

Bijlage 2 – Programma van Eisen (perceel 1: Overijssel)

Betreft: Europese aanbestedingsprocedure Mobiliteitsvoorziening

1. Eisen ten aanzien van communicatie	
Eis 1 Communicatie	Opdrachtnemer ontzorgt Opdrachtgever ter zake van de communicatie over de Mobiliteitskaart richting medewerkers. Opdrachtgever biedt dus <i>tijdig</i> informatie aan waarnaar Opdrachtgever op internet of andere communicatiekanalen kan verwijzen, of die Opdrachtgever (direct) op haar intranet of andere communicatiekanalen kan zetten, danwel -en daar gaat de voorkeur van Opdrachtnemer naar uit- ondersteuning van een medewerker van Opdrachtnemer op het provinciehuis, die ook eventuele vragen van medewerkers kan beantwoorden, zulks gedurende de implementatiefase (bijvoorbeeld twee dagen per week). Dit betreft op de organisatie van Opdrachtgever gerichte informatie (dus niet slechts algemene informatie), waaronder in ieder geval begrepen: • (praktische) uitleg en informatie over het gebruik Mobiliteitskaart en bijbehorende app, in de vorm van een filmpje / Frequently Asked Questions et cetera; • de link naar de gepersonaliseerde online-omgeving voor medewerkers (eis 3.2 onder K); • de contactgegevens van de Helpdesk/Servicedesk van Opdrachtnemer (eis 3.5) Voorname informatie staat uitgewerkt in het implementatieplan en is onderdeel van de gesprekken tussen Opdrachtgever en (de accountmanager van) Opdrachtnemer (eis 4.4)
2. Eisen ten aanzien van financiën	
Eis 2 Facturatie	Opdrachtnemer verstuurt maandelijks -achteraf- een digitale factuur voor de Dienstverleningsfee en maandelijks achteraf een digitale factuur voor de Vervoerskosten (aantoonbaar gebaseerd op de door de OV-dienstverleners in rekening gebrachte kosten). Deze factuur komt overeen met wat er in de loonjournaalpost van Opdrachtgever is verwerkt. Zitten hierin verschillen dan ondersteunt Opdrachtnemer Opdrachtgever in het achterhalen van het probleem en oplossen ervan. In vorenbedoelde factuur is in ieder geval opgenomen: • contract-id; • verplichtingnummer indien dienstverlening fee • kostenplaats; • de periode waar de kosten betrekking op hebben; • een uitsplitsing op totaalniveau van de kosten per vervoersmiddel zowel ex- als inclusief BTW. De specificatie van de factuur kan Opdrachtgever te allen tijde inzien en downloaden in het portal, als genoemd in eis 3.2 onder L.
3. Algemene gebruikseisen	
Eis 3.1 Onderhoud met downtime	Opdrachtnemer garandeert dat het onderhoud aan de voorzieningen van Opdrachtnemer -dat wil zeggen werkzaamheden met downtime- zo veel mogelijk wordt uitgevoerd buiten kantoor tijden, zodat (de medewerkers van) Opdrachtgever hiervan geen hinder ondervindt. Om incidenten te voorkomen, te beperken of om urgente beveiligingsverbeteringen door te voeren, kan

	hiervan afgeweken worden. U dient hier Opdrachtgever van op de hoogte te stellen.
