Verwerkersovereenkomst

Waterschap Drents Overijsselse Delta
Dokter van Deenweg 186
8025 BM Zwolle
088-2331200
info@wdodelta.nl

Partijen/Ondergetekenden:

1 Waterschap Drents Overijsselse Delta zetelend te Meppel, en vertegenwoordigd door mevrouw I. Geveke*, plv. Secretaris-Directeur,* hierna te noemen: "Verwerkingsverantwoordelijke";

en

2 *<volledige naam en rechtsvorm contractant>*, *<statutair>* gevestigd te *<plaats>*, te dezen vertegenwoordigd door *<de heer/mevrouw> <naam>*, *<functie>,* hierna te noemen: "Verwerker";

overwegen het volgende:

I Verwerkingsverantwoordelijke en Verwerker zijn op *<datum>* een overeenkomst met registratienummer *<invullen>* aangegaan ten behoeve van Fysieke toegangsbeveiliging (hierna: de Overeenkomst);

II Verwerker verwerkt Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke in het kader van de Overeenkomst;

III Verwerkingsverantwoordelijke is ingevolge artikel 28 lid 1 AVG verplicht uitsluitend een beroep te doen op een verwerker die afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van betrokkene zijn gewaarborgd;

IV Partijen leggen hun afspraken over de verwerking van Persoonsgegevens door Verwerker vast in deze verwerkersovereenkomst (hierna: Verwerkersovereenkomst) als bedoeld in artikel 28 lid 3 AVG;

V Op de verwerking van Persoonsgegevens door Partijen zijn de AVG en de UAVG van toepassing;

en komen het volgende overeen:

1 Begripsbepalingen

1.1 In de Verwerkersovereenkomst wordt verstaan onder:

a. "AVG": algemene verordening gegevensbescherming (Verordening (EU) 2016/679);

b. "Bijlagen": bijlagen bij de Verwerkersovereenkomst die deel uitmaken van de Verwerkersovereenkomst;

c. "Inbreuk in verband met persoonsgegevens" (datalek): een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. (artikel 4 onder 12) AVG);

d. "Persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de Betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. (artikel 4 onder 1) AVG);

e. "Subverwerker" (Derde): een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder

rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om de Persoonsgegevens te verwerken. (artikel 4 onder 10) AVG);

f. "Toezichthouder": de toezichthoudende autoriteit zoals bedoeld in artikel 51 AVG. In Nederland is dat de Autoriteit Persoonsgegevens;

g. "UAVG": Uitvoeringswet Algemene verordening gegevensbescherming;

1.2 Indien een in de Verwerkersovereenkomst gebruikt begrip niet onder 1.1 is gedefinieerd geldt de definitie uit de AVG. De begrippen kunnen zonder verlies van hun inhoudelijke betekenis in enkelvoud en/of in meervoud worden gebruikt.

2 Duur van Verwerkersovereenkomst

2.1 De Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

2.2 De Verwerkersovereenkomst eindigt nadat en voor zover Verwerker alle Persoonsgegevens overeenkomstig artikel 9 heeft terugbezorgd en/of gewist, met inachtneming van het bepaalde in artikel 11.1.

2.3 De Verwerkersovereenkomst kan niet tussentijds worden beëindigd.

3 Verplichtingen Verwerker

3.1 Verwerker verwerkt de Persoonsgegevens uitsluitend namens en in opdracht van Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst. Verwerker verwerkt de Persoonsgegevens in overeenstemming met de (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 Verwerker verwerkt de Persoonsgegevens niet voor enig ander doel dan waarvoor deze zijn ontvangen zelfs niet wanneer deze in een zodanige vorm zijn gebracht dat deze niet tot Betrokkenen herleidbaar zijn, behoudens dwingendrechtelijke verplichtingen.

3.3 Verwerker garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de AVG en andere toepasselijke wet- en regelgeving voldoet en de bescherming van de rechten van de Betrokkene zijn gewaarborgd.

