Bewerkersovereenkomst tussen Doorbetalers en TC De Groote Wielen

Template versie: 2
Document Versie: 1.0
Datum: 18-05-2018
Schrijver: Benjamin de Jong
Referentie: DbBo.27.2018.1

Overzicht van de contractsbepalingen

Contractsbepalingen

Partijen:

1. TC De Groote Wielen Vereniging, Kvk 54596033, gevestigd aan de Groote Vlietlaan 61 te Rosmalen, hierna te noemen **"VERANTWOORDELIJKE"**;

en

2. Doorbetalers VOF, Kvk 59855835, gevestigd aan de Zuiderweg 237 Hilversum, hierna te noemen **"BEWERKER"**

hierna gezamenlijk te noemen: 'Partijen'

OVERWEGENDE DAT

A. VERANTWOORDELIJKE en BEWERKER een overeenkomst hebben gesloten op 18-05-2018, hierna de "Overeenkomst". In het kader van de uitvoering van de Overeenkomst verleent BEWERKER diensten aan VERANTWOORDELIJKE.

B. BEWERKER in het kader de uitvoering van de Overeenkomst ook Persoonsgegevens verwerkt voor VERANTWOORDELIJKE.

C. Dat partijen wettelijk verplicht zijn afspraken te maken en vast te leggen met betrekking tot de verwerking van Persoonsgegevens door BEWERKER.

d. De bepalingen van deze Bewerkersovereenkomst vóór gaan op alle andere afspraken die tussen Partijen gelden en betrekking hebben op de verwerking van Persoonsgegevens door BEWERKER voor VERANTWOORDELIJKE.

KOMEN ALS VOLGT OVEREEN:

Artikel 1. Definities

Naast de wettelijke definities hebben de volgende termen de volgende betekenis:

"AP"	Autoriteit Persoonsgegevens, ook College Bescherming Persoonsgegevens genoemd, de toezichthoudende autoriteit voor de naleving van de geldende privacywetgeving;
"AVG"	Algemene Verordening Gegevensbescherming, voluit: Verordening (EU) 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;
"Betrokkene"	de natuurlijke persoon waarop de Persoonsgegevens die BEWERKER verwerkt voor VERANTWOORDELIJKE en/of haar opdrachtgevers in het kader van de uitvoering van de Overeenkomst betrekking hebben;
"Beveiligingsincident"	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 Persoonsgegevens;
"Bewerkersovereenkomst"	de onderhavige overeenkomst inclusief alle bijlagen die onlosmakelijk hieraan zijn verbonden;
"Bijlage"	Iedere bijlage bij deze Bewerkersovereenkomst, welke een onlosmakelijk deel daarvan uitmaakt;
"Derde"	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verantwoordelijke, noch de Bewerker, noch de personen die onder rechtstreeks gezag van de Verantwoordelijke of de bewerker gemachtigd zijn om de Persoonsgegevens te verwerken;
"Diensten"	Alle diensten die BEWERKER aan VERANTWOORDELIJKE verleent, zoals omschreven in de Overeenkomst;
"EER"	Europese Economische Ruimte;

"Persoonsgegevens"	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon die BEWERKER ontvangt van of verwerkt voor VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst;
"Sub-bewerker"	een partij die door BEWERKER wordt ingeschakeld voor de uitvoering van de Overeenkomst en de daarbij horende verwerking van Persoonsgegevens;
"Wbp"	Wet bescherming persoonsgegevens;
"Verwerken"	elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

Artikel 2. Algemeen

2.1 VERANTWOORDELIJKE wordt ten aanzien van de Persoonsgegevens beschouwd als Verantwoordelijke in de zin van de Wbp en Verwerkingsverantwoordelijke in de zin van de AVG. BEWERKER is Bewerker in de zin van de Wbp en Verwerker in de zin van de AVG.

2.2 BEWERKER en VERANTWOORDELIJKE verstrekken elkaar over en weer tijdig alle benodigde informatie om een goede naleving van de geldende privacywet- en regelgeving mogelijk te maken.

