1.20 Vulnerability scanning, anti-virus, patching en hardening</a> | 2  |
| <a href="#">1.21 Beveiliging van netwerkverkeer/transport</a>                  | 2  |
| <a href="#">1.22 Architectuur</a>                                              | 2  |
| <a href="#">1.23 Databeveiliging</a>                                           | 2  |
| <a href="#">1.24 Applicatie in de SAAS omgeving</a>                            | 2  |

### 1.1 Personeel en geheimhouding

1. Opdrachtnemer zal voor de leveringen en/of diensten voldoende personen inzetten met voldoende opleiding, vaardigheden en kennis van de bedrijfsvoering en organisatie van Opdrachtgever, om de prestaties te verrichten. Wanneer de hierboven genoemde personen zich bij Opdrachtgever bevinden, of in direct contact met Opdrachtgever staan, zal het personeel van Opdrachtnemer de gedragsvoorschriften van Opdrachtgever naleven. Hiermee zal gevolg gegeven worden aan redelijke verzoeken van Opdrachtgever.
2. Opdrachtnemer zal het bestaan, de aard en de inhoud van de Overeenkomst, evenals overige bedrijfsinformatie van Opdrachtgever geheimhouden en niets daaromtrent openbaar maken zonder schriftelijke toestemming van Opdrachtgever. Opdrachtnemer staat er voor in dat personeel van Opdrachtnemer, overige personeelsleden en derden de bepalingen betreffende gedrag, vertrouwelijkheid en bescherming van gegevens naleven.
3. Personen die werken voor de Opdrachtnemer of (sub)Verwerker moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Opdrachtnemer/Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding. De Opdrachtnemer/verwerker hanteert een integriteitscode/interne gedragscode voor zijn medewerkers waaruit blijkt dat de medewerkers en door de Opdrachtnemer/verwerker ingeschakelde derden de vertrouwelijkheid in acht nemen. De Opdrachtnemer houdt een administratie bij van de getekende geheimhoudingsverklaringen en zal hierover op verzoek van de Opdrachtnemer verantwoording over afleggen.
4. Alle voorwaarden en eisen die gelden voor personeel van Opdrachtnemer zijn ook van toepassing op derden, die in opdracht van Opdrachtnemer diensten verrichten en/of leveringen uitvoeren voor Opdrachtgever, zoals in geval van SAAS dienstverlening de SAAS-leverancier.

### 1.2 Naleven standaarden

5. Naleven standaarden: De software is volgens relevante standaarden beveiligd en van voldoende kwaliteit. De richtlijnen van de Autoriteit Persoonsgegevens (AP), Nationaal Cyber Security Centrum (NCSC), Informatiebeveiligingsdienst voor gemeenten (IBD) en Open Web Application Security Project (OWASP) zijn hierbij normstellend. Opdrachtnemer kan toepassing van deze richtlijnen aantonen voorafgaand aan afsluiten van het contract.
6. Opdrachtnemer is verplicht om jaarlijks aan Opdrachtgever/ Verwerkingsverantwoordelijke te overleggen:
  - a. Certificering van het verplichte normenstelsel (ISO27001) en verklaring van toepasselijkheid (VVT)
  - b. Een assurance-rapport (TPM, bijvoorbeeld ISAE3402 of SOC type 2) van een onafhankelijke derde/auditor die ter zake aantoonbaar deskundig is;
  - c. Rapportages van pen/hacktesten bij webapplicaties en SAAS-toepassingen van een onafhankelijke derde/auditor die ter zake aantoonbaar deskundig is.
7. Opdrachtnemer conformeert zich aantoonbaar (door certificering) aan de NEN/ISO 27001 en past de maatregelen die relevant zijn voor Opdrachtgever met betrekking tot onderhavige Apparatuur toe op de geleverde producten en/of diensten. Indien opdrachtnemer bij het afsluiten van het contract niet beschikt over een geldig ISO27001 certificaat zal de Opdrachtnemer:

- binnen 1,5 jaar een geldig ISO27001 certificaat overleggen. In dit geval zal de Opdrachtnemer per kwartaal schriftelijk over de voortgang van de certificering rapporteren aan de Opdrachtgever.
- 8. De dienstverlening voldoet aantoonbaar aan de relevante normen van de Baseline Informatiebeveiliging Overheid (BIO) op Basis Beveiligings Niveau (BBN) 2. Opdrachtnemer toont aan dat hij aan de normen uit de BIO voldoet (door een GAP analyse). De GAP analyse zal voorafgaand aan het afsluiten van het contract aan Opdrachtgever worden verstrekt en mag geen afwijkingen met grote impact bevatten.
- 9. In geval van SAAS dienstverlening geeft de SAAS-leverancier zekerheid over de getroffen beveiligings- en privacy maatregelen middels een ISAE3402 type II verklaring, alsmede geldige ISO27001, ISO27017 en ISO27018 certificaten.

### **1.3 Beveiliging tegen dataverlies**

- 10. Opdrachtnemer beveiligt alle gegevens van Opdrachtgever op adequate wijze zodanig dat bescherming wordt geboden tegen gegevensverlies als wel toegang tot gegevens door onbevoegden. Met "alle gegevens" wordt bedoeld zowel "data in use" als "data in motion" en "data at rest". Opdrachtnemer informeert Opdrachtgever direct bij een (vermoeden van) toegang door onbevoegden.

### **1.4 Bedreigingen en incidenten**

- 11. Opdrachtnemer dient voor de software en infrastructuur (Apparatuur) doorlopend maatregelen te nemen om bedreigingen en aanvallen zoals onder meer side channel, guest-hopping, hyperjacking en SQL-injection te voorkomen.
- 12. Opdrachtnemer/verwerker implementeert een proces waarbij een (vermoedelijk) beveiligingsincident met betrekking tot de persoonsgegevens binnen 24 uur wordt gemeld aan de Opdrachtgever. Opdrachtnemer/verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.
- 13. Opdrachtgever beslist of een (beveiligings-)incident kan worden gekwalificeerd als datalek en zorgt in dat geval voor de melding aan de Autoriteit Persoonsgegevens en het in kennis stellen van de betrokkenen. Niet door Opdrachtnemer/verwerker gemelde beveiligingsincidenten die leiden tot een boete van de Autoriteit Persoonsgegevens en/of aan een betrokkene toe te kennen schade als gevolg van schending van diens privacy, zal Opdrachtgever verhalen op Opdrachtnemer die deze zal vergoeden.
- 14. In geval van een Inbreuk neemt Opdrachtnemer/verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen.
- 15. Opdrachtnemer/verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien wanneer deze daarom vraagt.

16. Opdrachtgever/Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Opdrachtnemer/verwerker ondersteunt de Opdrachtgever/verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

## **1.5 Verwijdering van gegevens**

17. Op een verifieerbaar authentiek schriftelijk verzoek van Opdrachtgever verwijdert Opdrachtnemer aantoonbaar en gegarandeerd alle betreffende gegevens, ook die op eventuele back-upmedia, volledig en onomkeerbaar, tenzij anders overeengekomen.

## **1.6 Data portabiliteit**

18. Opdrachtnemer staat toe dat alle relevante data op verzoek als archief in een algemeen bruikbaar en bewerkbaar bestandsformaat gedownload kan worden door Opdrachtgever en dan wel naar een andere – door Opdrachtgever aan te wijzen - opdrachtnemer kan worden overgezet, in een algemeen bruikbaar en bewerkbaar bestandsformaat en , met inachtneming van vertrouwelijkheid & integriteit van de data.