3.4 Onderwerp, aard en doeleinden van de Verwerkingen die Verwerker uitvoert in het kader van de Overeenkomst, de categorieën van Betrokkenen en de soort van Persoonsgegevens zijn omschreven in Bijlage 1.

3.5 Verwerker houdt een register bij, zoals bedoeld in artikel 30 lid 2 AVG, van alle categorieën van verwerkingsactiviteiten die Verwerker ten behoeve van Verwerkingsverantwoordelijke uitvoert.

3.6 Verwerker informeert Verwerkingsverantwoordelijke onverwijld over door Verwerker ontvangen verzoeken van Betrokkenen of de Toezichthouder. Verwerker verleent aan Verwerkingsverantwoordelijke alle medewerking, zodat Verwerkingsverantwoordelijke binnen de wettelijke termijnen kan voldoen aan de verplichtingen op grond van de AVG met betrekking tot Betrokkenen of de Toezichthouder.

3.7 Verwerker verwerkt Persoonsgegevens niet buiten de Europese Economische Ruimte (EER), tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Verwerkingsverantwoordelijke en behoudens afwijkende wettelijke verplichtingen.

4 Geheimhoudingsplicht

4.1 Verwerker en medewerkers/personen die werken voor of namens Verwerker zijn verplicht tot geheimhouding van alle Persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt en/of zelf verzamelt in het kader van de Overeenkomst.

4.2 Verwerker stelt de Persoonsgegevens niet aan derden ter beschikking, tenzij Verwerkingsverantwoordelijke, voorafgaande aan het ter beschikking stellen, schriftelijke toestemming heeft gegeven.

4.3 Verwerker draagt er zorg voor dat de onder 4.1 bedoelde medewerkers/personen een geheimhoudingsverklaring hebben ondertekend.

5 Meldplicht Inbreuk in verband met Persoonsgegevens (datalek)

5.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging en **uiterlijk binnen vierentwintig (24) uur na kennisneming** over een Inbreuk in verband met Persoonsgegevens of een redelijk vermoeden van een Inbreuk in verband met Persoonsgegevens. Deze verplichting geldt onverminderd de verplichting van Verwerker de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken en indien ongedaan making onmogelijk is, deze gevolgen te beperken.

5.2 Verwerker verschaft op het eerste verzoek van Verwerkingsverantwoordelijke, alle inlichtingen waar Verwerkingsverantwoordelijke om verzoekt om de in 5.1 bedoelde Inbreuk in verband met Persoonsgegevens te kunnen beoordelen. Daarbij overlegt Verwerker in ieder geval de informatie aan Verwerkingsverantwoordelijke zoals omschreven in Bijlage 2.

5.3 Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van Inbreuken in verband met Persoonsgegevens, zoals bedoeld onder 5.1 en zal Verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt Verwerkingsverantwoordelijke op de hoogte van materiële wijzigingen in het plan van aanpak.

5.4 Alleen Verwerkingsverantwoordelijke verricht meldingen aan de Toezichthouder.

5.5 Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) Inbreuken in verband met Persoonsgegevens, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in Bijlage 2 is opgenomen. Verwerker geeft op eerste verzoek van Verwerkingsverantwoordelijke inzage in het logboek.

6 Beveiligingsmaatregelen en audits

6.1 De door Verwerker genomen passende technische en organisatorische maatregelen om de Persoonsgegevens, te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking zijn opgenomen in Bijlage 4.

6.2 Verwerker toont aan door middel van een door een onafhankelijke, externe deskundige uitgevoerde audit/certificering dat Verwerker voldoet aan de AVG en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens. De kosten van deze audit/certificering zijn voor rekening van Verwerker.

6.3 Verwerker verricht ten minste één keer per twee jaar een audit, zoals bedoeld in artikel 6.2. Indien bijzondere categorieën van Persoonsgegevens (als bedoeld in artikel 9 AVG) worden verwerkt, verricht Verwerker ten minste één keer per jaar een audit.