Artikel 3. Verwerken van Persoonsgegevens

3.1 VERANTWOORDELIJKE zal de Persoonsgegevens in overeenstemming met de geldende wet- en regelgeving verwerken en heeft de categorieën van Betrokkenen, het soort Persoonsgegevens en de aard en het doel waarvoor de Persoonsgegevens worden verwerkt opgenomen in **Bijlage 1**. BEWERKER zal de Persoonsgegevens niet voor andere doeleinden of op andere wijze gebruiken dan voor het doel waarvoor de Persoonsgegevens zijn verstrekt of haar bekend zijn geworden.

3.2 BEWERKER zal de Persoonsgegevens uitsluitend verwerken op basis van de schriftelijke instructies van VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst en de verleende Diensten, dan wel in verband met een wettelijke verplichting.

3.3 BEWERKER zal de Persoonsgegevens niet aan een Derde verstrekken, tenzij deze uitwisseling plaatsvindt in opdracht van VERANTWOORDELIJKE in het kader van de uitvoering van de Overeenkomst of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting.

3.4 BEWERKER draagt er zorg voor dat de Persoonsgegevens niet buiten de EER worden verwerkt, tenzij VERANTWOORDELIJKE daar schriftelijke toestemming voor heeft gegeven. Bij ondertekening van de Bewerkersovereenkomst heeft VERANTWOORDELIJKE toestemming gegeven voor Verwerking van de Persoonsgegevens in de landen die zijn opgenomen in **Bijlage 1**.

Artikel 4. Geheimhouding

4.1 BEWERKER houdt de Persoonsgegevens die zij verwerkt in het kader van de uitvoering van de Overeenkomst geheim en zal alle nodige maatregelen treffen om geheimhouding van de Persoonsgegevens te verzekeren. BEWERKER zal de verplichting tot geheimhouding tevens opleggen aan haar personeel en alle door haar ingeschakelde personen.

4.2 De in dit artikel bedoelde geheimhoudingsplicht geldt niet indien VERANTWOORDELIJKE uitdrukkelijk schriftelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, of een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken.

Artikel 5. Beveiliging Persoonsgegevens

5.1 VERANTWOORDELIJKE zal in overeenstemming met de geldende wettelijke regels de beveiliging van de Persoonsgegevens waarborgen en daartoe passende technische en organisatorische maatregelen treffen.

5.2 BEWERKER zal in overeenstemming met de geldende wettelijke regels technische en organisatorische maatregelen treffen, in stand houden en zo nodig aanpassen om een op het risico afgestemd beveiligingsniveau te waarborgen. Om hieraan te kunnen voldoen zal VERANTWOORDELIJKE BEWERKER informeren over de betrouwbaarheidseisen die op de verwerking van toepassing zijn en tijdig de benodigde informatie verstrekken in geval van wijzigingen in de verwerking van Persoonsgegevens.

5.3 BEWERKER zal bij het treffen van beveiligingsmaatregelen rekening houden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

5.4 Indien VERANTWOORDELIJKE een beoordeling wenst uit te voeren van een beoogde verwerkingsactiviteit in het kader van de uitvoering van de Overeenkomst zal BEWERKER alle redelijke medewerking verlenen om deze beoordeling in overeenstemming met de geldende wet- en regelgeving uit te kunnen voeren. Tevens zal BEWERKER alle redelijke medewerking verlenen indien een voorafgaande raadpleging van de AP nodig is op grond van de geldende privacywetgeving. VERANTWOORDELIJKE zal BEWERKER de in dit kader gemaakte redelijke kosten vergoeden.

5.5 In **Bijlage 2** zijn de afspraken tussen Partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen die BEWERKER treft. Deze maatregelen worden periodiek geëvalueerd en indien nodig aangepast. Verwerkingsverantwoordelijke erkent dat zij de in **Bijlage 2** opgenomen afspraken voldoende acht voor een passende beveiliging van de Persoonsgegevens in overeenstemming met de geldende wettelijke verplichtingen.