## **1.7 Bewaartermijnen**

19. Tijdens de geautomatiseerde scans worden foto's gemaakt die worden gebruikt voor (1) eventuele nacontrole en (2) het op verzoek beoordelen van het gebruik van parkeerplaatsen voor andere doeleinden. De bewaartermijn van de scandata voor scans in categorie (1) geldt dat zij beschikbaar zijn vanaf week 2 tot week 4, en vernietigd zijn na week 5, voor scans/foto's van categorie (2) geldt een soortgelijke termijn.
20. Opdrachtnemer/verwerker vernietigt – na overleg met opdrachtgever/Verwerkersverantwoordelijke - gedurende de looptijd van de Hoofdovereenkomst en de Verwerkersovereenkomst de persoonsgegevens na ommekomst van de bewaartermijn.
21. Het dienstverlening door Opdrachtnemer moet functionaliteit bevatten die Opdrachtgever in staat stelt om de door Opdrachtgever gewenste dan wel wettelijke bewaartermijnen te handhaven:
  - a. Er moet een bewaartermijn (inclusief termijnbewaking) kunnen worden ingericht op basis van een geïdentificeerd werkproces;
  - b. Data en bijbehorende metadata moeten onherstelbaar kunnen worden vernietigd op basis van de opgegeven vernietigingstermijn;
  - c. Van data die voor vernietiging in aanmerking komt moeten overzichten kunnen worden gecreëerd;
  - d. Van de vernietiging van data moet een verklaring worden opgeleverd waarin minimaal wordt aangegeven om welke informatie/data het gaat, dat de vernietiging volledig is uitgevoerd en om hoeveel data het gaat (TB, MB, etc.). Opdrachtgever kan (laten) controleren of deze data daadwerkelijk vernietigd is.
22. Opdrachtnemer garandeert dat bij een backup-recovery geen gegevens terug in productie worden gezet die formeel al vernietigd zijn.

### **1.8 Exit strategie**

23. Partijen moeten in de Hoofdovereenkomst afspraken maken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissen van Persoonsgegevens
24. Opdrachtnemer/Verwerker stelt op schriftelijk verzoek van Opdrachtgever/Verwerkingsverantwoordelijke aan hem, of aan een door Opdrachtgever/Verwerkingsverantwoordelijke aan te wijzen derde, onmiddellijk alle persoonsgegevens ter hand die in het kader van de Verwerkersovereenkomst worden verwerkt. Hieronder worden mede begrepen kopieën en bewerkingen van persoonsgegevens. Een dergelijk verzoek kan door Opdrachtgever/Verwerkingsverantwoordelijke worden gedaan gedurende de looptijd van de Verwerkersovereenkomst en op het moment dat de Hoofdovereenkomst wordt beëindigd.
25. De Opdrachtgever/Verwerkingsverantwoordelijke kan zo nodig eisen stellen aan de wijze van beschikbaarstelling van de persoonsgegevens, waaronder begrepen de eisen aan het bestandsformaat
26. Opdrachtnemer/Verwerker zal te allen tijde bij de hiervoor beschreven overdracht van persoonsgegevens waarborgen dat er geen sprake is van verlies van functionaliteit of (delen van) de persoonsgegevens. De overdracht vindt verder op een zodanige wijze plaats dat de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Opdrachtnemer/verwerker wordt belemmerd. Opdrachtnemer/verwerker is gehouden de na overdracht achtergebleven kopieën te vernietigen.
27. Van de overdracht en de gevraagde vernietiging wordt door Opdrachtnemer/Verwerker een verslag gemaakt. Opdrachtgever/Verwerkingsverantwoordelijke kan van de vernietiging een bewijs verlangen. De kosten van overdracht en vernietiging komen voor rekening van Opdrachtnemer/Verwerker.

### **1.9 Privacy, rechten van betrokkenen**

28. De Opdrachtnemer ondersteunt Opdrachtgever in de naleving van de AVG, inzake de rechten van betrokkenen. Onder meer door het mogelijk te maken dat gedeelten van persoonsregistraties kunnen worden gewijzigd, gewist of beperkt toegankelijk kunnen worden gemaakt. Dit met het oog op het effectief opvolging kunnen gegeven aan een verzoek tot inzage, rectificatie en aanvulling, vernietiging of beperking van verwerking van persoonsgegevens.

### **1.10 Privacy, verwerkersovereenkomst**

29. Verwerkersovereenkomst: Omdat er persoonsgegevens worden verwerkt en de systemen van Opdrachtnemer buiten de organisatie en invloedssfeer van Opdrachtgever (bijvoorbeeld bij SAAS), is Opdrachtnemer (en in geval van SAAS de SAAS-leverancier) bereid een verwerkersovereenkomst (conform de standaard van Opdrachtgever) af te sluiten als onderdeel van de Overeenkomst. Dit betreft de model-verwerkersovereenkomst van de VNG, aangevuld met een addendum met bepalingen die specifiek hebben te gelden voor de Gemeente Amsterdam (zie bijlage). Tevens worden in de Overeenkomst afspraken vastgelegd betreffende aansprakelijkheid en schade in geval van incidenten.