6.4 Verwerkingsverantwoordelijke heeft het recht bij Verwerker een audit te laten uitvoeren indien hij het vermoeden heeft dat Verwerker in ernstige mate tekortschiet in de bescherming van de Persoonsgegevens. De kosten van deze audit zijn voor rekening van Verwerkingsverantwoordelijke, tenzij de auditor één of meer tekortkomingen betreffende de bescherming van de Persoonsgegevens van niet ondergeschikte aard constateert.

6.5 Verwerker voert de door de auditor of Verwerkingsverantwoordelijke aangegeven aanbevelingen zo spoedig mogelijk uit.

6.6 Verwerker rapporteert jaarlijks over de opzet en werking van de maatregelen en procedures, gericht op naleving van de Verwerkersovereenkomst. Daarbij stelt Verwerker alle informatie ter beschikking die nodig is om aan te tonen dat de

verplichtingen uit deze Verwerkersovereenkomst zijn en worden overgenomen.

7 Subverwerkers

7.1 Verwerker maakt alleen gebruik van nieuwe Subverwerkers na voorafgaande toestemming van Verwerkingsverantwoordelijke.

7.2 Verwerkingsverantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden op het gebied van geheimhouding en ter naleving van de verplichtingen uit de Verwerkersovereenkomst.

OF

7.3 Verwerker stelt Verwerkingsverantwoordelijke vooraf schriftelijk op de hoogte van de benoeming van een nieuwe Subverwerker, met een volledige beschrijving van de door de Subverwerker te verrichten verwerkingen. Indien Verwerkingsverantwoordelijke redelijke bezwaren heeft tegen een dergelijke nieuwe Subverwerker, dan zal Verwerkingsverantwoordelijke Verwerker binnen 21 (één-en-twintig) kalenderdagen na ontvangst van de kennisgeving daarvan schriftelijk op de hoogte stellen.

7.4 Indien Verwerkingsverantwoordelijke bezwaar maakt tegen een Subverwerker, dan zal de Verwerker zich redelijkerwijs inspannen om de betreffende diensten aan te passen of een andere commercieel redelijke aanpassing in de levering van de betreffende diensten aan te bevelen om verwerking van persoonsgegevens door de betreffende Subverwerker te voorkomen.

7.5 In Bijlage 3 */….bijlage 3 invullen…/* zijn vermeld de bij het aangaan van de Verwerkersovereenkomst door Verwerker ingeschakelde Subverwerkers.

7.6 Wanneer Verwerker een Subverwerker inschakelt, blijft Verwerker aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit de Verwerkersovereenkomst. Verwerker garandeert dat deze Subverwerkers schriftelijk vergelijkbare plichten op zich nemen als tussen Verwerkingsverantwoordelijke en Verwerker zijn overeengekomen. Op verzoek van Verwerkingsverantwoordelijke geeft Verwerker inzage in de overeenkomsten met Subverwerkers.

8 Aansprakelijkheid

8.1 Ingevolge artikel 82 lid 2 van de AVG is Verwerker aansprakelijk voor de schade die door Verwerker is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot Verwerker gerichte verplichting van de AVG of buiten dan wel in strijd met de rechtmatige instructies van Verwerkingsverantwoordelijke is gehandeld.

8.2 Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle aanspraken en boeten ingesteld tegen en opgelegd aan Verwerkingsverantwoordelijke, die een gevolg zijn van het niet voldoen door Verwerker aan de AVG, de UAVG, andere toepasselijke wet- en regelgeving, of de Verwerkersovereenkomst betreffende de verwerking van Persoonsgegevens door Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot medewerkers en/of Subverwerkers. Op deze vrijwaringsclausule kan geen beroep worden gedaan indien Verwerker bewijst dat hij geen schuld heeft aan de schade toebrengende gebeurtenis.