Artikel 6. Controle

6.1 VERANTWOORDELIJKE heeft het recht om maximaal één maal per jaar op eigen kosten door onafhankelijke deskundigen een audit te laten uitvoeren inzake de verwerking van Persoonsgegevens door BEWERKER ter controle op de naleving van deze Bewerkersovereenkomst. BEWERKER zal alle redelijke medewerking verlenen aan een audit, waaronder het verlenen van toegang tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie. Partijen zullen met elkaar in overleg treden over de wijze van optreden en de verdeling van de kosten.

6.2 BEWERKER zal in overleg met VERANTWOORDELIJKE de aanbevelingen ter verbetering van de onafhankelijke deskundigen zo spoedig mogelijk uitvoeren. Indien de aanpassingen het gevolg zijn van gewijzigde inzichten of wetgeving dan zal VERANTWOORDELIJKE de redelijke kosten voor deze aanpassingen vergoeden. Indien de aanpassingen het gevolg zijn van een tekortkoming in de nakoming van de beveiligingseisen uit de Bewerkersovereenkomst dan zal bewerker deze kosten voor eigen rekening nemen.

6.3 In geval van een onderzoek door de AP of een andere bevoegde autoriteit zal BEWERKER alle redelijke medewerking verlenen en VERANTWOORDELIJKE zo snel mogelijk informeren. Partijen zullen met elkaar in overleg treden over de wijze van optreden en de verdeling van de kosten.

Artikel 7. Beveiligingsincidenten

7.1 BEWERKER informeert VERANTWOORDELIJKE onverwijld nadat BEWERKER kennis heeft genomen van een Beveiligingsincident met betrekking tot de verwerking van de Persoonsgegevens.

7.2 In geval van een Beveiligingsincident zal BEWERKER alle redelijke maatregelen treffen om de gevolgen van het incident te beperken en/of een nieuw incident te voorkomen. BEWERKER zal alle medewerking verlenen aan VERANTWOORDELIJKE om het beveiligingsincident te beoordelen en te kunnen voldoen aan haar eventuele wettelijke meldplicht en haar eventuele plicht tot het informeren van Betrokkenen.

7.3 Partijen leggen hun afspraken over de informatie-uitwisseling in verband met incidenten vast in een "Procedure Meldplicht Datalekken" in **Bijlage 3**. Deze bijlage kan ten allen tijde in overleg door Partijen worden gewijzigd. De bijlage zal in ieder geval worden aangepast indien de regelgeving omtrent de Meldplicht Datalekken of de uitleg daarvan wijzigt.

7.4 In geval van een Beveiligingsincident bij BEWERKER dat leidt tot een meldplicht of een informatieplicht voor VERANTWOORDELIJKE, zal de melding of inde informatieverstrekking in overleg met BEWERKER door VERANTWOORDELIJKE worden verricht. Partijen zullen in goed overleg afspraken maken over de verdeling van de kosten die daarmee zijn gemoeid.

Artikel 8. Verzoeken van Betrokkenen

8.1 Indien BEWERKER een verzoek of bezwaar van een Betrokkene ontvangt, zoals een verzoek om informatie, inzage, rectificatie, gegevenswissing, verwerkingsbeperking, overdracht van de Persoonsgegevens, stuurt BEWERKER dat verzoek onmiddellijk door naar VERANTWOORDELIJKE.

8.2 BEWERKER verleent VERANTWOORDELIJKE alle redelijke medewerking om ervoor te zorgen dat VERANTWOORDELIJKE binnen de wettelijke termijnen kan voldoen aan de verplichtingen op grond van de geldende wet- en regelgeving. De redelijke kosten voor deze medewerking zullen door VERANTWOORDELIJKE aan BEWERKER worden vergoed.

Artikel 9. Sub-bewerkers

9.1 BEWERKER heeft bij de verwerking van de Persoonsgegevens de mogelijkheid om, met schriftelijke toestemming van VERANTWOORDELIJKE, Sub-bewerkers in te schakelen. VERANTWOORDELIJKE zal een redelijk verzoek om toestemming niet onthouden. In **Bijlage 1** houden Partijen een geactualiseerde lijst bij met de relevante gegevens over de Sub-bewerkers.

9.2 BEWERKER zal met de door haar ingeschakelde Sub-bewerkers een overeenkomst sluiten die in overeenstemming is met de relevante wet- en regelgeving en deze Bewerkersovereenkomst. BEWERKER zal in ieder geval iedere Sub-BEWERKER contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na laten leven met betrekking tot de verwerking van de Persoonsgegevens.

