

TMC B.V.

Assurance rapportage inzake
Yellowbrick systeem 2010

Amstelveen, 11 maart 2011
Kenmerk: jdv/esc/3878



VERTROUWELIJK

TMC B.V.
t.a.v. de heer P.W. Staartjes
Postbus 94143
1090 GC AMSTERDAM

Amstelveen, 11 maart 2011
Kenmerk: jdv/esc/3878
Betreft: Assurance rapportage inzake Yellowbrick systeem 2010

Geachte heer Staartjes,

OPDRACHT

Conform uw opdracht met kenmerk jdv/esc/3663 d.d. 14 september 2010 hebben wij onderzoek uitgevoerd naar de opzet, het bestaan en de werking van de getroffen beheersmaatregelen met betrekking tot de dienstverlening met versie 4.20 van het Yellowbrick systeem voor het per mobiele telefoon afrekenen van parkeergelden, welke beheerd wordt door TMC B.V..

Het onderzoek was gericht op de integriteit, onweerlegbaarheid, beschikbaarheid, controleerbaarheid en fraudebestendigheid van dit proces, inclusief de privacyaspecten. De normen waaraan wij de beheersmaatregelen hebben getoetst zijn weergegeven in de bijlage a bij deze mededeling. De normen zijn onder meer opgesteld aan de hand van de CROW alsmede op basis van ITIL, ISO-standaarden en publicaties van het Platform Informatiebeveiliging.

De dienstverlening die onder de naam Yellowbrick wordt aangeboden, is ontwikkeld en wordt beheerd onder verantwoordelijkheid van de leiding van Yellowbrick B.V. en TMC B.V.. Daarmee zijn uitsluitend Yellowbrick B.V. en TMC B.V. verantwoordelijk voor de betrouwbare werking van de dienstverlening.

BDO Audit & Assurance B.V. heeft met deze opdracht de verantwoordelijkheid op zich genomen om door middel van een gefundeerd onderzoek met aantoonbare bevindingen een goed onderbouwd oordeel te geven betreffende de betrouwbaarheid en continuïteit van deze dienstverlening.

WERKZAAMHEDEN

Ons onderzoek is verricht in overeenkomstig in Nederland algemeen aanvaarde richtlijnen met betrekking tot assuranceopdrachten. Een assuranceopdracht omvat onder meer een onderzoek door middel van interviews en deelwaarnemingen van relevante gegevens.

Het onderzoek wordt verricht in overeenstemming met de Verordening gedragscode (VGC) voor registeraccountants en de Nadere voorschriften Controle- en overige standaarden (COS3000), alsmede de richtlijn 3000 en Code of Ethics voor IT-auditors. Het onderzoek is gericht op het verkrijgen van een redelijke mate van zekerheid.

Het onderzoek is uitgevoerd in de periode 10 november 2010 tot en met 12 november 2010 en periode 22 februari 2011 tot en met 2 maart 2011 en omvatte onder meer interviews met betrokken medewerkers, bestudering van relevante documentatie, deelwaarnemingen bij TMC B.V., en specifieke controles gericht op de technische beveiliging. De getoetste onderdelen vindt u in bijlage A.

DOORDEEL

Op basis van ons onderzoek zijn wij van oordeel dat de opzet, bestaan en werking van de getroffen beheersmaatregelen met betrekking tot het Yellowbrick systeem versie 4.20 in voldoende mate de integriteit, onweerlegbaarheid, beschikbaarheid, controleerbaarheid, fraudebestendigheid en privacybescherming (zoals weergegeven in bijlage A) waarborgen over de periode 1 januari 2010 tot en met 31 december 2010.

BEPERKINGEN

De TPM heeft alleen betrekking op het verwerken van parkeertransacties van gemeenten, en niet op de financiële afwikkeling tussen TMC, Yellowbrick en de stichting Beheer Mobiliteitsgelden. De 'Billing engine' binnen Yellowbrick is daarom niet in het onderzoek meegenomen. Het gebruik van internettechnologie kent een aantal inherente beperkingen met betrekking tot de beheersmaatregelen ervan. Deze beperkingen zijn onvermijdbaar, waardoor het mogelijk is dat fouten niet (tijdig) worden ontdekt. Daarnaast hebben beheersmaatregelen te maken met veranderende omstandigheden (nieuw beschikbare technologie), waardoor de werking ervan kan worden aangetast. Auditresultaten uit het verleden bieden geen waarborgen voor de toekomst.