Eis 3.2 mobiliteitskaart	Opdrachtnemer levert (medewerkers van) Opdrachtgever een Mobiliteitskaart en bijbehorend(e) app / portal, die -ongeacht de concessie/concessiehouder- 24/7 te gebruiken is en: A. waarvan de levertijd, na aanvraag door Opdrachtgever, maximaal <i>tien</i> werkdagen bedraagt; B. toegang geeft tot gebruik van Openbaar Vervoer: trein, bus, tram, metro, alsmede de Ov-fiets en Ov-vervoer over water; C. de mogelijkheid biedt om eventuele door Opdrachtnemer aan Opdrachtgever verstrekte kortingen, ook voor privéreizen van medewerkers te laten gelden; D. de mogelijkheid biedt de gemaakte reizen met het Openbaar vervoer te classificeren (in beginsel 2^e klasse en incidenteel 1^e klasse) en de mogelijkheid -voor zover het woon-werkverkeer betreft- de extra kosten hiervan door te belasten aan de medewerker; E. de mogelijkheid biedt (a.) woon-werkverkeer, (b.) dienstreizen en (c.) privéreizen te onderscheiden, waarbij privéreizen direct (via de salarisadministratie) doorbelast kunnen worden aan de medewerker of via split billing wordt georganiseerd; F. de mogelijkheid biedt de gemaakte reizen met eigen vervoer te registreren ten behoeve van het uitbetalen (of fiscaliseren) van de kilometervergoeding door Opdrachtgever, waarbij onderscheid kan worden gemaakt tussen verschillende vervoersvormen (auto, fiets, lopen); G. de mogelijkheid biedt om verschillende <i>kilometervergoedingen</i> toe te kennen op basis van type reis (woon-werk, dienstreis) / vervoersvorm (auto, lopen, fietsen) / werklocatie, en -als de kilometervergoeding hoger is dan fiscaal vrijgesteld- een deels belaste en deels onbelaste vergoeding te verwerken voor eenzelfde reis (volgens een -nog in richtengoedkeuringsworkflow). Dit betekent nadrukkelijk ook dat het voor medewerkers mogelijk is om meerdere vervoerssoorten in één rit vergoed te krijgen (bijvoorbeeld eerst met de fiets naar het station, vervolgens verder met het OV en aansluitend lopend de reis voortzetten); H. de mogelijkheid biedt om reizen naar meerdere werklocaties van Opdrachtgever op te geven; I. de mogelijkheid biedt thuiswerkdagen te registreren; J. de mogelijkheid biedt om een cumulatie van een (een vergoeding van een) thuiswerkdag en (het vergoeden van) reiskosten woon-werkverkeer te voorkomen; K. de mogelijkheid biedt dat medewerkers in een gepersonaliseerde online-omgeving (portal): - o zelf reizen kunnen merken als 'zakelijk' of 'privé'; - o zelf kaart- en (historische)reisgegevens kunnen beheren en dus ook zelf eventueel afwijkend reisgedrag kunnen vaststellen, waarop hij / zij (binnen vier weken na de bewuste reis) actie kan ondernemen; - o hun data in het kader van de rapportage werkgebonden personenmobiliteit (WPM) kunnen inzien, in welk kader de medewerker (bewerkbare) overzichten in Excel-formaat kan downloaden. L. de mogelijkheid geeft aan Opdrachtgever om in een online-omgeving (portal) in ieder geval het volgende in te zien: - o op personeelsnummerniveau en gecumuleerd: ▪ reisgegevens (onder andere): datum, algemene reistijden (bijvoorbeeld binnen/buiten spits), vertreklocatie, aankomstlocatie, gereisde kilometers, kosten(afwijkingen) en classificatie et cetera. LET OP! van privéreizen van medewerkers is deze data ten dele inzichtelijk, namelijk het totaal aantal gereisde

	kilometers per medewerker, het aantal reizen en de datum; ▪ type reis (zakelijk / woon-werk / privé), alsmede de vervoerssoort (OV / trein / fiets et cetera), in welk kader Opdrachtnemer -ongeacht eventuele abonnementen- gedurende de gehele looptijd van de Overeenkomst (dus vanaf dag één) volledig inzicht geeft, namelijk van alle medewerkers, alle reisgegevens (met uitzondering van privéreizen): ○ data, die van belang is voor een (fiscale) steekproef van Opdrachtgever. Te denken valt dan aan een overzicht van eventueel afwijkend reisgedrag; ○ data, die van belang is in het kader van de rapportage werkgebonden personenmobiliteit (WPM), maar liever nog: een complete rapportage die kan worden ge-upload op de website van RVO; ○ van de verstrekte Mobiliteitskaarten: datum uitgifte/activering, alsmede informatie over eventuele geblokkeerde / gewijzigde Mobiliteitskaarten, in