Artikel 10. Toegang tot de Persoonsgegevens

10.1 De zeggenschap over de Persoonsgegevens blijft volledig berusten bij VERANTWOORDELIJKE. Op verzoek van VERANTWOORDELIJKE en tegen vergoeding van de redelijke kosten zal BEWERKER alle of een gedeelte van de Persoonsgegevens in gangbaar formaat ter beschikking stellen aan VERANTWOORDELIJKE.

10.2 BEWERKER zal ervoor zorgdragen dat VERANTWOORDELIJKE te allen tijde toegang behoudt tot de Persoonsgegevens en zal in geval van een geschil tussen Partijen deze toegang niet blokkeren. BEWERKER zal maatregelen treffen om ervoor te zorgen dat VERANTWOORDELIJKE ook in geval van faillissement of surséance van betaling van BEWERKER toegang blijft houden tot de Persoonsgegevens.

Artikel 11. Aansprakelijkheid en vrijwaring

11.1 Indien een Partij tekortschiet in de nakoming van de Bewerkersovereenkomst is deze Partij aansprakelijk voor de schade en kosten die de andere Partij daardoor lijdt of heeft geleden.

11.2 BEWERKER vrijwaart VERANTWOORDELIJKE voor boetes en/of dwangsommen van of namens de AP en/of andere bevoegde autoriteiten die aan VERANTWOORDELIJKE worden opgelegd en waarbij vast is komen te staan dat deze zijn toe te schrijven aan overtredingen van de geldende privacywetgeving door BEWERKER met in achtneming van de genoemde beperkingen in artikel 11.1. Om een beroep te kunnen doen op deze vrijwaring is VERANTWOORDELIJKE gehouden om:

(i) BEWERKER terstond op de hoogte te brengen van enig onderzoek of andere aanleiding die zou kunnen leiden tot een voornemen van een toezichthouder tot het opleggen van een boete of last onder dwangsom,

(ii) in samenspraak met BEWERKER te handelen en te communiceren richting de toezichthouder én

(iii) tegen opgelegde boetes in bezwaar en/of beroep te gaan indien daar redelijkerwijs aanleiding voor is.

11.3 VERANTWOORDELIJKE vrijwaart BEWERKER voor boetes en/of dwangsommen van of namens de AP en/of andere bevoegde autoriteiten die aan BEWERKER worden opgelegd en waarbij vast is komen te staan dat deze zijn toe te schrijven aan overtredingen van de geldende privacywetgeving door VERANTWOORDELIJKE. Om een beroep te kunnen doen op deze vrijwaring is BEWERKER gehouden om:

(i) VERANTWOORDELIJKE terstond op de hoogte te brengen van enig onderzoek of andere aanleiding die zou kunnen leiden tot een voornemen van een toezichthouder tot het opleggen van een boete of last onder dwangsom,

(ii) in samenspraak met VERANTWOORDELIJKE te handelen en te communiceren richting de autoriteit
en

(iii) tegen opgelegde boetes in bezwaar en/of beroep te gaan indien VERANTWOORDELIJKE daar redelijkerwijs aanleiding voor is.

Artikel 12. Duur en beëindiging

12.1 Deze Bewerkersovereenkomst treedt in werking op de datum van ondertekening en eindigt van rechtswege bij beëindiging van de Overeenkomst. Verplichtingen met een duurkarakter blijven tussen partijen in stand, zoals de geheimhoudingsverplichting uit artikel 4 van de Bewerkersovereenkomst.

12.2 BEWERKER zal bij beëindiging van de Overeenkomst op verzoek van VERANTWOORDELIJKE en tegen vergoeding van de redelijke kosten de Persoonsgegevens in een gangbaar formaat ter beschikking stellen aan VERANTWOORDELIJKE of aan een door VERANTWOORDELIJKE aangewezen Derde.