### **1.11 Privacy, beveiligingsmaatregelen**

30. Opdrachtnemer/Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG.

### **1.12 Privacy, verwerkingslocatie**

31. Verwerking van de gegevens door de Opdrachtnemer vindt in principe plaats binnen de Europese Economische Ruimte (EER). Opdrachtnemer/Verwerker mag alleen Persoonsgegevens buiten de EER (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 en 46 AVG. Wanneer er sprake is van een verwerking buiten de EER dan vraagt de Opdrachtnemer/verwerker de Opdrachtgever/verwerkingsverantwoordelijke vooraf om toestemming.

#### **Privacy, impact analyse**

32. Op verzoek van Opdrachtgever/Verwerkingsverantwoordelijke werkt Opdrachtnemer/Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

### **1.13 Privacy, Subcontractors**

33. Opdrachtnemer/Verwerker garandeert te allen tijde expliciet compliance van onderaannemers en gelieerde partners aan de overeengekomen regels met Opdrachtgever. Opdrachtnemer verifieert dit ook actief.
34. De ten tijde van het afsluiten van de Verwerkersovereenkomst bekende subverwerkers vermeldt Opdrachtnemer/Verwerker in de verwerkersovereenkomst.
35. Opdrachtgever/Verwerkingsverantwoordelijke verleent algemene toestemming voor de inschakeling van subverwerkers. Het is Opdrachtnemer/Verwerker verboden, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van Opdrachtgever/Verwerkingsverantwoordelijke, de uitvoering van een Overeenkomst geheel of gedeeltelijk aan derden over te dragen of uit te besteden, dan wel gebruik te maken van ter beschikking gestelde of ingeleende arbeidskrachten.
36. Opdrachtnemer houdt na de start van de werkzaamheden de Opdrachtgever op de hoogte van de beoogde inschakeling van nieuwe subcontractors, waarbij opdrachtgever in aanvulling op het bepaalde van artikel 4.5 van de VNG-Verwerkersovereenkomst en artikel 28, tweede lid, van de AVG door opdrachtgever een termijn van vier weken wordt gegund om bezwaar te kunnen maken tegen de inschakeling van een (sub)verwerker. In deze vier-weken periode is het Opdrachtnemer/verwerker niet toegestaan gebruik te maken van de voorgestelde (sub)verwerker.
37. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.

### **1.14 Autorisaties**

38. Opdrachtnemer garandeert een juiste werking van de software en onderliggende infrastructuur. Een gebruiker mag slechts toegang krijgen tot de gegevens die deze voor de uitoefening van zijn/haar

functie nodig heeft. De software dient een indeling naar rollen dan wel gebruikersprofielen mogelijk te maken. De Opdrachtnemer biedt een autorisatiemodel waarbij de rechten ingesteld moeten kunnen worden conform de wensen van Opdrachtgever.

### **1.15 Authenticatie**

39. Voor alle toegang tot de software en infrastructuur geldt dat authenticatie plaatsvindt door middel van tenminste een wachtwoord en (voor toegang van buiten het ADW domein ): multi-factor authenticatie. De applicatie faciliteert daarom twee Factor Authenticatie (2FA) door middel van de combinatie gebruikersnaam/wachtwoord + Token voor de niet-gemeente Amsterdam medewerker. MFA is verplicht voor toegang van buiten het ADW domein.
40. De applicatie kan gebruik maken van Single of Same Sign On (SSO) op basis van het SAML2 protocol of het OAUTH2 protocol. De gemeente Amsterdam medewerker authenticiseert zich hiermee conform de Identity Access Management (IAM) oplossing van de gemeente Amsterdam. De medewerker kan hiermee inloggen met de Amsterdamse netwerk inlognaam en wachtwoord en token.
41. Opdrachtnemer biedt de mogelijkheid dat een gebruiker zélf zijn wachtwoord kan wijzigen waarbij eisen aan constructie, geldigheidsduur en toepassing zijn gebaseerd op het vigerende wachtwoordbeleid van Opdrachtgever. Accounts zonder wachtwoordbeveiliging of met hetzelfde wachtwoord als een ander account zijn niet toegestaan. Voor toegang over publieke netwerken (van buiten het ADW domein) geldt dat altijd multi-factor authenticatie plaatsvindt.
42. Wachtwoorden worden bij invoer niet op het scherm getoond en worden versleuteld (gehashed) opgeslagen, waarbij de versleutelde waarde niet zichtbaar kan worden gemaakt via beheerinterfaces en/of reverse engineering.

### **1.16 Procedure toegangsverlening**

43. Opdrachtnemer geeft inzicht in hoe het aanvragen en muteren van toegang door gebruikers (inclusief toegang op afstand) plaatsvindt en hoe wachtwoorden worden toegewezen. De Opdrachtnemer houdt een administratie van uitgegeven en ingetrokken accounts bij. Deze administratie is voor Opdrachtgever benaderbaar en inzichtelijk.

### **1.17 Audit**

44. Indien naar het oordeel van Opdrachtgever/Verwerkingsverantwoordelijke omstandigheden daartoe aanleiding geven, is Verwerkingsverantwoordelijke gerechtigd, ook in de situatie dat Opdrachtnemer/Verwerker beschikt over een geldige certificering, de Opdrachtnemer/verwerker te verzoeken de verwerking van persoonsgegevens te doen laten controleren door middel van een audit. Onder een audit moet tevens worden begrepen een pen-en hacktest waarmee kan worden aangetoond dat de applicatie en de infrastructuur waarmee persoonsgegevens worden bewerkt voldoen aan de Open Web Application Security Project (OWASP) criteria en de in de Verwerkersovereenkomst nader gespecificeerde criteria.
45. Opdrachtnemer/Verwerker is verplicht Opdrachtgever/Verwerkingsverantwoordelijke of de - in opdracht van Verwerkingsverantwoordelijke- controlerende instantie toe te laten en alle medewerking

te verlenen, waaronder het verlenen van de verlangde informatie, zodat de controle daadwerkelijk uitgevoerd kan worden. Verwerkingsverantwoordelijke zal de audit slechts (laten) uitvoeren na een voorafgaande melding aan Opdrachtnemer/verwerker en met inachtneming van een redelijke termijn.

46. De kosten van de hiervoor genoemde audit wordt gedragen door Opdrachtgever/Verwerkingsverantwoordelijke tenzij de auditor een of meer tekortkomingen van niet ondergeschikte aard van Opdrachtnemer/verwerker constateert, die ten nadele zijn van Verwerkingsverantwoordelijke.
47. De kosten voor eventuele hertesten, herstelwerkzaamheden en het oplossen van de bevindingen worden gedragen door Opdrachtnemer/Verwerker, tenzij Partijen in overleg anders overeenkomen.
48. Indien Opdrachtnemer/Verwerker niet beschikt over een geldige certificering als bedoeld in 4.2. van de Verwerkersovereenkomst rapporteert Opdrachtnemer/Verwerker jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van het bepaalde in de Verwerkersovereenkomst. Deze rapportage betreft ook, indien van toepassing, de werkzaamheden van door hem ingeschakelde derden.. Opdrachtnemer/verwerker zal na een verzoek daartoe van Verwerkingsverantwoordelijke minimaal eens per jaar kosteloos een TPM c.q. een verklaring van een onafhankelijke externe deskundige aan Verwerkingsverantwoordelijke verstrekken over de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen.

#### **1.18 Logging en audit trail**

49. Logging: Binnen de applicatie houdt Opdrachtnemer een niet-muteerbare audit trail bij waarin automatisch registratie en opslag van de volgende gegevens plaatsvindt:
  - a. alle handelingen (functionaliteiten) die door gebruikers met betrekking tot metagegevens, processen, documenten, dossiers of andere objecten worden verricht;
  - b. de gebruiker, datum en tijd van de uitvoering van de handeling binnen de Systeemprogrammatuur.Opdrachtnemer stelt deze informatie op verzoek beschikbaar aan Opdrachtgever.

## **Technische maatregelen voor beveiliging van de infrastructuur**

### **1.19 Vulnerability scanning, anti-virus, patching en hardening**

50. Alle betrokken systeemcomponenten en onderliggende infrastructuur (Apparatuur) worden frequent (ten minste driemaandelijks en na elke significante verandering in de (samenstelling van) de Apparatuur en systeemcomponenten) gescand op kwetsbaarheden volgens marktconforme 'best practices'.
51. Anti-virus protectie en bewaking van anti-virus alerts wordt toegepast op alle systeemcomponenten. Toegepaste vulnerability scanning en anti-virus tooling vereisen goedkeuring van Opdrachtgever. Er is een schriftelijk vastgelegd proces voor vulnerability scanning en anti-virus monitoring en follow up van noodzakelijke verbeteringen bij Opdrachtnemer danwel de SAAS-leverancier van toepassing.
52. Alle betrokken systeemcomponenten worden (gelijk aan het scannen op kwetsbaarheden) frequent gepatcht volgens marktconforme 'best practices'. Kritische security patches moeten direct worden toegepast. Er is een schriftelijk vastgelegd proces voor patching en wijzigingsbeheer bij Opdrachtnemer danwel de SAAS-leverancier van toepassing.
53. Alle betrokken systeemcomponenten zijn ontworpen om en getest op het voorkomen van gegevensverlies, lekken van gegevens en systeemproblemen. Systeemcomponenten dienen veilig te worden geconfigureerd conform best practice hardening guidelines. Er is een schriftelijk vastgelegd proces voor hardening voor alle systeemcomponenten bij Opdrachtnemer danwel de SAAS-leverancier van toepassing.

### **1.20 Beveiliging van opslag/netwerkverkeer/transport**

54. De opdrachtnemer zorgt voor versleutelde opslag van de gegevens tijdens uitvoering van het scanproces, voor versleutelde communicatie van de gegevens van de scanauto's naar de omgeving waarin de gegevens worden verwerkt (SAAS omgeving) en voor versleutelde communicatie vanuit de SAAS omgeving naar de gebruikers/afnemers van de gegevens.
55. De Opdrachtnemer zorgt ervoor dat gezichten van herkenbare personen in de resultaten van de scans worden geblurd, direct bij de centrale verwerking op de thuisbasis of in de SAAS omgeving.
56. Data die de Opdrachtnemer heeft verwerkt wordt geanonimiseerd geleverd aan de afnemer(s) binnen de Opdrachtnemer/gemeente.
57. De gebruikers interface van de applicatie die wordt geleverd door Opdrachtnemer maakt gebruik van web-services die via het HTTP applicatie-protocol versleuteld (HTTPS) wordt aangeboden.
58. Het netwerkverkeer en koppelingen met andere omgevingen binnen is in detail gedocumenteerd.
59. Bij koppelingen (in- en uitgaand) biedt de applicatie een mechanisme om het datatransport te versleutelen (TLS 1.2 of hoger).
60. Opdrachtnemer zorgt er voor dat versleuteling van gegevens tijdens opslag, informatie-uitwisseling en andere vormen van communicatie plaatsvindt in overeenstemming met de risicoclassificatie van die

gegevens waarbij persoons- en andere vertrouwelijke gegevens te allen tijde via een versleutelde verbinding worden verzonden. De applicatie en de onderliggende infrastructuur (Apparatuur) wordt te allen tijde benaderd op basis van een beveiligde verbinding conform de laatste bekende beveiligingsinzichten (normenkader: BIO-Overheid) en stand van de techniek.

61. Bij systeemkoppelingen (in- en uitgaand) vindt er wederzijds systeemauthenticatie plaats door middel van basic toegang authenticatie in combinatie met HTTPS of PKI-overheid certificaten afgedwongen door de dataclassificatie.
62. Toegang tot de SaaS oplossing via een Internet Browser vindt versleuteld plaats ("https over poort 443") met TLS1.2 of hoger.

### **1.21 Architectuur**

63. De SaaS oplossing is horizontaal en/of verticaal schaalbaar. Het systeem is in staat om schommelingen in gebruik binnen de marges van de gebruiksvoorwaarden, adequaat op te vangen.
64. Communicatie met het gemeentelijke infrastructuur vindt alleen plaats via het daarvoor bestemde koppelvlak.
65. Data van de gemeente mag niet voor andere gebruikers beschikbaar komen. In geval van "multi-tenancy" oplossingen mogen API-services en netwerk-services shared zijn, maar data niet. De data blijft alleen per tenant toegankelijk.
66. In geval van toepassing van IT infrastructuur die gedeeld wordt met derde partijen (bijvoorbeeld SaaS) worden er door Opdrachtnemer afdoende maatregelen getroffen om te voorkomen dat gegevens van Opdrachtgever onbedoeld worden gedeeld met derden dan wel worden gecombineerd met gegevens van andere klanten door aggregatie of interferentie.
67. Leverancier heeft netwerksegmentatie geïmplementeerd waarbij omgevingen met verschillende beveiligingsniveaus van elkaar gescheiden worden. Onder andere de ontwikkel-, acceptatie-, en productie omgevingen.
68. Output, exports of gecreëerde bestanden worden via de gebruikers interface van de applicatie benaderbaar gemaakt. Tevens moeten deze output compatible zijn met MS Office 2013 of hoger.

### **1.22 Databeveiliging**

#### **Applicatie standaarden**

69. De applicatie dient door alle type gebruikers te kunnen worden gebruikt via de actuele versies van de gangbare internet browsers waaronder Internet Explorer, Firefox en Chrome. Specifieke client-applicaties of plugins zijn niet toegestaan.

## Connectiviteitsstandaarden

70. De mogelijkheid om vanuit de SAAS oplossing, mail te sturen naar medewerkers binnen de gemeente via het publieke mail adres van de betreffende medewerker (bijvoorbeeld: "[voornaam.achternaam@amsterdam.nl](mailto:voornaam.achternaam@amsterdam.nl)"): Richting: van de SaaS oplossing naar het MX record van het domain "amsterdam.nl". Batch/Realtime: Realtime, Transport/Bestandsformaat: SMTP
71. Voor koppelingen tussen de SAAS oplossing en gemeentelijke systemen in beide richtingen:  
Batch/Realtime: Batch/Scheduled en/of Realtime. Transport: Data uitwisseling via REST/SOAP over HTTPS of bestandsuitwisseling via SFTP, FTPS of HTTPS. Bestandsformaat: XLSx, JSON, CSV of XML. Beveiliging: gebruikersnaam + wachtwoord + certificaat, gebruikersnaam + wachtwoord of SAML 2.0
72. Voor koppelingen, integratie, import en export vindt data uitwisseling plaats via bestanden en protocollen die voorkomen in de lijst van open standaarden <https://www.forumstandaardisatie.nl/open-standaarden> of de facto standaarden die gelden in het parkeer-domein.
73. De leverancier zorgt voor de complete implementatie (technisch en functioneel) van koppelingen met andere SAAS-leveranciers. De gemeente Amsterdam stelt daarbij de informatie beveiligingskaders vast. Het gaat hier om de bestaande en in de toekomst nog aan te leggen koppelingen met andere SAAS-leveranciers.

### 1.23 Applicatie in de SAAS omgeving

74. De gemeente Amsterdam verwacht van SAAS-leveranciers een actuele kennis op het gebied van risico's, kwetsbaarheden en security.
75. <sup>1</sup>U/TV.01 Wachtwoorden worden gebruikt op basis van de geldende beveiligingseisen uit de BIO en worden eenrichting-versleuteld (hash en salt) opgeslagen.
76. U/WA.02 Het applicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
77. U/PW.05 Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
78. U/NW.04 De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.
79. C.06 In de applicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
80. C.07 De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
81. C.08 Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van applicaties tijdig, geautoriseerd en getest worden doorgevoerd.
82. C.10 Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest.

---

<sup>1</sup> Betreft nummering van normen uit de NCSC 'ICT beveiligingsrichtlijnen voor web applicaties'