welk kader Opdrachtgever bewerkbare (management)rapportages kan downloaden, die aansluiten op de provincierapportages en dashboards (in PowerBI). N. de mogelijkheid biedt van 'leenkaarten', voor stagiaires, (bepaalde) trainees, externe inhuur et cetera, dus niet-medewerkers, die relatief kort voor de Opdrachtgever werken. Deze kaarten zullen fysiek aanwezig zijn in het provinciehuis en worden uitgegeven door een medewerker van het facilitair Servicepunt, zulks na een reservering (van de betreffende persoon) in het reserveringssysteem van Opdrachtgever. In de eerste week van iedere maand zal een rapportage vanuit het reserveringssysteem van Opdrachtgever gestuurd worden aan Opdrachtnemer en deze wordt vervolgens onderdeel van haar (algehele) rapportages; ➤ Een eventueel alternatief voor 'leenkaarten' is bespreekbaar. Opdrachtgever laat zich in dat kader adviseren door Opdrachtnemer, mede in verband met het feit dat de kosten van 'leenkaarten', alsmede de daarmee gemaakte reiskosten, de wijze van factureren en verwerken, compliceerder maakt (Eis 5.1 onder D). O. de mogelijkheid biedt voor Opdrachtgever verschillende groepen medewerkers inclusief bijbehorende (verschillende) reisvoorwaarden te onderscheiden, waaronder ook begrepen: het eventueel blokkeren van (een) Mobiliteitskaart(en), voor welke kaart(en) dan dus ook geen kosten meer gerekend worden door Opdrachtnemer. Van belang in dit kader is dat voor politieke ambtsdragers (PS) ándere kilometervergoedingen gelden (bijv. declareren in plaats van fiscaliseren van autokilometers), alsmede een andere goedkeuringsflow (bijv. eerste controle door penningmeester van de fractie en tweede controle door de managementassistent van Griffie), dan voor medewerkers. Voor deze afgebakende groep is dus maatwerk -en goed overleg tussen Opdrachtgever en Opdrachtnemer- vereist. P. indien een in- of uitcheck gemist wordt, de medewerker de mogelijkheid heeft om dit op eenvoudige manier te herstellen. Het maximaal aantal keren dat op deze wijze 'geld wordt teruggevraagd' is minimaal gelijk aan de maxima die de vervoerders daaraan stellen. In een dergelijke situaties -dus een in- of uitcheck gemist- geeft het systeem van Opdrachtnemer een signaal aan de betrokken medewerker, waarop hij / zij dus actie kan ondernemen; Q. een routeplanner kent, waarmee reizen eenvoudig (vooruit) kunnen worden gepland; R. door besturingssysteem iOS en Android wordt ondersteund, minimaal drie versies eerder dan de versie die op dát moment het meest actueel is; S. in de Nederlandse en Engelse taal beschikbaar is;
--	---

	T. landelijke dekking biedt in Nederland.
Eis 3.3 Declaraties	Opdrachtnemer biedt medewerkers van Opdrachtgever de mogelijkheid om kosten die met de reis samenhangen, zoals parkeergelden en kosten van eten / drinken, eenvoudig te declareren. Het gaat hier dus om kosten die niet via de OV-dienstverleners gemaakt worden, maar wel in samenhang voorkomen.
Eis 3.4 Aflevering kaart	Opdrachtnemer levert persoonlijke Mobiliteitskaart(en) op het Provinciehuis of op verzoek van Opdrachtgever, en met inachtneming van privacywetgeving, op het huisadres van de medewerker. Uit de begeleidende communicatie (o.a. korte gebruikershandleiding van de Mobiliteitskaart en -app) blijkt dat dit namens Opdrachtgever wordt aangeboden. Opdrachtnemer zorgt ervoor dat nieuwe medewerkers in staat worden gesteld om op hun eerste werkdag met de kaart te reizen, mits de Mobiliteitskaart tijdig is aangevraagd.
Eis 3.5 Helpdesk/Service desk	Opdrachtnemer is ten behoeve van gebruikersondersteuning tenminste op maandag t/m vrijdag tijdens kantooruren (tussen 08:00 en 18:00) telefonisch bereikbaar met een Nederlandstalige helpdesk, waarvan de beschikbaarheid voor minimaal 99,5% is gegarandeerd. Bij een grote storing, bijvoorbeeld wanneer medewerkers niet kunnen reizen met de Mobiliteitskaart, wordt Opdrachtgever terstond geïnformeerd en op de hoogte gehouden van de voortgang.
4. Algemene organisatie-eisen	
Eis 4.1 Vervoerscontracten	Ten behoeve van onderhavige aanbesteding sluit Opdrachtgever één overeenkomst met Opdrachtnemer en niet -separaat- nog één met (een) vervoerder(s), zoals de NS.