12.3 BEWERKER zal na overdracht van de Persoonsgegevens aan VERANTWOORDELIJKE de nog aanwezige Persoonsgegevens vernietigen, tenzij een langere opslag wettelijk verplicht is. BEWERKER zal tevens zorgdragen voor vernietiging van de Persoonsgegevens bij de Sub-bewerkers.

Artikel 13. Wijziging Bewerkersovereenkomst

13.1 Bij wijzigingen in de Diensten, regelgeving of andere relevante omstandigheden die van invloed zijn op de verwerking van de Persoonsgegevens, zullen Partijen in overleg treden over een eventueel benodigde wijziging van de Bewerkersovereenkomst. De wijzigingen in de tekst van deze Bewerkersovereenkomst kunnen uitsluitend schriftelijk door de bevoegde vertegenwoordigers van Partijen worden overeengekomen.

13.2 Wijzigingen in de Bijlagen kunnen door Partijen op ieder moment schriftelijk worden gedaan onder vermelding van het versienummer en de datum van ingang van de nieuwe versie.

Artikel 14. Toepasselijk recht / Bevoegde rechter

14.1 Op deze Bewerkersovereenkomst is uitsluitend Nederlands recht van toepassing.

14.2 Alle geschillen die ontstaan naar aanleiding van deze Bewerkersovereenkomst worden beslecht op dezelfde wijze als opgenomen in de Overeenkomst.

BIJLAGE 1 - Toepassing Bewerkingen

A. Categorieën Betrokkenen
De personen waarop de Persoonsgegevens betrekking hebben zijn in ieder geval:

- Klanten van VERANTWOORDELIJKE die betaalgegevens verstrekken om betalingen via VERANTWOORDELIJKE of via BEWERKER te laten uitvoeren of registreren

B. Soort Persoonsgegevens
De Persoonsgegevens die door BEWERKER worden verwerkt zijn in ieder geval:

- NAW-gegevens,
- Emailadressen,
- Bankrekeningnummers,
- Omschrijvingen van betalingen.

C. Aard en doel van de verwerking
De aard van de verwerking is gerelateerd in het genereren van betaalbestanden en facileren van betalingen;

De Persoonsgegevens worden in ieder geval voor de volgende doelen verwerkt:

- Het opslaan van betaalgegevens,
- Vertalen naar incasso bestanden,
- Doorsturen aan de bank van betaalverzoeken en betaalstatussen,
- Het rapporteren over uitgevoerde of mislukte betalingen.

D. Verwerking buiten de EER
De Persoonsgegevens worden in de volgende landen buiten de EER verwerkt (denk ook aan onderhoud door personen die zich buiten de EER bevinden of cloudopslag bij een cloudprovider van buiten de EER, zoals uit de VS): Géén, alle gegevens worden binnen Nederland verwerkt en opgeslagen.

E. Gegevens Sub-bewerkers
BEWERKER maakt voor de Diensten gebruik van de volgende Sub-bewerkers:
- ABN AMRO Bank N.V., Gustav Mahlerlaan 10, 1082 PP Amsterdam, KvK: 34334259
- TransIP, Schipholweg 9B, 2316 XB Leiden, KvK: 24345899
- Conscribo online boekhouden, Gildekamp 2130, 6545KG Nijmegen, KvK: 09197284
- Zerotop Interware, Zuiderweg 237, 1221 HH Hilversum, KvK: 32096976

F. Contactgegevens
Voor vragen of opmerkingen over de Bewerkersovereenkomst en Bijlagen is de contactpersoon van

VERANTWOORDELIJKE: Naam: Leonie Puijn,Telefoon: 06-28912669, Email: penningmeester@tcdegrootewielen.nl.

BEWERKER: Benjamin de Jong, Commercieel Manager Doorbetalers, benjamin@doorbetalers.nl

BIJLAGE 2 - Technische en organisatorische beveiligingsmaatregelen

Omschrijving van de technische en organisatorische beveiligingsmaatregelen die door de BEWERKER zijn geïmplementeerd

Zoals opgenomen in art. 5 worden hieronder de afspraken tussen partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen. De getroffen maatregelen zijn opgenomen in deze bijlage en worden aangevuld of gewijzigd indien dat nodig is. VERANTWOORDELIJKE acht genoemde maatregelen passend voor de Verwerking van de Persoonsgegevens.