TOELICHTING

Het goedkeurend oordeel wil niet zeggen dat aan alle eisen wordt voldaan. Op een aantal onderdelen zijn door ons verbeterpunten geconstateerd, met name rondom de back-up. De geconstateerde verbeterpunten vormen geen cruciale risico's en doen geen afbreuk aan het totaaloordeel. Deze zaken zijn nader toegelicht in de managementletter aan TMC B.V..

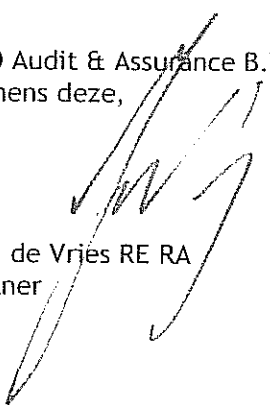
VERSTREKKING AAN DERDEN

Deze mededeling is bestemd voor TMC B.V. en haar (potentiële) cliënten.

Tevens geven wij TMC B.V. toestemming om de mededeling integraal (dat wil zeggen in zijn geheel zonder aanpassing, toevoeging of verwijdering) te publiceren op de website van Yellowbrick.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd en zijn graag bereid de inhoud van deze rapportage verder toe te lichten.

BDO Audit & Assurance B.V.
Namens deze,



J.G. de Vries RE RA
Partner

BIJLAGE A

Normenkader

Algemeen

- Het systeem dient te functioneren conform de in de overeenkomsten opgenomen specificaties.

Integriteit

- De volledigheid juistheid, tijdigheid van de registratie van transacties in het hele traject moet zijn gewaarborgd.
- De parkeertarieven en parkeerzones dienen te allen tijde accuraat te zijn en te blijven.
- De data dient te zijn beschermd tegen ongeautoriseerde beïnvloeding door TMC B.V. of andere dienstverleners.
- Gemeenten dienen realtime inzicht in de parkeersituatie te kunnen krijgen.
- Toereikende Incidentmanagementprocedures.
- Toereikende Problemmanagementprocedures.
- Toereikende Changemanagementprocedures voor zowel hardware als (systeem)software.
- Toereikende inrichting van besturingssystemen, databases en firewall.
- Toereikende toegangsbeveiliging.
- Toereikende virusprotectie.

Onweerlegbaarheid

- Van vastgelegde transacties dient de onweerlegbaarheid te allen tijde te kunnen worden vastgesteld:
 - Aanmeldingen van gebruikers via de website;
 - Telefonische parkeermeldingen;
 - Telefonische eindmeldingen.

Beschikbaarheid

- De beschikbaarheid van het systeem en de afzonderlijke componenten daarbinnen dient te zijn gewaarborgd conform hetgeen daartoe in de overeenkomst met de gemeenten is bepaald. Dit dient tot uiting te komen in:
 - Toereikende back-up voorzieningen;
 - Dubbele uitvoering van kritische componenten;
 - Toereikende fysieke beveiliging;
 - SLA dienstverleners;
 - Onderhoudsprocedures.

Controleerbaarheid

- Alle mutaties in vaste gegevens van gebruikers en gemeenten dienen controleerbaar te worden vastgelegd.
- Voor alle verwerkingen moet kunnen worden vastgesteld dat zij plaatsvinden met de juiste programmatuur en de juiste bestanden.

Fraudebestendigheid

- Het systeem dient zodanige beveiligingsmaatregelen te bevatten dat redelijkerwijs geen spraken kan zijn van fraude met behulp van het systeem.
- Gebruikers dienen niet meer mogelijkheden te ontvangen dan nodig is voor het vervullen van hun taken.
- Het aantal beheeraccounts moet beperkt zijn.
- Toegang tot de aanwezige beheeraccounts en systeemaccounts (accounts waaronder applicaties c.q. processen draaien) moet voldoende zijn beperkt.

Privacy bescherming

- De verwerking dient te voldoen aan de bepalingen van de Wet Bescherming Persoonsgegevens.