Eis 4.2 Migratie kosteloos	Een eventuele (platform)migratie aan de zijde van Opdrachtnemer tijdens de contractperiode -bijvoorbeeld vervanging van (een deel van de faciliteiten van) de Mobiliteitskaart door de Mobiliteitsapp- brengt geen extra kosten met zich voor Opdrachtgever.
Eis 4.3 Optimaliseren vervoerskosten	Opdrachtnemer borgt dat voor Opdrachtgever de meest gunstige Vervoerskosten gelden en komt tenminste één keer per jaar met een voorstel voor optimalisatie van deze kosten, bijvoorbeeld als op basis van het reisgedrag van (een) medewerker(s) blijkt dat een abonnementsvorm gunstiger is dan 'pay per use'.
Eis 4.4 Accountmanager Opdrachtnemer	Gedurende de looptijd van de Overeenkomst stelt Opdrachtnemer een accountmanager aan, die het vaste aanspreekpunt is voor Opdrachtgever. Met deze accountmanager is periodiek overleg. Onderdeel van dit overleg is het eerdergenoemde Optimaliseren vervoerskosten / een eventuele (platform)migratie, alsmede (andere) relevante operationele, tactische en strategische aspecten ter zake van de Mobiliteitskaart en dienstverlening. Ten slotte is onderdeel van het overleg: eventuele vervoersproducten, die Opdrachtgever zelf (via door haar verstrekte concessies) aanbiedt, zoals Voordeel Oost van RRRreis, van welke producten medewerkers eventueel óók gebruik kunnen gaan maken via de Mobiliteitskaart of app van Opdrachtnemer.
Eis 4.5 Verlies, diefstal, beëindiging kaart	Opdrachtnemer garandeert dat bij het blokkeren / beëindigen van de Mobiliteitskaart door Opdrachtgever -bijvoorbeeld wegens verlies / diefstal, misbruik of einde dienstverband- de kaart niet langer bruikbaar is. Vanaf het moment waarop Opdrachtgever een dergelijke blokkade / beëindiging schriftelijk kenbaar maakt aan Opdrachtnemer (op de tussen partijen contractueel afgesproken wijze) dient dit te worden verwerkt binnen één werkdag. Eventuele nog met deze kaart daarna gemaakte kosten komen dus voor rekening en risico van Opdrachtnemer.
Eis 4.6 Implementatie en exit bij afloop overeenkomst	Opdrachtnemer verricht bij afloop van de Overeenkomst kosteloos alle noodzakelijke activiteiten (waaronder eventuele inname of volledige blokkade van de Mobiliteitskaarten) voor een goede afronding / transitie naar een volgende opdrachtnemer. Opdrachtnemer zorgt er dus voor dat na beëindiging van de Overeenkomst, geen gebruik meer kan worden gemaakt van de Mobiliteitskaart en de -app, zodat van kosten voor Opdrachtnemer of haar medewerkers géén sprake kan zijn.

Eis 4.7 Toegankelijkheid medewerkers (visuele / fysieke) beperkingen	Opdrachtnemer garandeert dat alle websites en mobiele applicaties die gebruikt worden in het kader van de diensten voldoen aan de standaard EN 301 549, zodat Opdrachtgever kan voldoen aan alle verplichtingen in het Tijdelijk besluit digitale toegankelijkheid overheid. Opdrachtnemer overlegt alle relevante documentatie en levert alle nodige medewerking aan Opdrachtgever om overeenstemming met de standaard EN 301 549 aan te (kunnen) tonen. Indien Opdrachtnemer nog niet (volledig) vorenbedoelde standaard voldoet, garandeert hij dat dit binnen een jaar na ingangsdatum van de Overeenkomst wél het geval is, ter zake waarvan bij aanvang van de Overeenkomst alle relevante documentatie wordt overgelegd (waaruit dus volgt welke stappen reeds gezet zijn; wat er -concreet- nog te doen staat om aan deze standaard te voldoen; en welk tijdspad hiervoor staat).
Eis 4,8 Informatiebeheer (archief)	Opdrachtnemer garandeert dat haar systemen / de Mobiliteitskaart / de app compliant is met de archiefwet en (dus) dat: A. gegevens na afloop van de daarvoor vastgestelde termijn worden vernietigd. Voor personele en financiële-/reisgegevens is dat op dit moment 10 jaar. De laatste persoonsgegevens worden pas vernietigd nadat de gegevens van het laatste reisjaar van de betreffende persoon zijn vernietigd. B. na vernietiging van persoonsgegevens deze ook niet meer terugkomen in rapportages en overzichten.