A. Betrouwbaarheidseisen

Beschikbaarheid: 99,8% op basis van 24*7 uur/week met uitzondering van tijdig aangekondigde onderhoudsvensters.

Maximaal dataverlies: gegevens van minder dan 24 uur oud

Snelheid van oplossen incidenten:

- Totale onbeschikbaarheid: 80% binnen 8 uur
- Onbeschikbaarheid van delen van de dienstverlening: 80% binnen 24 uur
- Alle overige incidenten: best-effort

Gebruikersondersteuning voor betalende klanten:

- Per e-mail, In 80% van de gevallen response binnen 5 werkdagen.
- Telefonisch bij calamiteiten (= serieuze continuïteitsproblemen bij de klant waarbij Doorbetalers invloed heeft op snel herstel) mits afgesproken in contract.

Uitwijkfaciliteiten
Doorbetalers past diens acceptatieomgeving toe als uitwijkfaciliteit. Er is een Busines Continuity Procedure beschikbaar om dit te borgen. Er wordt alleen uitgeweken indien de productie omgeving niet binnen 8 uur terug hersteld kan zijn.

B. Beveiligingsniveau

Zonering
Afhankelijk van de classificatie van de data, wordt deze in een zone aangeboden. De zonering wordt niet op IP nummer aangebracht maar op applicatie interfaces

Firewall policy

Netwerktechnisch wordt op systemen alleen open gezet wat strikt noodzakelijk is. Vanaf het internet betreft dit alleen SSH en HTTPS. Wanneer ook andere services benodigd zijn, worden deze over een SSH tunnel getransporteert. HTTP is alleen toegestaan voor redirects en testomgevingen.

Cryptografie
Alle data is encrypted opgeslagen op het filesystem en alle verbindingen zijn te alle tijden encrypted. Symmetrische encryptie: sleutellengte minimaal 192 bit, bij voorkeur 265, algoritme naar keuze, bij voorkeur Rijndael. Asymmetrische encryptie: RSA of DH/DSS, sleutellengte minimaal 2048 of PGP (PGP gebruikt DH/DSA en RSA). Hashing: SHA 256 (SHA1 nog beperkt toegestaan voor short lived sessies, niet voor opslag)

Software
Doorbetalers maakt alleen gebruik van open source software en/of van software waar we zelf de juiste licenties voor hebben aangekocht.
Servers worden, tenzij expliciet onderbouwd, altijd uitgerust met het Debian operating system.

Patch management
Alle systemen krijgen elk kwartaal een standaard patch ronde. Hierbij worden het operating system, de database en de vanaf internet bereikbare applicaties gepatched. Operating systems en applicaties zijn supported en niet als end of life verklaard.

OTAP
OTAP staat voor Ontwikkel, Test, Acceptance en Productie. Alle Doorbetalers diensten en producten doorlopen deze stadia wanneer deze geintroduceerd of aangepast worden.

Monitoring
Systemen die online transacties verwerken worden gemonitored op beschikbaarheid en capaciteit. De monitoring is zo opgezet worden dat er tijdig alerts ontstaan zodat proactief voorkomen wordt dat incidenten ontstaan.

Local access rights
Gebruikers en applicaties krijgen 'Need to have' toegang tot systeem resources met eigen accounts. Wanneer elevated rights nodig zijn voor beheeractiviteiten wordt er eerst aangelogd met een limited account en vervolgens via 'Sudo' naar het elevated level gegaan.

Uitwijk
Doorbetalers past diens acceptatieomgeving toe als uitwijkfaciliteit. Er is een Business Continuity Procedure beschikbaar om dit te borgen. Er wordt alleen uitgeweken indien de productie omgeving niet binnen 8 uur terug hersteld kan zijn.

Backup, Syncronisatie en Restore
Alle productie data wordt geregeld veiliggesteld, dagelijks on-site, wekelijks off-site.

Internet tijd
Alle systemen lopen syncroon met een NTP server op het internet.

C. Maatregelen van bewerker om te zorgen dat uitsluitend bevoegd personeel toegang heeft tot de Persoonsgegevens:

Password policy
Passwords geven toegang tot gegevens met een bepaald potentieel op CI's. Per classificatie zijn password eisen vastgesteld.