9 Terugbezorgen en/of wissen Persoonsgegevens

9.1 Zodra de Overeenkomst is beëindigd, draagt Verwerker naar keuze van Verwerkingsverantwoordelijke zorg voor:

a. het aan Verwerkingsverantwoordelijke terugbezorgen van alle of een door Verwerkingsverantwoordelijke bepaald gedeelte van aan Verwerker ter beschikking gestelde Persoonsgegevens en/of

b. het wissen van (een deel van) de Persoonsgegevens op alle locaties.

9.2 Bij beëindiging van de Overeenkomst verwijdert Verwerker kopieën, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen en behoudens afwijkende wettelijke voorschriften.

10 Contactpersonen en melden Inbreuk in verband met Persoonsgegevens ("datalek")

10.1 Contactpersoon voor Verwerkingsverantwoordelijke is: Functionaris Gegevensbescherming van de verwerkingsverantwoordelijke.

10.2 Contactpersoon voor Verwerker is: *<…naam contactpersoon en functie…>*.

10.3 Verwerker meldt een (mogelijke) Inbreuk in verband met Persoonsgegevens ("datalek") bij de Functionaris Gegevensbescherming van verwerkingsverantwoordelijke, middels een mail naar fg@wdodelta.nl.

11 Ingebrekestelling, aansprakelijkheid

11.1 In afwijking van de algemene voorwaarden die van toepassing zijn op de Overeenkomst, regelen de volgende bepalingen het aansprakelijkheidsregime voor de verplichtingen die voortvloeien uit de Verwerkersovereenkomst.

11.2 Indien de Opdrachtnemer tekortschiet in de nakoming van de verplichting uit deze Verwerkersovereenkomst kan Opdrachtgever hem in gebreke stellen. Opdrachtnemer is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de Opdrachtnemer een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Opdrachtnemer in verzuim.

11.3 Ingevolge artikel 82 van de AVG is Opdrachtnemer aansprakelijk voor de schade die door Opdrachtnemer is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot Opdrachtnemer gerichte verplichting van de AVG of buiten dan wel in strijd met de rechtmatige instructies van Opdrachtgever is gehandeld.

11.4 Opdrachtnemer vrijwaart Opdrachtgever voor alle aanspraken, boeten en/of maatregelen van derden, daaronder begrepen Betrokkenen en de Toezichthouder, die jegens Opdrachtgever worden ingesteld of opgelegd wegens een schending van de Verwerkersovereenkomst en/of de AVG en/of andere toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens door of namens Opdrachtnemer en/of door Opdrachtnemer ingeschakelde (rechts)personen, waaronder maar niet beperkt tot personeel van Opdrachtnemer en/of Sub-verwerkers. Op deze vrijwaringsclausule kan geen beroep worden gedaan wanneer de Verwerker bewijst dat hij geen schuld heeft aan de schade toebrengende gebeurtenis.

11.5 Bij niet gemelde incidenten waar persoonsgegevens bij betrokken zijn, vergoedt Opdrachtnemer een eventueel door Opdrachtgever ontvangen boete en de opgelopen schade aan Opdrachtgever.

12 Overige bepalingen

11.1 Al hetgeen in deze Verwerkersovereenkomst naar zijn aard bestemd is om ook na het einde van de Verwerkersovereenkomst van kracht te blijven, blijft na beëindiging daarvan tussen Partijen van kracht.

11.2 In geval van strijdigheid tussen de Overeenkomst en Verwerkersovereenkomst, prevaleren de bepalingen van de Verwerkersovereenkomst.