5. Eisen ten aanzien van processen en systemen	
Eis 5.1 Afstemming salarisverwerking YouForce	Opdrachtnemer garandeert, in relatie tot het salarisverwerkingssysteem (Youforce) en de partij (SSC Ons) bij wie Opdrachtnemer (en omliggende gemeenten) dit heeft ondergebracht: A. dat per medewerker, alle vervoersbewegingen per maand en de door SSC Ons gewenste (salaris)coderingen in een zogenaamd DPIA 100-bestand worden aangeleverd; B. dat Opdrachtnemer kan koppelen met de file api van Visma Raet, zodat aanlevering van voornoemd DPIA 100-bestand met de maandelijkse mutaties geautomatiseerd verloopt; C. dat per maand de juiste bedragen op de juiste coderingen worden weergegeven, zodat dit correct en zonder fouten in de salarisverwerking kan worden verwerkt; D. dat het door Opdrachtgever aan Opdrachtnemer te betalen bedrag per maand aan vervoerskosten, zoals blijkt uit de factuur van Opdrachtnemer, overeenkomt met de loonjournaalpost van Opdrachtgever. En dat de Dienstverleningsfee, alsmede de eventuele kosten van 'leenkaarten' (die genoemd staan Eis 3.2, onder M) en daarmee gemaakte vervoerskosten via een verplichting met verplichtingsnummer gefactureerd worden door Opdrachtnemer aan Opdrachtgever Dit vraagt -goed- overleg tussen Opdrachtgever en Opdrachtnemer en de afspraken hieromtrent worden vastgelegd in het implementatieplan (die genoemd staat in Eis 1). E. dat in verband met 'het automatisch uitruilen van reiskosten woon-werk verkeer', de fiscale ruimte automatisch wordt bepaald (op basis van enkele reis x 2 (vice versa) x aantal dagen x 0,23 ct) en dat dit bedrag te boeken is op een door SSC Ons gewenste salariscode. Vorenbedoelde 0,23 per kilometer staat voor het momentele fiscaal vrijgestelde bedrag. Dit kan in de toekomst uiteraard wijzigen, waarvan Opdrachtgever Opdrachtnemer dan op de hoogte stelt; F. dat opdrachtnemer de (wijze van totstandkoming van de) stamgegevens van medewerkers inzichtelijk maakt via een API koppeling, zoals 'de kilometers enkele reis woon-werk afstand', alsmede inzichtelijk maakt hoe dit werkt bij eventuele wijzigingen / verhuizingen; G. dat, als er iets fout gaat met de aanlevering van (reis)data of de uitbetaling van reiskostenvergoedingen, HR-service van SSC Ons bij de Servicedesk van Opdrachtnemer terecht kan om dit op te lossen, waaronder de mogelijkheid begrepen van het verkrijgen van duidelijkheid op medewerkersniveau;

	H. dat, in verband met jaarlijkse controle's audits van SSC Ons en externe accountant, opdrachtnemer op aanvraag van SSC Ons tijdige aanlevering garandeert van gegevens door middel van rapportage of brondocumenten van de aangeleverde salarismutaties (zie onderdeel A tot en met D).
6. Eisen ten aanzien van (informatie)beveiliging	
Eis 6.1 Gemeentelijke Inkoopvoorwaarden	De leverancier accepteert Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT 2023) als leidende inkoopvoorwaarden.
Eis 6.2 Single Sign On	Opdrachtnemer ondersteunt het gebruik van Microsoft SSO t.b.v. inloggen op de applicatie of het portal.
Eis 6.3 Audit en kwaliteitsmetingen	Opdrachtgever heeft het recht om – voor eigen rekening – audits en/of kwaliteitsmetingen (PEN-testen) te (laten) uitvoeren wanneer de Opdrachtnemer onvoldoende kan aantonen dat de resultaten van eigen audits (uitgevoerd door een gekwalificeerde externe partij) en PEN-testen (uitgevoerd door een gekwalificeerde PEN-tester) toereikend zijn en wanneer de Opdrachtgever redenen heeft om aan te nemen dat er onvolkomenheden zijn die niet zijn gerapporteerd. Deze audits en/of kwaliteitsmetingen vinden plaats op de interne beheersing van aspecten qua, informatiebeveiliging, vertrouwelijkheid, integriteit en beschikbaarheid en efficiency van de door Opdrachtnemer aan Opdrachtgever ter beschikking gestelde diensten en de daaraan gerelateerde activiteiten. Indien uit de audit of kwaliteitsmeting naar voren komt dat Opdrachtnemer niet (volledig) voldoet aan zijn verplichtingen uit deze Overeenkomst, zal Opdrachtnemer de kosten van die audit of kwaliteitsmeting aan Opdrachtgever vergoeden, onverminderd de overige rechten van Opdrachtgever.
Eis 6.4 Software scheiding	Voor de software is sprake van een gescheiden test en productie omgeving (OTAP).
Eis 6.5 Broncode	De leverancier heeft maatregelen genomen om de toegang tot de broncode van informatiesystemen te beperken tot de medewerkers, die deze code onderhouden of installeren.
Eis 6.6 Kwaliteit Applicaties	Applicaties worden ontwikkeld en getest op basis van landelijke normen en richtlijnen voor beveiliging, zoals de NCSC richtlijnen voor beveiliging van webapplicaties. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de Open Web Application Security Project (OWASP) top 10
Eis 6.7 Audit rapport.	Opdrachtnemer verstrekt op eerste verzoek van Opdrachtgever maar in ieder geval ieder jaar een auditrapport en/of -verslag van een onafhankelijke partij (auditor) ten aanzien van haar interne beheersing dat niet ouder is dan één jaar, gebaseerd op de ISAE 3402- of een ISAE 3000-rapportage, of een vergelijkbare verklaring van een derde partij.
Eis 6.8 Onrechtmatige inbreuken contactpersoon	Indien en zodra Opdrachtnemer een mogelijkheid tot en/of (een poging tot) een onrechtmatige of anderszins ongeautoriseerde inbreuk op de beveiliging van informatie van Opdrachtgever signaleert (waaronder ook een datalek wordt begrepen), zal zij Opdrachtgever hierover binnen 24 uur inlichten en zal Opdrachtnemer op eigen kosten alle redelijkerwijs benodigde maatregelen treffen om deze en verdere onrechtmatige of anderszins ongeautoriseerde inbreuken te beëindigen, te voorkomen of te beperken, een en ander onverminderd de verplichting van Opdrachtnemer om de eventueel door Opdrachtgever daardoor geleden schade te vergoeden. De verplichting tot schadevergoeding is beperkt tot directe schade, die causaal verband houdt met een toerekenbare tekortkoming van Opdrachtnemer.
Eis 6.9 Bewaken en rapportage kwetsbaarheden	Opdrachtnemer is verantwoordelijk voor het uitvoeren van het bewaken van kwetsbaarheden in het product of geleverde dienst. In geval van de constatering van een kritieke kwetsbaarheid, welke mogelijk tot een beveiligingsincident kan leiden voor Opdrachtgever, dient deze binnen 24 uur gerapporteerd te worden. De indicatie is hier dat er informatie van Opdrachtgever gelekt zou kunnen worden.
Eis 6.10 Vulnerability	Opdrachtnemer heeft een vulnerability en patch management proces ingericht, realiseert adequate mitigerende maatregelen voor software kwetsbaarheden en heeft hiervoor een procedure. Kwetsbaarheden worden

	op basis van een risico-indicatie (bijvoorbeeld een CVSS score, common vulnerabilities scoring system) geprioriteerd en opgelost. Kwetsbaarheden met een CVSS-score 'critical' en "High" worden binnen een week verholpen. Op verzoek van de Opdrachtgever wordt hiervan onverwijld schriftelijk bewijs verstrekt.
Eis 6.11 Hacktest	Opdrachtnemer beschikt over een managementsamenvatting waarin een overzicht van bevindingen wordt gepresenteerd van een recent uitgevoerde hacktest en verstrekt op verzoek van de Opdrachtgever onverwijld een schriftelijk exemplaar hiervan aan de Opdrachtgever. De hacktest kent geen bevindingen die onacceptabele risico's inhouden voor het gebruik van het te leveren product of de te leveren dienst door Opdrachtgever.
Eis 6.12 Logging en monitoring	Opdrachtnemer beschikt over logging- en monitoringinformatie bij security-incidenten en verstrekt na verzoek van de Opdrachtgever onverwijld deze informatie aan Opdrachtgever.
Eis 6.13 Beveiligingsmaatregelen instemming	Indien een wijziging kan leiden tot significante degradatie van beveiligingsmaatregelen of een dreiging ontstaat dat niet langer wordt voldaan aan toepasselijke wet- en regelgeving of de gestelde security eisen, dan vindt die wijziging alleen plaats met voorafgaande schriftelijke instemming van Opdrachtgever. Wijzigingen zonder negatieve impact op de beveiliging ook zonder voorafgaande schriftelijke instemming kunnen worden doorgevoerd.
Eis 6.14 Beveiligingsmaatregelen	Opdrachtnemer zal alle technische en organisatorische beveiligingsmaatregelen nemen en implementeren die noodzakelijk zijn om aan de verplichtingen uit deze Overeenkomst te voldoen, waaronder in ieder geval digitale doorgifte van vertrouwelijke informatie aan Opdrachtgever via een beveiligde verbinding zoals secure email of een dienst voor beveiligde bestandsoverdracht alsmede (voor zover van toepassing) de technische en organisatorische beveiligingsmaatregelen zoals in het Beschrijvend document vermeld. 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 de aard van de Informatie meebrengen.
Eis 6.15 Beheersessies	Indien Opdrachtnemer beheersessies op afstand uitvoert, heeft Opdrachtgever het recht om de beheersessie tijdens de uitvoering hiervan of achteraf te controleren.
Eis 6.16 Geografische locatie	Alle informatie van Opdrachtgever wordt door Opdrachtnemer opgeslagen binnen de EER.
Eis 6.17 Beëindiging Overeenkomst	Opdrachtnemer dient binnen tien werkdagen na beëindiging van de Overeenkomst: (i) alle Informatie aan Opdrachtgever terug te geven, zonder daarvan een kopie te behouden; en (ii) alle Informatie die zich in geautomatiseerde systemen bevindt die niet aan Opdrachtgever toebehoren, te verwijderen. Het voorgaande geldt niet ten aanzien van informatie die Opdrachtnemer op grond van enig wettelijk voorschrift dient te bewaren. Opdrachtgever heeft het recht om te controleren of de verplichting tot teruggave en verwijdering van Informatie door Opdrachtnemer is nageleefd en Opdrachtnemer verleent daartoe alle redelijkerwijs benodigde medewerking.
Eis 6.19 Uitbesteding dienst	Indien Opdrachtnemer een volledige dienst, of een deel daarvan, uitbesteedt, dient voorafgaand schriftelijk toestemming te worden gevraagd aan Opdrachtgever.
Eis 6.20 Onderaannemers toeleveranciers	Indien Opdrachtnemer de diensten uitoefent met onderaannemers of toeleveranciers, dienen de onderaannemers of toeleveranciers te voldoen aan dezelfde beveiligingseisen en -normen zoals benoemd in deze Overeenkomst. Het is de verantwoording van de Opdrachtgever om ervoor te zorgen dat aan deze eisen en/of normen wordt voldaan.
Eis 6.21 ISO eisen	De Opdrachtnemer beschikt -nu of binnen één jaar na ingang van de Overeenkomst- over een adequaat en uitgewerkt informatiebeveiligingsbeleid, gebaseerd op de ISO27001/ISO27002 of een vergelijkbare andere

	industriestandaard, en verstrekt hiervan schriftelijk bewijs aan de Opdrachtgever bij de Inschrijving.
Eis 6.22 Beveiligde verbinding	Omdat er persoonsgegevens in de app worden gezet en verwerkingsgegevens terugkomen, moet een beveiligde verbinding gerealiseerd worden tussen SuccessFactors en het systeem van de opdrachtnemer bij voorkeur met een API-koppeling.
Eis 6.23 Eigendom gegevens	Opdrachtgever blijft eigenaar van de gegevens binnen applicatie en deze gegevens mogen niet voor andere doeleinden gebruikt worden door de Opdrachtnemer van de applicatie. Dit geldt zowel voor gegevens in de Test-, Acceptatie- als Productieomgevingen.
Eis 6.24 Toegang authenticatie	Toegang vanuit een onvertrouwde zone naar een vertrouwde zone gebeurt alleen op basis van minimaal twee-factor-authenticatie.
Eis 6.25	Binnen de test omgeving wordt geen gebruik gemaakt van productiedata
7. Eisen ten aanzien van verwerking persoonsgegevens	
Eis 7.1 Verwerking van persoonsgegevens	De mobiliteitskaart en -app verwerken reisdata van medewerkers. Daarmee is er sprake van de verwerking van persoonsgegevens en is de Algemene verordening gegevensbescherming (AVG) van toepassing. Opdrachtnemer dient te garanderen dat voor registratie en verwerking van persoonsgegevens wordt voldaan aan de kaders gesteld in de AVG of andere relevante wetgeving.
Eis 7.2 Verwerking persoonsgegevens	Opdrachtnemer verwerkt persoonsgegevens van medewerkers van Opdrachtgever alleen binnen de context van deze opdracht.
Eis 7.3 Privacy by design and default	Opdrachtnemer richt de mobiliteitskaart en -app conform de beginselen van <i>privacy by design en default</i> in en legt uit hoe zij dit heeft gedaan.
Eis 7.4 Verwerkersovereenkomst	Afhankelijk van hoe de dienstverlening precies wordt vormgegeven kan Opdrachtnemer persoonsgegevens verwerken onder eigen verwerkingsverantwoordelijkheid of optreden als een verwerker die namens en op instructie van Opdrachtgever persoonsgegevens verwerkt. In het laatste geval gaat Opdrachtnemer gaat akkoord met het model van de verwerkersovereenkomst van Opdrachtgever
Eis 7.5 Gegevens privé reizen	Wanneer reizen door de gebruiker als privé worden gelabeld is het voor opdrachtgever slechts beperkt mogelijk om ritgegevens in te zien (eis 3.2 onder L).
Eis 7.6 Europese Economische Ruimte (EER)	Persoonsgegevens worden te allen tijde binnen de Europese Economische Ruimte (EER) verwerkt
Eis 7.7 Verklaring omtrent gedrag (VOG)	Opdrachtnemer zorgt ervoor dat medewerker die persoonsgegevens verwerken een verklaring omtrent gedrag (VOG) hebben.
Eis 7.8 Minimale machtigingen	Opdrachtnemer dient te garanderen dat de Mobiliteitskaart en -app uitsluitend vraagt naar noodzakelijke machtigingen. Tevens is de mobiliteitsapp zo ingericht dat instellingen standaard op de minimale variant staan. Dat wil zeggen: die zorgt voor de minste inbreuk op de privacy (zie het punt over <i>privacy by design en default</i>)
Eis 7.9 Privacyverklaring	Opdrachtnemer garandeert dat is voorzien in een privacyverklaring die voldoet aan de wettelijk gestelde eisen, zowel in de mobiliteitsapp als op andere plekken waar dat noodzakelijk is.
Eis 7.10 DPIA	Opdrachtnemer werkt op verzoek van Opdrachtgever mee aan een Data Protection Impact Analyse (DPIA).
8. Eisen ten aanzien van de vervoerskosten	
Eis 8.1 Resell-tarieven	Opdrachtnemer hanteert uitsluitend de zogenoemde OV resell-tarieven, inclusief geldende periodekortingen, van de vervoerders als inkoop- en doorbelastingsbasis richting Opdrachtgever.

	Deze resell-tarieven zijn: • Vastgesteld door de concessieverlenende overheid op basis van de MaaS-bepalingen en/of concessievoorwaarden; • Publiek inzichtelijk en gelijk voor alle marktpartijen; Niet onderhandelbaar of variabel per inschrijver.
Eis 8.2 Wijzigingen in resell-tarieven	De OV resell-tarieven worden gedurende de gehele contractperiode als bovengrens gehanteerd. Abonnementen of alternatieve prijsconstructies zijn slechts toegestaan indien de totale kosten (abonnement + reizen buiten het abonnement) aantoonbaar lager zijn dan wanneer dezelfde reizen zouden worden afgerekend op basis van het vastgestelde resell-tarief. Wijzigingen in resell-tarieven, zowel stijgingen als dalingen, worden één-op-één doorbelast aan de opdrachtgever, overeenkomstig de door de concessieverlener vastgestelde aanpassingen.
Eis 8.3 OV vervoersbedrijven	Voor OV vervoersbedrijven die zelf als inschrijver optreden, geldt dat zij niet bij zichzelf kunnen inkopen. Voor deze partijen wordt daarom bepaald dat hun inkoop- of doorbelastingsprijs aantoonbaar gelijk moet zijn aan het resell-tarief dat zij hanteren richting derden.