D. Maatregelen om de Persoonsgegevens te beschermen tegen verlies of wijziging en tegen onbevoegde of onrechtmatige verwerking, toegang of openbaarmaking:

Cryptografie
Alle data is encrypted opgeslagen op het filesystem en alle verbindingen zijn ten alle tijden encrypted. Symmetrische encryptie: sleutellengte minimaal 192 bit, bij voorkeur 265, algoritme naar keuze, bij voorkeur Rijndael. Asymmetrische encryptie: RSA of DH/DSS, sleutellengte minimaal 2048 of PGP (PGP gebruikt DH/DSA en RSA). Hashing: SHA 256 (SHA1 nog beperkt toegestaan voor short lived sessies, niet voor opslag)

BIJLAGE 3 - Procedure Meldplicht Datalekken

Tussen Partijen zijn met betrekking tot de meldplicht datalekken de volgende afspraken gemaakt:

1) BEWERKER registreert alle Beveiligingsincidenten;
2) In geval van een Beveiligingsincident informeert BEWERKER VERANTWOORDELIJKE onverwijld en zal de relevante informatie over het incident melden aan de hand van de hieronder opgenomen vragenlijst;
3) VERANTWOORDELIJKE zal beoordelen of een melding verricht dient te worden bij de AP. VERANTWOORDELIJKE zal daarbij in overleg treden met BEWERKER;
4) Voordat VERANTWOORDELIJKE de melding bij de AP verricht zal VERANTWOORDELIJKE de inhoud van de melding met BEWERKER bespreken;
5) Indien VERANTWOORDELIJKE oordeelt dat tevens betrokkenen geïnformeerd dienen te worden, zal VERANTWOORDELIJKE de inhoud van die informatie met BEWERKER bespreken.

BIJLAGE 4 - Vragenlijst Beveiligingsincident bij de Procedure Meldplicht Datalekken

Deze is gebaseerd op het meldformulier van de AP

De contactpersonen bij VERANTWOORDELIJKE voor de meldplicht datalekken zijn:
Naam: Leonie Puijn,Telefoon: 06-28912669, Email: penningmeester@tcdegrootewielen.nl.

BEWERKER zal bij een Beveiligingsincident de volgende vragen beantwoorden:

☐ **Geef een omschrijving van het Beveiligingsincident:**

.....
(bijvoorbeeld "gestolen laptop met klantgegevens" of "een hack op systeem [X]" of "inloggegevens verstuurd naar ontvanger Y ipv X")

☐ **De persoonsgegevens van hoeveel personen zijn getroffen door het Beveiligingsincident?**

.....
(geef een minimum en maximum aantal aan)

☐ **Omschrijf de groep personen waarop de Persoonsgegevens betrekking hebben.**

.....
(bijvoorbeeld sollicitanten of cliënten van VERANTWOORDELIJKE)

Is er sprake van één van deze specifieke groepen personen (omcirkel het antwoord):

Ouderen: JA / NEE
Kinderen: JA / NEE
Zieken of mensen met een verstandelijke beperking: JA / NEE

☐ **Datum en tijdstip van het incident:**

.....
(kan een vast tijdstip zijn of een periode, als dit niet bekend is "onbekend" invullen)

☐ **Wanneer is het beveiligingsincident ontdekt?**

.....

☐ **Wat is de aard van de inbreuk? Omcirkel de antwoorden en vul in waar nodig**

Kan een onbevoegde de gegevens lezen: JA / NEE
Kunnen/zijn de gegevens (worden) gekopieerd door een onbevoegde: JA / NEE
Kunnen/zijn de (bron)gegevens (worden) gewijzigd (bijv. hack in het systeem): JA / NEE

Kunnen/zijn de (bron)gegevens (worden) verwijderd of vernietigd (bijv. ransom ware of brand datacenter): JA / NEE
Zijn de gegevens gestolen: JA / NEE
Overig: .....
(invullen, of als de aard niet bekend is: "onbekend" invullen)

☐ **Om welk type gegevens gaat het? Omcirkel de antwoorden en vul in waar nodig:**