11.3 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

Aldus in tweevoud opgemaakt op *<..datum..>* te *<…plaats..>*

Namens Verwerkingsverantwoordelijke

Namens <naam Verwerker>

<…handtekening…>

Naam, functie

<..naam en functie…>

<…handtekening…>

Naam, functie

<…naam en functie…>

Bijlage 1 – De Verwerking van persoonsgegevens

1. **Onderwerp/aard van de verwerking**
   Op basis van rollen en autorisaties rechtmatige toegang te kunnen verlenen aan medewerkers van de Verwerkingsverantwoordelijke en derden die toestemming hebben verkregen.

2. **Doeleinden van de verwerkingen**
   Conform de relevante en geldende wet- en regelgeving de objecten en locaties van verwerkingsverantwoordelijke beter te beveiligen, concreet om toegang te verlenen aan medewerkers en derden en de locatie of het object ook weer te kunnen verlaten.

   In geval van een incident wordt gebruikgemaakt van loggegevens om te toetsen wie tot de aangewezen locaties toegang heeft verkregen. Denk hierbij bijvoorbeeld aan de serverruimtes. Hierbij is het uitdrukkelijk niet de bedoeling om medewerkers en deze genoemde derden te volgen.

3. **Grondslag van de verwerking**
   De Verwerkingsverantwoordelijke baseert de verwerking van de betreffende gegevens op het gerechtvaardigd belang als bedoeld in artikel 6 lid 1 onder f van de AVG. Dit belang vloeit voort uit de noodzaak om de veiligheid van personen en eigendommen te waarborgen, het kunnen registreren en controleren van toegang tot locaties en het voorkomen van onbevoegde toegang. Deze verwerkingen wegen zwaarder dan de belangen of fundamentele rechten en vrijheden van de betrokkenen. De verwerking wordt derhalve aangemerkt als noodzakelijk en proportioneel in relatie tot het nagestreefde doel, mede omdat uitsluitend de minimaal benodigde persoonsgegevens worden verwerkt en passende waarborgen worden getroffen om de privacy van betrokkenen te beschermen.

4. **Categorieën betrokkenen**
   - Medewerkers
   - Inhuur (daaronder vallen ook bijv. schoonmakers)
   - Bezoekers
   - Bestuurders

5. **Beschrijving te verwerken persoonsgegevens**

   De aard van de te verwerken persoonsgegevens verschilt per toegangsmaatregel. Hieronder wordt per toegangsmaatregel uiteengezet welke persoonsgegevens noodzakelijk zijn.

   Toegangsdruppel/RFID pas
   - Uniek ID van de druppel/pas (RFID-tagnummer)
   - Gebruikersidentiteit (naam, personeelsnummer, functie/rollen/taken) m.b.v. een koppeling met de IAM-applicatie van Verwerkingsverantwoordelijke waarbij slechts de genoemde gegevens worden gekoppeld.
   - Toegangsrechten (deuren/zones)
   - Loggegevens (tijdstip, locatie)

- Status van de druppel/pas (actief, geblokkeerd, verloren)

Fysieke toegangspas
- Pasnummer / chip-ID
- Naam en foto van de gebruiker
- Afdeling / functie / rollen / taken
- Toegangsprofiel
- Geldigheidsduur van de pas
- Loggegevens van gebruik

Toegangsmaatregel: Auto (kentekenherkenning)
- Kenteken
- Gekoppelde gebruiker
- Tijdstip van binnenkomst/vertrek
- Eventueel voertuigtype of merk

Toegangsmaatregel: Telefoon / App
Benodigde gegevens:
- Gebruikersaccount (e-mailadres, gebruikersnaam)
- Device-ID of app-token
- Gegevens ter identificatie van gebruiker. Hierbij wordt gebruikgemaakt van biometrie: gezichtsherkenning en wachtwoord. Deze biometrie verloopt uitsluitend via lokale opslag op het device en wordt niet zelfstandig verwerkt door Verwerkingsverantwoordelijke en/of Verwerker
- Locatiegegevens
- Toegangslogboeken
- Pushmeldingen of notificatiegeschiedenis

Bijlage 2 - Inlichtingen verschaffen om incidenten te beoordelen ter uitwerking van artikel 5.2

Verwerker zal alle inlichtingen verschaffen die Verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft Verwerker in ieder geval de volgende informatie aan Verwerkingsverantwoordelijke:

- wat de (mogelijke) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij Opdrachtnemer of bij een door hem ingeschakelde derde of onderaannemer;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Bijlage 3 - Subverwerkers als bedoeld in artikel 7.2

Verwerker maakt bij het aangaan van de Verwerkersovereenkomst gebruik van onderstaande Subverwerkers.

Subverwerker 1	
Naam:	
Vestigingsadres:	
Registratienummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden gesteld door Verwerkingsverantwoordelijke:	
Naam functionaris voor de verwerking:	
E-mail:	
Telefoonnummer:	

Subverwerker 2	
Naam:	
Adres:	
Registratienummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden gesteld door Verwerkingsverantwoordelijke:	
Naam functionaris voor de verwerking:	
E-mail:	
Telefoonnummer:	

Bijlage 4 – Technische en organisatorische maatregelen ter uitwerking van artikel 6

De verwerker treft passende technische en organisatorische maatregelen om de persoonsgegevens die worden verwerkt in het kader van het fysieke toegangscontrolesysteem te beveiligen. Deze maatregelen zijn afgestemd op de aard van de verwerking, de risico's, de stand van de techniek en de relevante wet- en regelgeving (AVG, BIO, NEN-ISO/IEC 27001).

1. Certificering en aantoonbaarheid

- Verwerker dient te beschikken over een geldig ISO/IEC 27001-certificaat voor een Information Security Management System (ISMS). Dit certificaat dient te zijn afgegeven door een onafhankelijke certificerende instelling die geaccrediteerd is door een nationale of internationale accreditatie-instantie (zoals RvA, UKAS, DAkkS of een vergelijkbare instantie).
- De scope van het ISMS dient expliciet de dienstverlening, processen, systemen en locaties te omvatten die onder deze overeenkomst vallen.
- Verwerker dient op eerste verzoek van Verwerkingsverantwoordelijke het meest recente en geldige certificaat, een actuele Verklaring van Toepasselijkheid (Statement of Applicability, SoA) en een auditrapport (niet ouder dan twaalf maanden) te overleggen waaruit blijkt dat het ISMS effectief functioneert en onderhouden wordt.
- Indien Verwerker (sub)verwerkers inschakelt voor de uitvoering van de diensten, dient Verwerker ervoor zorg te dragen dat deze aantoonbaar onder de beheersmaatregelen van het ISMS vallen dan wel een gelijkwaardig beveiligingsniveau hanteren.

2. Encryptie en transmissie

- Verwerker dient alle datatransmissies (waaronder communicatie tussen hardware, mobiele applicaties en webapplicaties) te versleutelen. Alle TLS-verbindingen dienen te voldoen aan de op het moment van uitvoering geldende ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), zoals vastgesteld door het Nationaal Cyber Security Centrum (NCSC).

3. Logging en monitoring

- Verwerker dient alle security-logging van applicaties, mobiele applicaties en hardware (waaronder card-readers) te ontsluiten naar de centrale logserver van Verwerkingsverantwoordelijke.

4. Mobiele applicaties

- Verwerker dient mobiele applicaties blijvend te beschermen tegen de meest actuele OWASP Mobile Top 10 kwetsbaarheden.

5. Webapplicaties

- Verwerker dient webapplicaties blijvend te beschermen tegen de meest actuele OWASP Top 10 kwetsbaarheden.

6. API-koppelingen

- Verwerker dient API-koppelingen blijvend te beschermen tegen de meest actuele OWASP API Security Top 10 kwetsbaarheden.

7. Toegang en Identity & Access Management

- Verwerker dient ervoor te zorgen dat het informatiesysteem kan integreren met Hello-ID als Identity & Access Management (IAM)-oplossing.