Naam-, adres- en woonplaatsgegevens: JA / NEE
Telefoonnummer: JA / NEE
E-mailadres of andere adres voor elektronische communicatie: JA / NEE
Inloggegevens (gebruikersnaam/wachtwoord, klantnummer of ander identificatienummer): JA / NEE, zo ja;
welke gegevens zijn het: .....(invullen)
Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer): JA / NEE
Burgerservicenummer (BSN) of sofinummer: JA / NEE
Paspoortkopieën of kopieën van andere legitimatiebewijzen: JA / NEE
Geslacht: JA / NEE
Geboortedatum en/of leeftijd: JA / NEE
(Pas)foto: JA / NEE
Geboorteland: JA / NEE
Medische gegevens (waaronder ook medicijnen of medische hulpmiddelen): JA / NEE
Biometrische gegevens (bijv. vingerafdruk, DNA): JA / NEE,
zo ja; welke gegevens zijn het: ..... (invullen)
Gegevens over schulden/kredieten: JA / NEE
Inkomensgegevens: JA / NEE
Gegevens over iemands betalingsverkeer: JA / NEE
Gegevens over wettelijke vertegenwoordiging (bewindvoerder/mentor): JA / NEE
Verslavingsgegevens: JA / NEE
School/werkprestaties: JA / NEE
Gegevens over relationele problemen: JA / NEE
Gegevens over (vermoeden van) mishandeling: JA / NEE
Religie: JA / NEE
Strafrechtelijke gegevens (ook bijv. straatverboden): JA / NEE
Politieke overtuiging: JA / NEE
Vakbondslidmaatschap: JA / NEE
Seksuele voorkeur/geaardheid: JA / NEE
Overige gegevens: ..... (invullen)

☐ **Welke gevolgen kan de inbreuk hebben voor de getroffen personen? Omcirkel de antwoorden en vul in waar nodig:**

Stigmatisering of uitsluiting: JA / NEE
Schade aan de gezondheid: JA / NEE
Kans op identiteitsfraude: JA / NEE
Kans op financiële schade (bijv. fraude met creditcardgegevens): JA / NEE
Blootstelling aan spam of phishing: JA / NEE
Andere gevolgen, namelijk: ..... (invullen)

☐ **Omschrijf welke technische en organisatorische maatregelen zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?**

.....

☐ **Zijn de gelekte persoonsgegevens beveiligd? Omcirkel de antwoorden en vul in waar nodig:**

Zijn de gegevens versleuteld: JA /NEE,
zo ja; welke versleuteling: ..... (invullen)
geldt deze versleuteling voor alle persoonsgegevens of voor een deel? Indien voor een deel, voor welk deel:
..... (invullen)

Zijn de gegevens gehasht: JA /NEE,
zo ja; op welke wijze: ..... (invullen)

Kunnen de gegevens vanaf afstand worden gewist: JA /NEE,
zo ja; is dat gebeurd en wanneer is dat gebeurd: ..... (invullen)

Zijn de gegevens op een andere manier onbegrijpelijk of ontoegankelijk gemaakt: JA /NEE,
zo ja; op welke manier: ..... (invullen)

☐ **Zijn er Persoonsgegevens van personen in andere EU-landen getroffen door het Beveiligingsincident? Zo ja, welke uit welke landen:**

.....

Ondertekening

ALDUS OVEREENGEKOMEN EN IN TWEEVOUD GETEKEND
TC De Groote Wielen Vereniging, Kvk 54596033, gevestigd aan de Groote Vlietlaan 61 te Rosmalen (VERANTWOORDELIJKE) sluit bij deze de Bewerkersovereenkomst af met Doorbetalers VOF, Kvk 59855835, gevestigd aan de Zuiderweg 237 Hilversum (BEWERKER) onder referentienummer DbBo.27.2018.1.

Namens VERANTWOORDELIJKE

Naam: Leonie Puijn Functie: Penningmeester Datum: 25-5-2018

Handtekening:

Namens BEWERKER

Naam: *B. de Jong* Functie: *Commercieel manager* Datum: *18-05-2018*

Handtekening: