ICT infrastructure, privacy & security

Bijlage 1: Privacy statement TMA B.V. t.a.v. TMS

Bijlage 2: Register van verwerkers

CERTIFIED ISO/IEC 27001

Pythagoraslaan 101
3584 BB Utrecht
+31 (0)30-2670444
KVK Utrecht 30174292
www.tmamethod.com
info@tmamethod.com
Btw NL8104.03.171.B.01
NL52 RABO 0160 6925 20

Inhoudsopgave

Pythagoraslaan 101
3584 BB Utrecht
+31 (0)30-2670444
KVK Utrecht 30174292
www.tmamethod.com
info@tmamethod.com
Btw NL8104.03.171.B.01
NL52 RABO 0160 6925 20

Inleiding

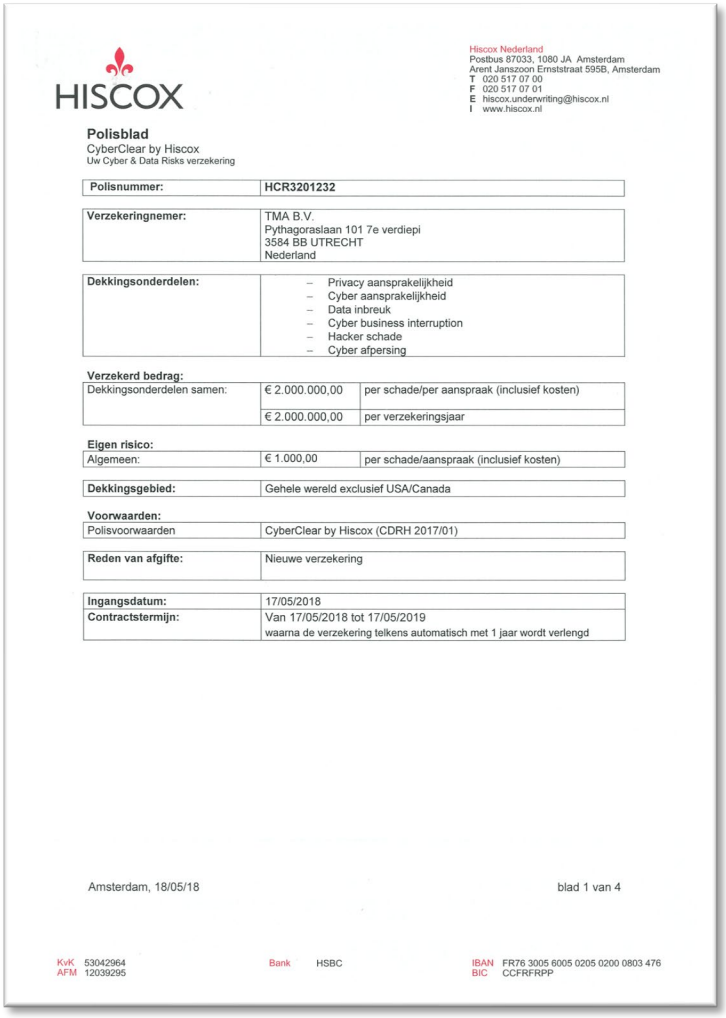
In dit document staan de systeemvereisten, IT infrastructuur en de veiligheidsmaatregelen voor het Talent Management Systeem (TMS) van TMA B.V. beschreven.

Het Talent Management Systeem (TMS) is het modulaire platform met TMA Instrumenten en Content welke TMA B.V. online uitgeeft als SaaS (Software as a Service) dienst en waar een organisatie één of meerdere implementaties van in gebruik krijgt als deze een licentieovereenkomst met TMA B.V. heeft.

Tevens staan er in dit document hoe TMA B.V. rekening houdt met de privacy van gebruikers. TMA is in het bezit van een ISO 27001 certificering waardoor TMA periodiek wordt gecontroleerd of zij de richtlijnen binnen deze normeringen ook nog op de juiste manier toepast. Tijdens deze audits worden de door TMA B.V. opgestelde organisatorische en technische beveiligingsmaatregelen gecontroleerd en getoetst op de uitvoering hiervan. Wij verwijzen naar de artikelen binnen dit document voor de organisatorische en technische maatregelen die door TMA zijn genomen om de persoonsgegevens en data te beveiligen.

CERTIFIED
ISO/IEC 27001

Mocht er onverhoopt toch een incident plaatsvinden op het gebied van data security en privacy waardoor er schade ontstaat waarvoor TMA B.V. aansprakelijk is dan is TMA B.V. verzekerd tot een bedrag van 2 miljoen Euro per jaar bij Hiscox.



HISCOX

Hiscox Nederland
Postbus 87033, 1080 JA Amsterdam
Arent Janszoon Ernststraat 595B, Amsterdam
T 020 517 07 00
F 020 517 07 01
E hiscox.underwriting@hiscox.nl
I www.hiscox.nl

Polisblad
CyberClear by Hiscox
Uw Cyber & Data Risks verzekering

Polisnummer:	**HCR3201232**
Verzekeringnemer:	TMA B.V. Pythagoraslaan 101 7e verdiepi 3584 BB UTRECHT Nederland
Dekkingsonderdelen:	– Privacy aansprakelijkheid – Cyber aansprakelijkheid – Data inbreuk – Cyber business interruption – Hacker schade – Cyber afpersing

Verzekerd bedrag:

Dekkingsonderdelen samen:	€ 2.000.000,00	per schade/per aanspraak (inclusief kosten)
	€ 2.000.000,00	per verzekeringsjaar

Eigen risico:

Algemeen:	€ 1.000,00	per schade/aanspraak (inclusief kosten)

Dekkingsgebied:	Gehele wereld exclusief USA/Canada

Voorwaarden:

Polisvoorwaarden	CyberClear by Hiscox (CDRH 2017/01)
Reden van afgifte:	Nieuwe verzekering
Ingangsdatum:	17/05/2018
Contractstermijn:	Van 17/05/2018 tot 17/05/2019 waarna de verzekering telkens automatisch met 1 jaar wordt verlengd

Amsterdam, 18/05/18 blad 1 van 4

KvK 53042964 AFM 12039295 Bank HSBC IBAN FR76 3005 6005 0205 0200 0803 476 BIC CCFRFRPP

Pythagoraslaan 101
3584 BB Utrecht
+31 (0)30-2670444
KVK Utrecht 30174292
www.tmamethod.com
info@tmamethod.com
Btw NL8104.03.171.B.01
NL52 RABO 0160 6925 20

ICT-infrastructuur

System requirements

Gebruikers hebben de onderstaande technisch zaken minimaal nodig om van het TMS gebruik te kunnen maken:

- Een standalone Windows of Mac computer met internetverbinding.
- Een uniek persoonlijk emailadres.
- Minimaal de één na laatste versie van een van de volgende browsers: Google Chrome, Apple Safari, Mozilla Firefox, Microsoft Edge.
- Browsers dienen javascript te ondersteunen, sessievariabelen te accepteren en de beeldschermresolutie dient minimaal 1024 x 768 pixels te zijn.
- Om de PDF rapportages te bekijken dient men Adobe Acrobat reader te hebben van Adobe. Deze kunt u kosteloos downloaden van de website van Adobe of een vergelijkbare oplossing dat pdf documenten kan openen.
- De mailserver(s) van licentienemer moeten de e-mails van het TMS accepteren.

Organisatie requirements

De organisatie die het TMS gebruikt, is verantwoordelijk voor het gebruik van de persoonsgegevens vanuit het TMS en stelt zelf voorwaarden op voor het gebruik van de persoonsgegevens. Dit betekent bijvoorbeeld dat deze organisatie voorafgaand aan het gebruik van het TMS de volgende zaken formaliseert:

- Aangeven wat de doelen en de voorwaarden zijn voor het gebruik van persoonsgegevens vanuit het TMS. Dit kan in het TMS worden ingebouwd indien de organisatie die het TMS gebruikt dit aangeeft.
- Aangeven wie toegang heeft tot de persoonsgegevens. De organisatie die het TMS gebruikt, is zelf verantwoordelijk voor het toewijzen van autorisaties waarmee specifieke gebruikers toegang krijgen tot persoonsgegevens vanuit het TMS gebruikt. Ook de manier van het gebruik van de persoonsgegevens en het gebruiksdoel zijn de verantwoordelijkheid van de organisatie die het TMS gebruikt.
- Wel of niet expliciet toestemming aan gebruikers vragen voor gebruik van de persoonsgegevens (een zogenaamde opt-in-functie). Dit kan in het TMS worden ingebouwd indien de organisatie die het TMS gebruikt dit aangeeft.
- Wel of niet instellen van een zogenaamde ‘opt-out-procedure’ waarmee gebruikers achteraf kunnen aangeven dat de persoonsgegevens vanuit het TMS niet meer gebruikt mogen worden.

ICT platform

Het TMS maakt gebruik van de FIPS 140-2 gecertificeerde Cloud van Microsoft Azure welke SOC 1, 2 en 3 compliant is. Het TMS is gebouwd op het Microsoft .NET framework. Wij gebruiken alleen componenten die ook in het .NET Framework zitten en of door Microsoft als add-on worden geboden, tenzij er een gegronde reden is om af te wijken. Alle afwijkingen zullen worden gedocumenteerd inclusief de reden van de afwijking.
Hieronder een overzicht van de technische componenten die wij gebruiken:

- .NET Framework 4.7.1
- ASP.NET MVC 5
- ASP.NET Web API 2
- Microsoft Identity 2.2.1
- Microsoft Entity Framework 6.2.0

Externe netwerken

Er zijn twee verschillende koppelingen met externe netwerken te beschrijven.

1. Het externe netwerk van de gebruiker van het TMS. Dit zijn de gebruikers die de functionaliteit van het TMS gebruiken.
2. Het externe netwerk van de partij die de software onderhoudt en door ontwikkelt. Deze partij heeft bij releases en bug fixes toegang tot het productienetwerk in de vorm van het uitrollen van een release of het installeren van een fix of het onderzoeken (potentiële) software-, functionele fout.

Hosting locatie(s)

Het TMS wordt op de Microsoft Cloud omgeving gehost Voor de hosting locatie op Microsoft Azure hebben we als hoofdlocatie de locatie voor West-Europa waar het datacenter in Amsterdam staat. Als uitwijklocatie is er gekozen voor de locatie in Noord-Europa waar het datacenter in Dublin staat. Met de uitwijklocatie bedoelen we de locatie waar we naar overschakelen als er een grote storing is in onze hoofdlocatie. Verder worden alle back-ups die worden gemaakt opgeslagen op de locatie in Dublin.

Infrastructuur

Omdat het TMS op de Microsoft Cloud omgeving wordt gehost, wordt het onderhoud aan de infrastructuur uitgevoerd door de Cloud leverancier. De leverancier van de Cloud omgeving zal al het onderhoud aan de infrastructuur uitvoeren. Wanneer onderhoud resulteert in downtime dan zullen wij dit aan de gebruikers van ons platform bekend maken. Wij hebben als applicatieleverancier dan evenmin toegang tot de datacenters en of de infrastructuur.

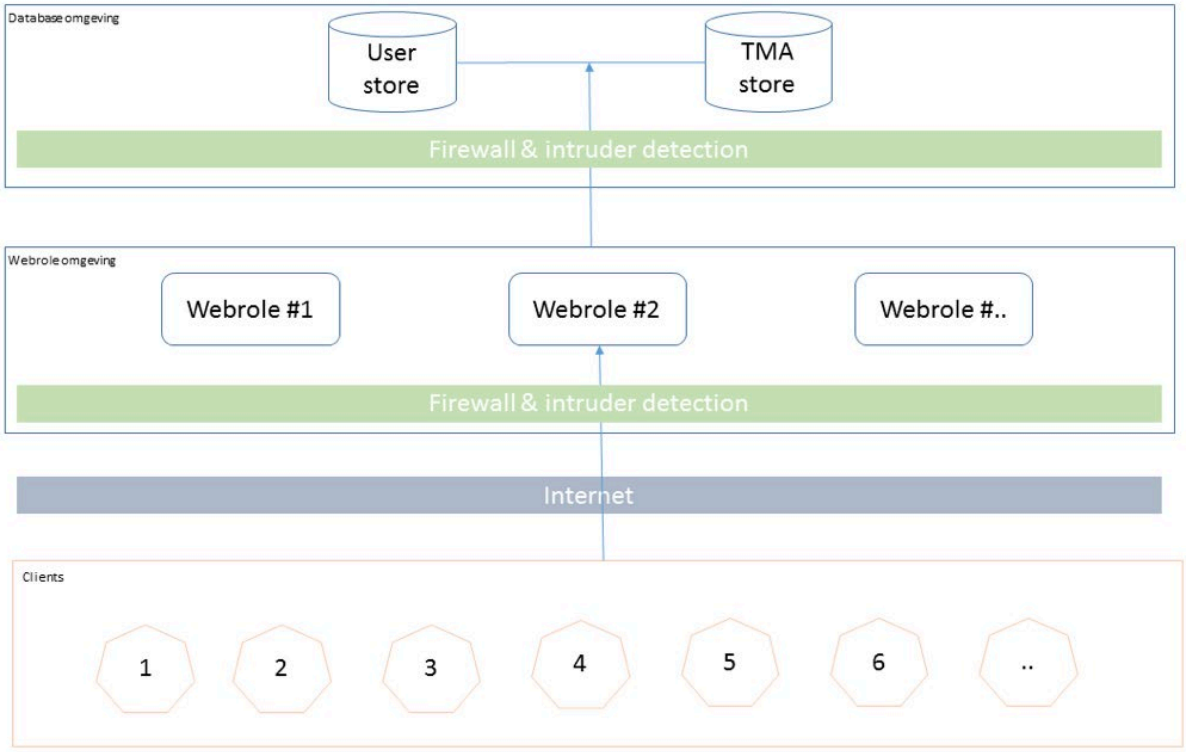
Operating system

Het TMS op de Microsoft Cloud omgeving wordt gehost binnen de zogenoemde ‘Webrollen’ en het onderhoud van het operating systeem wordt gedaan door de Cloud leverancier. Door het gebruik van de zogenoemde ‘Webrollen‘ hebben wij geen toegang tot het operating systeem, waardoor het onderhoud van het operating system wordt gedaan door de Cloud leverancier. De Microsoft Azure Cloud staat erom bekend dat het operating systeem goed wordt onderhouden met de laatste updates. Op het Azure platform voor de “App service” is de antimalware voor Azure geactiveerd.

Webservers

Daar wij gebruik maken van de genoemde ‘Webrollen’ valt het onderhoud gelijk met die van het operating system zoals beschreven in het hoofdstuk hiervoor. De ‘Webrollen’ zijn zo ingesteld dat wanneer de load van een webrol boven de 80% uitkomt er automatisch een tweede wordt bijgezet door het Cloud platform. En wanneer de load van de main webrole weer daalt onder de 80% dan wordt de tweede automatisch weer opgeruimd. Hierdoor hebben we op zeer drukke momenten altijd genoeg resources beschikbaar.

Visuele weergave hosting omgeving



Database servers

De databases van het TMS worden ook gehost op Microsoft Azure als Azure SQL Databases. Voor elke database zit een firewall waar je de toegang naar de database kunt regelen. Standaard zit alles dicht. Standaard zullen alleen de Webservers (Webrollen) toegang krijgen tot de database. Echter is er een uitzondering en dat is wanneer de databases wel met het internet worden gekoppeld. Wanneer er voor het uitvoeren van een release of bug fix toegang tot de database nodig is dan wordt de firewall van de database voor deze beperkte tijd aangepast zodat het IP-nummer van waar de release of bug fix wordt doorgevoerd toegang heeft tot de database. Wanneer de release of bug fix installatie is afgerond, wordt het IP-nummer weer uit de firewall van de databases gehaald.

TMS webrole back-up

Het TMS (geïnstalleerd op de Azure Cloud omgeving) wordt niet nachtelijks geback-upt. Omdat we vanuit development met geautomatiseerde deployment richting de omgevingen van de Azure Cloud werken, is het uitrollen van de laatste versie bij calamiteiten veiliggesteld. Tijdens de deployment van het TMS zal de applicatie ook volledig geautomatiseerd geconfigureerd worden.

Wanneer we tijdens calamiteiten moeten uitrollen naar een ander datacenter van de Azure Cloud omgeving zullen er slechts een paar parameters van deployment aangepast hoeven te worden waarna de applicatie ook naar de uitwijkmogelijk geautomatiseerd uitgerold kan worden.

Database

De database is encrypted via Azure Transparent Data Encryption. Databases worden elke nacht geback-upt en kunnen via de restore-functie worden teruggeplaatst. Wanneer we tijdens calamiteiten moeten uitwijken naar een ander datacenter dan kunnen we het back-up bestand inladen om de database te restoren met de data van de afgelopen nacht.

Toegangsvoorzieningsbeleid

Binnen het TMS zijn de area's programma technisch van elkaar gescheiden. Binnen het TMS kennen wij de volgende area's:

- Kandidaat Area: dit is de area waar de kandidaat de analyse maakt
- Feedback Area: dit is de area waar de feedbackgevers zonder account op basis van een token feedback geven
- Customer Area: dit is de area waar de klant van TMA B.V. alle klantgerelateerde zaken kan uitvoeren.
- Documentation Area: dit is de area waar de ontwikkelaars de documentatie over het TMS bijhouden en waar klanten en ICT partners de documentatie kunnen lezen.
- Administration Area: dit is de area waar de servicedesk van TMA B.V. alle administratieve zaken rondom de applicatie kan uitvoeren
- Application Area: dit is de area waar de monitoring dashboards van het TMS in staan

Voor toegang tot elk van de bovenstaande area's moeten mensen door de servicedesk van TMA B.V. expliciet geautoriseerd worden, met uitzondering van de feedback area, deze werkt op basis van tokens. Zonder de juiste autorisatie is het niet mogelijk om toegang tot een specifieke area van het TMS te krijgen of tot de data behorende bij de area.
Per klant wordt er bekeken tot welke area's toegang wordt verschaft. Dit laat onverlet dat organisaties die toegang tot het TMS hebben, zelf verantwoordelijk zijn voor het daadwerkelijk autoriseren van mensen binnen de toegewezen area's.

Rechten voor gebruikers

Het TMS werkt met rollen. Per area zijn er specifieke rollen gedefinieerd.

Rechten voor platformaccounts

Door het TMS in diverse area's in te delen en voor elke area eigen rollen toe te kennen, hebben wij een splitsing gemaakt in de diverse functionaliteiten. Door deze splitsing is het zonder de benodigde rollen niet mogelijk om toegang te hebben tot een andere area en de data behorende bij deze area.

Autorisaties worden altijd door de mensen van de servicedesk van TMA B.V. ingesteld met uitzondering van de Customer area. Binnen de Customer area is het mogelijk voor een klant om zelf gebruikers aan te maken op basis van diverse rollen binnen deze de eigen area en binnen het eigen data domein.

Security & privacy

Policy-compliance-checks TMS

De Security van het TMS wordt minimaal 1 maal per jaar met een penetratietest gecontroleerd. Van een penetratietest wordt een rapportage gemaakt.

Policy-compliance-checks hosting

Wanneer er fundamentele wijzigingen zijn op het hosting platform waarbij een grote impact op de compliance ontstaat, worden de wijzigingen onderzocht.

Verbeteringen

Wanneer er uit de policy-compliance-checks verbetervoorstellen komen en worden geïmplementeerd in het TMS, dan zullen deze verbeteringen, mits geen gevoelig karakter, worden opgenomen in de release notes van het TMS. Wanneer de verbetervoorstellen een gevoelig karakter hebben, zullen de verbetervoorstellen in een intern systeem worden opgenomen.

Technische controlefunctie

Binnen de ontwikkelomgeving van het TMS wordt gebruikt gemaakt van CodeIt.Right om geautomatiseerd tijdens het ontwikkelen geautomatiseerde scans uit te voeren over de gehele broncode. Verder geeft CodeIt.Right tijdens het ontwikkelen de ontwikkelaar tips en maakt de ontwikkelaar attent op bepaalde zaken.

Logging incidenten

Incidenten met betrekking tot het TMS wordt geregistreerd en vastgelegd in een systeem zodat er overzicht is wat er is binnengekomen en wanneer ze worden opgelost en in welke versie. Externe meldingen worden in hetzelfde systeem vastgelegd en kullen leiden tot een hotfix/tussenrelease of worden in een reguliere release meengenomen. Verder zal van elke melding een rapport worden opgemaakt met de benodigde gegevens om te testen welke oplossing is geïmplementeerd en in welke release deze wordt opgeleverd.

Binnen het TMS kennen wij verschillende soorten logging:

- Application Error logging
- Authenticatie logging (succes/failure)
- Performance logging (snelheid van elke call naar de applicatie)

Wanneer onze logging mechanismen uitvallen, houdt dit voor het TMS in dat de gehele applicatie uit de lucht is. Het logging mechanisme is onderdeel van de applicatie en zit daarin in verweven. De enige uitzondering hierop is de logging van de hosting environment. Deze is via een aparte interface te benaderen.

Afhankelijk van de soort logging heeft het TMS een bewaartermijn voor haar logging, zie hieronder per soort logging wat de bewaartermijn is.

- Application Error Logging: Application error logging wordt 3 maanden bewaard.
- Authentication logging: Authentication logging wordt 3 maanden bewaard.
- Performance logging: Performance logging wordt 1 maand bewaard.

Het TMS maakt gebruik van een database om te loggen. Alleen de applicatie administrator heeft toegang tot deze database en kan logs verwijderen.

De servicedesk van TMA heeft een live view op alle bovengenoemde logs en controleert de authenticatielogs op verdachte omstandigheden. Indien nodig zal er actie worden ondernomen op basis van informatie uit een van de logbestanden. Deze actie zal worden gelogd in het release/incidenten systeem van het TMS.

Toegangsvoorzieningsmiddelen

In het TMS worden klanten aangemaakt via de servicedesk van TMA B.V. Dit komt voort uit een getekend contract waarmee de identiteit van deze klanten is vastgesteld. Na het aanmaken van de klant administrator is het de verantwoordelijkheid van de klant welke gebruikers hij aan het systeem toegevoegd. De controle op identiteit ligt bij de klant voor haar eigen omgeving van het TMS.

Binnen het door het TMS gebruikte ASP.Net Identity Model worden de wachtwoorden eenwegsvercijferd opgeslagen door het gebruik van een hashing in combinatie met een salt. Wachtwoorden kunnen alleen vergeleken worden maar kunnen nooit teruggebracht worden naar de oorspronkelijke karakters.

Authenticatiemiddelen

Het TMS kent een gebruikersnaam-wachtwoord-combinatie om toegang te verlenen. Wanneer hier een foutieve combinatie wordt ingevoerd, wordt er geen toegang verleend tot het TMS. Daarnaast wordt op basis van rollen bekeken of de juiste toegang tot een specifieke area kan worden verleend. Wanneer niet de juiste rollen voor een specifieke area aan de gebruiker zijn gekoppeld, wordt geen toegang tot de area verschaft. In het TMS kan er voor de toegang tot het systeem gebruikt worden gemaakt van 2-stapsverificatie. Deze instelling kan geactiveerd worden door de servicedesk van TMA B.V. Verder worden de functionaliteiten bepaald door de rollen in het TMS. De functionaliteiten kunnen per TMS implementatie samen met de service desk van TMA B.V. worden ingesteld.

Identiteits- en toegangsmanagement

Het TMS ondersteunt de complete levenscyclus van accounts, hieronder verstaan we:

- Aanvragen
- Toekennen
- Wijzigen
- Intrekken/schorsen/verwijderen

Het TMS logt wanneer een gebruiker is aangemaakt. Hierdoor kunnen wij exact zien wanneer een gebruiker toegang tot ons systeem heeft gekregen. Voor de activiteiten rondom het toegang verlenen tot onze systemen worden zowel de succesvolle als de niet succesvolle acties gelogd.

De klanten en/of aanroepende systemen zijn verantwoordelijk voor het blokkeren van een account. Wij bieden hen een interface om accounts te blokkeren. Wanneer het een klant of een aanroepend systeem betreft, dan blokkeert de servicedesk van TMA B.V. het account.

Het TMS stelt eisen aan de identificatie/authenticatie(mechanismen) om voldoende sterke wachtwoorden af te dwingen'.

Om te voorkomen dat login gegevens te vaak foutief ingevoerd worden, blokkeert het TMS een account na 5 pogingen voor 5 minuten. Binnen deze 5 minuten is het niet mogelijk met dit account in te loggen. Na deze 5 minuten zal het account weer actief zijn. TMA heeft deze maatregel genomen om de beveiliging van het TMS te verhogen. Door deze maatregelen worden login pogingen door middel van geautomatiseerde methodes (bijvoorbeeld Brute-force aanval) bemoeilijkt.

Nieuwe releases TMS

Nieuwe releases van het TMS worden uitgerold op de vastgestelde tijdstippen van de releasekalender. Een release wordt alleen dan uitgevoerd en naar productie gebracht als de stappen van Ontwikkeling, Test en Acceptatie zijn doorlopen.

Incident fixes

Incident fixes waarvoor geen workaround is, zullen, nadat ze grondig getest zijn, op de productie-omgeving worden doorgevoerd. Deze procedure wordt gevolgd om de overlast tot een minimum te beperken.

Validatie van de invoer op de server

Alle invoer op de portal wordt zowel clientside als serverside gevalideerd. Validatiemeldingen worden aan de gebruiker gecommuniceerd. Dit is de eerste stap voordat iets van de uiteindelijke code wordt uitgevoerd. Validatiemeldingen zitten in de response van de call en kunnen door het aanroepende systeem worden gebruikt om de gebruiker te informeren. Binnen het TMS maken we gebruik van AnitForgery-tokens in combinatie met Request Validation. Hierdoor kunnen we traceren of de call ook authentiek is en van onze server afkomt. Binnen het TMS hebben wij Request Validation ingeschakeld waardoor het niet mogelijk is om risicovolle tekens naar de server te versturen, tenzij dit expliciet voor een bepaald veld wordt gedoogd.

Privacy bevorderende technieken

Het TMS is ontworpen conform de privacy by designprincipes. Daar waar mogelijk worden persoonsgegevens geanonimiseerd of gepseudonimiseerd.

Versleuteling of hashing van gevoelige gegevens in databases en bestanden

Het TMS maakt gebruik van versleuteling dan wel hashing van gevoelige gegevens in de database en bestanden.

Cryptografisch sterke sessie-identificerende cookies

Het TMS gebruikt cryptografisch sterke sessie-identificerende cookies.

Communicatieversleuteling

Alle communicatie met het TMS gebeurd over TLS 1.2. De ICT-beveiligingsrichtlijnen voor Transport Layer Security zijn in het TMS toegepast.

Genereren en opslaan rapportages en dashboards

In het TMS krijgen gebruikers inzicht in de resultaten van de door deelnemers afgeronde TMA analyses en instrumenten via de rapportages en dashboards module. Alle zichtbare output wordt gegenereerd op het moment dat een geautoriseerde gebruiker een rapportage of dashboard opent als hij is ingelogd in het TMS. Deze rapportages en dashboards worden niet opgeslagen in de database van het TMS maar telkens opnieuw gegenereerd. Na het genereren delete het TMS deze automatisch. Wel bestaat tot zolang de toegang tot het TMS bestaat en gebruikers toegang hebben tot bepaalde rapportages en dashboards de mogelijkheid deze te downloaden als pdf bestand en op een eigen locatie op te slaan (bijv. op de eigen pc of in een cloud opslag zoals Google drive). Tevens is dit gedownloade pdf document dan te printen. Het TMS en de content van de TMA Methode kan enerzijds wijzigen en anderzijds kan de data die over een deelnemer beschikbaar is wijzigen (bijv. omdat hij een ander analyse heeft afgerond of opnieuw heeft gedaan of de normscores van een analyses zijn gewijzigd) waardoor in beide gevallen de dashboards en rapportages kunnen wijzigen in de loop van de tijd. De rapportages en dashboards zijn dus altijd een momentopname. Een gebruiker is zelf verantwoordelijk indien hij een document downloadt uit het TMS om deze op een veilige omgeving te bewaren. Het TMS slaat deze pdf documenten dus niet op in de database van het TMS. Mede om te vermijden dat privacy gevoelige documenten direct vanuit de database van het TMS ongeautoriseerd bij derden terecht kunnen komen.

TMS informatie

Commentaarregels worden tijdens compilatie niet meegenomen naar een release executabel/binarie. Voor code die niet gecompileerd maar geïnterpreteerd wordt, zal het commentaar zoveel mogelijk worden verwijderd. Het TMS heeft gevoelige configuratie vastgelegd in de Azure configuratie voor de Web Role waarbinnen de applicatie draait. Deze gegevens worden door het Azure systeem dynamisch en op een veilige manier aan de configuratie toegevoegd. Binnen het TMS worden commando- en queryteksten opgebouwd door het Microsoft Entity Framework. Dit framework (ontwikkeld en onderhouden door Microsoft) zorgt ervoor dat er geen SQL injectie kan plaatsvinden. Dit framework wordt dan ook door Microsoft onderhouden en aan het begin van elke release zal er worden gekeken of er een nieuwere versie is. Indien dit het geval is, zullen deze componenten worden ge-upgrade. De queryteksten worden

samengesteld door middel van LINQ. Binnen het TMS wordt de invoer van gegevens afgevangen en gevalideerd.

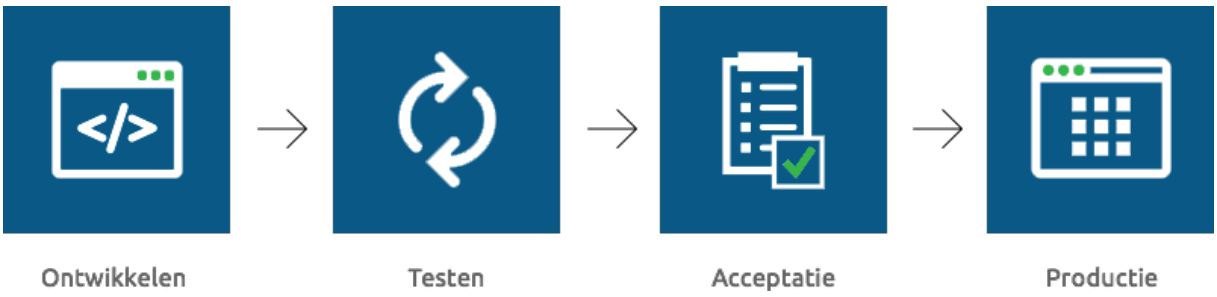
Ontwikkeling en verbetering van het TMS

De ontwikkeling van het TMS wordt gedaan door TMA B.V. en gedeeltelijk uitbesteed. TMA B.V. is in control en leidt de ontwikkeling van het TMS. TMA is eigenaar en heeft 24/7 toegang tot de laatste versie van de programmeercode. Tijdens de ontwikkeling worden er door TMA hoge eisen gesteld aan de beveiliging en mogelijke verwerking van persoonsgegevens. Voor zover de ontwikkeling plaats vindt door een andere partij zijn er over de beveiliging en verwerking van persoonsgegevens contractuele afspraken gemaakt.

De ontwikkeling van het TMS wordt gedaan doormiddel van de OTAP werkwijze.
Er zijn 4 verschillende omgevingen waar een update in de code doorheen moet.

De omgevingen die gepasseerd worden zijn:
- Ontwikkel (hierin wordt het TMS ontwikkeld met fictieve data)
- Test (TMA test nieuwe releases op deze omgeving met fictieve data)
- Acceptatie (Hier test TMA de deploy van het TMS alsof deze live staat.)
- Productie (Dit is de omgeving waar alle TMS implementaties die online zijn zich bevinden)

Over het publiceren van nieuwe releases zijn ook afspraken gemaakt. Elke 2e donderdag van de maand wordt een release gepubliceerd wanneer deze door de testprocedure is heen gekomen. Zogeheten “hotfixes” worden mogelijk sneller gepubliceerd zoals eerder beschreven bij het onderwerp “logging incidenten”.



Wanneer data op verzoek van de klant wordt gemigreerd, zal deze eerst naar de acceptatie-omgeving worden gezet. Wanneer de klant akkoord geeft dat de juiste data is gemigreerd wordt de migratie pas doorgevoerd naar de productie omgeving.

Tijdens het ontwikkelproces houden de ontwikkelaars zich aan het OWASP ontwikkel principe (meer informatie hierover kunt u vinden op https://www.owasp.org). Vanaf de start van de ontwikkeling van het TMS heeft privacy by design al een belangrijke rol. Tijdens de ontwikkeling wordt er constant gedacht over privacy verhogende maatregelen. Daarnaast wordt het uitgangspunt van dataminimalisatie (zo min mogelijk persoonsgegevens verwerken) steeds voor ogen gehouden.

TMS sessies

Binnen het TMS worden sessies die gedurende 20 minuten niet gebruikt worden automatisch beëindigd. Wanneer een gebruiker nog een bestaande sessie heeft, wordt deze herkend door het systeem en heeft de gebruiker toegang zonder een nieuwe sessie aan te maken. Wanneer er toch een nieuwe sessie wordt aangemaakt dan wordt de oude automatisch beëindigd. Binnen het TMS heeft de gebruiker de mogelijkheid om zijn/haar sessie via een menu item te beëindigen.
Binnen het TMS is het niet mogelijk om na het beëindigen van een sessie nog toegang te krijgen tot afgesloten delen van de applicatie of tot data binnen de applicatie. Gebruikers worden altijd verwezen naar het login scherm van de applicatie om hier een nieuwe sessie aan te vragen.

Webprotocollen

Instellingen met betrekking tot de http-requests validatie worden in de configuratie van het TMS vastgelegd. Deze configuraties worden op webserverniveau gevalideerd waardoor de http-requests geen code van het TMS zullen uitvoeren.

Binnen het TMS worden alle mogelijk aan te roepen endpoints door middel van autorisaties beveiligd. Deze autorisaties worden voordat een http-request code kan uitvoeren gevalideerd. Wanneer er geen gepaste authenticatie of autorisatie is dan resulteert dit in de daarvoor bestemde http-statuscode.

Voor het TMS zijn alleen de GET, POST en OPTIONS http-requestmethoden geactiveerd. Overige http-requestmethoden staan geblokkeerd in de configuratie. Binnen de portal van het TMS wordt geen gebruik gemaakt van de andere http headers dan de standaard noodzakelijke.

Het TMS geeft nimmer de fout en de fouttekst mee in een http-response. Hiermee is het mogelijk om contact op te nemen met de Service desk van TMA B.V. De medewerkers van de Service desk kunnen met dit nummer de fout achterhalen en de gepaste actie/procedure opstarten.

Webserver

Binnen de TMS configuratie is voor alle cookies de flags ‘secure’ en ‘HttpOnly’ ingesteld en wordt het afgedwongen op webserver niveau.

De headers ‘Content-Security-Policy: frame-ancestors’ en (tijdelijk) ‘X-Frame-Options’ zijn opgenomen om te voorkomen dat de schermen van het TMS niet binnen een andere applicatie geladen kunnen worden (bijvoorbeeld binnen een frame). Dit is door ons te overrulen door bij deze instellingen de geautoriseerde applicaties toe te voegen.

Pentesten

TMA B.V. heeft in haar ISMS opgenomen dat er periodiek pentesten worden uitgevoerd op de acceptatie omgeving. Deze acceptatie-omgeving biedt een goede representatie van de productieomgeving. De mate van beveiliging, de code en instellingen zijn gelijk aan een TMS in de productie-omgeving. Klantdata komt bij het uitvoeren van een pentest nimmer in gevaar. Bevindingen uit de rapportage van de pentest worden binnen de geadviseerde periode opgelost. TMA tracht dan ook de beveiliging van het TMS op een hoog niveau te houden zodat uw data veilig is. Indien zich een kritisch beveiligingsprobleem voordoet, zal TMA B.V. zich 100% in te zetten het probleem direct te verhelpen.

Error afhandeling

Het afvangen van errors is een basisvorm van beveiliging. Door middel van gedetailleerde errors kan een kwaadwillend persoon veel afleiden van een server of software. Deze informatie kan worden gebruikt voor een mogelijk gerichte aanval op een mogelijk zwak component van de server of software. TMA B.V. laat daarom dan ook alleen custom error melding zien met een id waarvan de betekenis alleen bekend is bij TMA B.V. en haar ontwikkelaars. De daadwerkelijk foutmelding wordt veilig opgeslagen in een database. TMA heeft alle mogelijke voorzorgsmaatregelen genomen om de error afhandeling op een zo goed mogelijke en veilige manier te doen. De verzamelde foutmeldingen worden gebruikt om het TMS te verbeteren.

Technische middelen voor identificatie, authenticatie en autorisatie

Het TMS wordt ontwikkeld op het Microsoft.NET platform. Binnen dit platform levert Microsoft identificatie, authenticatie en autorisatie componenten, genaamd Microsoft ASP.NET Identity. Het TMS implementeert deze componenten die worden aangeleverd aan en onderhouden door Microsoft. Hiermee heeft het TMS de zekerheid dat veiligheidsissues met betrekking tot deze componenten zullen worden opgelost door Microsoft. Bij elke release wordt gekeken of er een update van deze componenten beschikbaar is. Indien er een update beschikbaar is, zal deze update worden doorgevoerd.

Uniformiteit en flexibiliteit van authenticatiemechanismen

Het TMS maakt gebruik van 'Microsoft ASP.NET Identity'. Deze set van componenten implementeert diverse open standaarden. Deze set componenten geeft op een uniforme manier toegang tot verschillende manieren van authenticatie. Door deze flexibele opzet kunnen diverse authenticatiebronnen worden ontsloten door middel van ontwikkelde add-on's.

Wachtwoorden

Het TMS heeft de volgende vereisten met betrekking tot wachtwoorden.

- Wachtwoord moet minimaal 8 karakters lang zijn
- Wachtwoord moet zowel hoofdletters als normale letters bevatten
- Wachtwoord moet minimaal een special karakter of een numeriek karakter bevatten.

Het is voor de gebruiker mogelijk om zelf zijn wachtwoord te wijzigen. Het gebruik van 2-weg-authenticatie is per TMS implementatie te configureren.

Geïmplementeerde beveiligingsmaatregelen

Bij de implementatie van beveiligingsmaatregelen zijn de volgende punten in ieder geval meegenomen.

- Informatiebeveiliging beleidsdocumenten
- Toewijzen van verantwoordelijkheden m.b.t de toegang tot persoonsgegevens
- Toewijzen van verantwoordelijkheden m.b.t. informatiebeveiliging
- Beveiliging en beheer van bedrijfsmiddelen van TMA
- Beveiligde gebieden
- Toegangsbeveiliging
- Leveranciers beheer en beoordelingen
- Continuïteitsbeheer
- Registratie en handelen van incidenten/datalekken
- Laten uitvoeren van pentesten
- Logging en controle van logboeken
- Beveiligingsbewustzijn
- Monitoren en meten
- Risico-analyses
- Risicobehandelplan
- Directiebeoordelingen
- Projectbeheer
- Invoeren procedures bijvoorbeeld
    - Wijziging functie
    - Wijziging personeel
    - Veilig personeel
    - Toekennen rechten SaaS applicatie
    - Melding datalek
    - Toegang kantoorruimte TMA
    - In gebruik name ICT middelen
    - Wijziging in systemen
    - Controle op echtheid van legitimatie middelen
- Back-up beleid
- Opstellen competentieprofielen personeel TMA
- Versie beheer op documenten
- Geheimhoudingsclausules in contracten van medewerkers

In het kader van de ISO 27001 certificering van TMA zijn alle beveiligingsmaatregelen en beleidsdocumenten tegen het licht gehouden.

Sleutelmateriaal en certificaten.

Het TMS heeft als enige sleutelmateriaal het TLS Certificaat voor de encryptie van het dataverkeer tussen cliënt en server te versleutelen over het http(s) protocol. Het aanvragen van een TLS Certificaat en het

generen van het wachtwoord voor de private key wordt gedaan door de directie geautoriseerde systeem beheerder van TMA B.V. Tijdens de (her)installatie zal de systeembeheerder (of een gemachtigde vervanger) het wachtwoord van het sleutelmateriaal invoeren. Naast de systeembeheerder is er binnen TMA B.V. altijd minimaal één extra persoon die het wachtwoord kent. Het sleutelmateriaal van het TLS Certificaat wordt door de systeembeheerder van TMA B.V. opgeslagen op een veilige plaats. De plaats waar dit materiaal wordt opgeslagen is (naast de systeembeheerder van TMA B.V.) bekend bij de directie van TMA B.V.

Pythagoraslaan 101
3584 BB Utrecht
+31 (0)30-2670444
KVK Utrecht 30174292
www.tmamethod.com
info@tmamethod.com
Btw NL8104.03.171.B.01
NL52 RABO 0160 6925 20

ISO 27001:2013 Certificatie TMA

Hieronder een schematische weergave van het door TMA ingerichte ISMS (Information Security Management System).

Op basis van het door TMA gehanteerde ISMS is het ISO 27001 certificaat behaald. Jaarlijks wordt er bij TMA B.V. een externe audit uitgevoerd door Lloyd's Register om ISO 27001 gecertificeerd te blijven.

Het proces

De ISO 27001 certificering zorgt ervoor dat TMA B.V. als organisatie goed blijft nadenken over de gegevensbescherming in het TMS en de wijze waarop met (persoons)gegevens binnen de organisatie omgegaan dient te worden.

TMA heeft een ISMS ingericht waarbij constant de plan, do, check, act methode wordt toegepast. Deze methode zorgt er voor dat ISMS constant gecontroleerd en verbeterd wordt. Om het ISMS niet uit te laten uitgroeien tot een niet te controleren systeem is het ISMS opgedeeld in diverse documenten. Denk hierbij bijvoorbeeld aan het informatiebeveiligingsbeleid. Dit beleid bestaat uit 2 aparte documenten te weten het Algemeen informatiebeveiligingsbeleid en het Technisch informatiebeveiligingsbeleid. In beide documenten staat informatiebeveiliging centraal.

De Security & Privacy Officer (SPO) van TMA voert op geplande momenten interne audits uit. Deze interne audits zijn voor TMA een toetsingsmoment om te kijken of TMA zich nog houdt aan de regels en beveiligingsrichtlijnen waarop zij de certificering heeft behaald. De SPO houdt op dagelijkse basis in de gaten of TMA zich houdt aan de bepalingen zoals beschreven in het ISMS en die wettelijk zijn verankerd in de AVG.

Pythagoraslaan 101
3584 BB Utrecht
+31 (0)30-2670444
KVK Utrecht 30174292
www.tmamethod.com
info@tmamethod.com
Btw NL8104.03.171.B.01
NL52 RABO 0160 6925 20

Lloyd's Register

Huidige uitgiftedatum: 18 april 2021
Vervaldatum: 17 april 2024
Certificaatnummer: 10341722

Originele uitgiftedatum:
ISO/IEC 27001 - 16 december 2020

Certificaat

Hiermede wordt verklaard dat het managementsysteem van:

TMA B.V.

Pythagoraslaan 101, 3584 BB Utrecht, Nederland

door Lloyd's Register is goedgekeurd voor de volgende norm(en):

ISO/IEC 27001:2013

Goedkeuringsnummer: ISO/IEC 27001 – 00012740

Dit certificaat is geldig voor de volgende scope:

Alle informatiebeveiligings- en privacybeschermende maatregelen die van toepassing zijn bij het ontwikkelen, leveren en ondersteunen van de TMA Methode met de SaaS applicatie TMA Talent Management System (TMA Portal) voor competentie- en talentmanagement en persoonlijke ontwikkeling conform de Verklaring van Toepasselijkheid versie 5.0 d.d. 18 februari 2021.

Paul Graaf

Area Operations Manager North Europe

Afgegeven door: Lloyd's Register Nederland B.V.

voor en namens: Lloyd's Register Quality Assurance Limited

UKAS MANAGEMENT SYSTEMS
001

Page 1 of 1

Pythagoraslaan 101
3584 BB Utrecht
+31 (0)30-2670444
KVK Utrecht 30174292
www.tmamethod.com
info@tmamethod.com
Btw NL8104.03.171.B.01
NL52 RABO 0160 6925 20

Definities

API
: Een application programming interface (API) is een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander programma of onderdeel (meestal in de vorm van bibliotheken).

Cloud
: De term cloud is eigenlijk een beetje misleidend. De cloud is eigenlijk gewoon internet. Net als een wolk is het internet niet tastbaar. Een cloudserver is dan ook eigenlijk een server die verbonden is met internet. Data is toegankelijk via diverse apparaten of plaatsen. De hardware waarmee en de locatie waarvandaan verbinding wordt gemaakt met de server speelt een minder grote rol dan in het verleden. Een verbinding met internet is het belangrijkste om met de cloudserver te verbinden.

Code voor informatiebeveiliging
: De Code voor informatiebeveiliging beschrijft normen en maatregelen, die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging. De Code voor informatiebeveiliging bestaat uit twee delen de norm (ISO 27001) en een ‘code of practice’ (ISO 27002). Certificering gebeurd tegen de norm. De ‘code of practice’ geeft handreikingen voor de implementatie van maatregelen in de organisatie

Hashing
: Encryptiemethode. Een hashfunctie is een functie in de informatica die invoer uit een breed domein van waarden omzet in een (meestal) kleiner bereik, meestal een deelverzameling van de gehele getallen. De output wordt de hash, hashcode of digest van de input genoemd. Het is een vorm van pseudonimiseren.

IP-adres
: De afkorting IP staat voor Internet Protocol. Elke computer of netwerk die verbonden is met internet heeft een IP-adres. Dit is een nummer waarmee hij zichtbaar is voor alle andere computers op het internet. Je kan een IP-adres vergelijken met een telefoonnummer. Om het mogelijk te maken dat computers elkaar kunnen vinden en identificeren, hebben deze een eigen nummer nodig. Dat is het IP-adres. Een IP-adres is onder het protocol versie IPv4 32bit en onder het protocol versie IPv6 128bit. De IPv4 versie is het meest bekend en heeft een format van bijvoorbeeld 192.168.1.0 (dit voorbeeld tref je vaak op een intern netwerk)

IIS
: Internet Information Services. Dit is een verzameling serverdiensten ontwikkeld door Microsoft bedoeld voor windows machines op internet. Een windows machine die IIS draait, wordt door deze verzameling van diensten een webserver.

Informatie beveiliging
: Informatiebeveiliging is het geheel aan preventieve, detectieve, repressieve en correctieve maatregelen en procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een organisatie garanderen. Het doel is de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

ISMS
: Information Security Management System. Dit is een managementsysteem voor informatiebeveiliging. Het ISMS bestaat voor een deel uit IT onderdelen, maar daarnaast komen gedrag van medewerkers, standaard procedures en bedrijfsrichtlijnen aan de orde

ISO
: In een ISO norm worden eisen gesteld waaraan een organisatie dient te voldoen wanneer men een ISO certificaat wenst te behalen. Om aan de normeisen te voldoen, dient de organisatie haar bestaande managementsysteem kritisch te beoordelen om, indien nodig, bestaande processen en procedures conform aan te passen.

ISO 27001
: ISO 27001 is een standaard voor informatiebeveiliging. De norm specificeert eisen voor de implementatie van beveiligingsmaatregelen die zijn aangepast aan de behoefte van afzonderlijke organisaties of delen daarvan. Het ISMS is ontworpen om de keuze van adequate en proportionele beveiligingsmaatregelen die de informatie beschermen en vertrouwen bieden aan belanghebbende te waarborgen.

Persoonsgegevens
: Persoonsgegevens is elk gegeven over een geïdentificeerde of identificeerbaar natuurlijk persoon. Dit betekent dat informatie ofwel direct of indirect naar een persoon te herleiden is. Dat het om een natuurlijk persoon moet gaan, houdt in dat gegevens van overleden personen of van een organisatie geen persoonsgegevens zijn.

SaaS applicatie
: Software as a Service. Het TMS (voorheen TMA Portal) is een SaaS applicatie

Salt
: Bij 'salting', oftewel zouten, wordt willekeurige data toegevoegd aan een hashfunctie.

TLS
: Transport Layer Security (TLS) en diens voorganger Secure Sockets Layer (SSL), zijn encryptie-protocollen die de communicatie tussen computers (bijvoorbeeld op het internet) beveiligen.

TMS
: Talent Management Systeem / SaaS applicatie / Portal

Webapplicatie
: Webapplicatie is een term die gebruikt wordt voor een programma dat op een webserver draait, en via de webbrowser kan worden benaderd.

Webrollen / Web Roles
: Webrollen zijn zo geconfigureerd dat ze geschikt zijn om een een webapplicatie te draaien die geprogrammeerd zijn voor IIS.

Bronnen: kader-advies.nl; wikipedia; TMA technisch beleid; TMA algemeen beleid; NEN; Autoriteit Persoonsgegevens

Bijlage 1: Privacy statement TMA B.V. t.a.v. TMS

TMA B.V. exploiteert een webapplicatie met de naam 'Talent Management Systeem' (TMS) en geeft deze online uit als SaaS (Software as a Service) dienst. Organisaties kunnen een licentie nemen op het gebruik van een eigen TMS implementatie.

TMA B.V. verwerkt persoonsgegevens en wil gebruikers (betrokkenen) en gebruikmakende organisaties van het TMS hierover duidelijk informeren.

Organisatiegegevens

TMA B.V.
Pythagoraslaan 101
3584 BB Utrecht
Nederland

KvK nr: 30174292
Internet: www.tma.nl

Contactgegevens Security & Privacy Officer

Dhr. J.P. Klutz
Tel: +31 (0)30 - 2670444
Email: Privacy@tmamethod.com

Rechten met betrekking tot persoonsgegevens

Als gebruikers vragen hebben of willen weten welke persoonsgegevens wij van ze hebben, kunnen ze contact met ons opnemen. Betrokkenen hebben de volgende rechten:

- Een uitleg krijgen over de persoonsgegevens die we verwerken en wat we daarmee doen.
- De inzage in uw persoonsgegevens.
- Het corrigeren van terechte fouten.
- Het verwijderen van verouderde gegevens.
- Het intrekken van toestemming.
- Bezwaar maken tegen een bepaald gebruik.
- Het overdragen van uw gegevens naar een derde.

Verzoeken van gebruikers over hun persoonsgegevens zullen wij in principe doorverwijzen naar de organisatie die een TMS implementatie gebruikt waar de betreffende persoonsgegevens zich in bevinden van de gebruiker. Die organisatie is namelijk de verwerkingsverantwoordelijke en TMA B.V. is slechts de verwerker die alleen in opdracht van de verwerkingsverantwoordelijke mag handelen.

Als gebruikers vinden dat ze niet op de juiste manier geholpen worden, dan hebben ze het recht om een klacht in te dienen bij de bovenstaande contactpersoon of de Autoriteit Persoonsgegevens.

Van wie TMA B.V. persoonsgegevens verwerkt

TMA B.V. verwerkt in het TMS (persoons)gegevens van mensen die zijn aangedragen door de organisaties die een TMS implementatie gebruiken en daar een licentie voor hebben.

Als een organisatie die het TMS gebruikt, direct of indirect persoonsgegevens van gebruikers aan TMA B.V. verstrekt, dient deze organisatie de betrokken personen hierover te informeren.

Welke persoonsgegevens verwerkt worden

De volgende persoonsgegevens van de gebruiker worden verwerkt indien aanwezig:

- Voornaam, tussenvoegsel en achternaam
- Geslacht

- Emailadres
- Geboortedatum
- Opleidingsniveau
- Functienaam van de gebruiker
- Scores die een indicatie geven over de drijfveren, talenten, cognitieve capaciteiten, beroepsinteresses en competenties van een gebruiker. Deze gegevens worden alleen verwerkt indien een gebruiker één of meer analyses invult en afrondt of indien feedbackgevers en/of assessors één of meer feedback c.q. assessment analyses invullen over een gebruiker
- Rapportages en dashboards met geschreven en gevisualiseerde output op basis van de scores, teksten en persoonsgegevens die over een gebruiker beschikbaar zijn in het TMS / de TMA portal
- Teksten over de gebruiker die voortkomen uit de ingevulde vragen en de geschreven conclusies c.q. opmerkingen. Deze gegevens worden alleen verwerkt indien een gebruiker, feedbackgevers en/of assessors deze teksten geschreven hebben en in het TMS / de TMA Portal hebben geplaatst

De volgende persoonsgegevens van de gebruiker worden alleen verwerkt door TMA B.V. Deze persoonsgegevens worden gebruikt om foutmeldingen te verhelpen, de activiteiten van gebruikers in het TMS te loggen, gebruikers te ondersteunen bij het gebruik van het TMS en de beveiliging en gebruikerservaring van het TMS te verbeteren:

- Het IP adres van de gebruiker
- De locatie van de gebruiker op basis van IP adres
- Het besturingssysteem dat de gebruiker gebruikt
- De browser die de gebruiker gebruikt
- Het tijdstip van inloggen van een gebruiker

De volgende persoonsgegevens van de gebruiker kunnen optioneel aanvullend op de hierboven beschreven persoonsgegevens **anoniem** worden verwerkt door de TMA B.V. indien verstrekt ten behoeve van wetenschappelijk onderzoek en beloningsonderzoek:

- Salarisniveau van de gebruiker
- Percentage van het dienstverband (voltijd/deeltijd)
- Werk- en denkniveau
- Opleidingen
- Nationaliteit

Waarom persoonsgegevens verwerkt worden

TMA B.V. verwerkt deze persoonsgegevens om daarmee uitvoering te geven aan de overeenkomsten die zijn afgesloten met de organisaties die een licentie hebben genomen op de TMA Methode en het bijbehorende TMS.

Voor organisaties die gebruik maken van het TMS en daarmee inzicht willen krijgen in de talenten, drijfveren, beroepsinteresses, cognitieve capaciteiten en competenties van hun (potentiële) medewerkers en/of stagiaires en leerlingen, biedt TMA B.V. diverse analyses, instrumenten met daaruit voortvloeiende rapportages en dashboard via het TMS. Om het voor gebruikers mogelijk te maken om analyses in te vullen en rapportages en dashboards te genereren, heeft TMA B.V. een aantal persoonsgegevens nodig. Waarom een organisatie die een licentie heeft op het TMS persoonsgegevens gebruikt bepaalt de betreffende organisatie. Wij verwijzen gebruikers dan ook naar hen door als ze daarover vragen hebben.

Bewaartermijn

De persoonsgegevens die TMA B.V. verwerkt, worden zorgvuldig bewaard. De bewaartermijn wordt bepaald door de organisatie die een licentie op de TMA Methode en het TMS heeft. Op het moment dat deze organisatie aangeeft dat bepaalde persoonsgegevens verwijderd moeten worden of zodra de licentie voor het gebruik van het TMS met een organisatie is beëindigd, vernietigt TMA B.V. alle persoonsgegevens met uitzondering van geanonimiseerde persoonsgegevens voor wetenschappelijk en beloningsonderzoek.

Indien een individuele gebruiker verwijdering van zijn persoonsgegevens wil bewerkstelligen uit het TMS, moet hij hiertoe een verzoek indienen bij de organisatie die de licentie heeft voor het gebruik van het TMS.

Pythagoraslaan 101
3584 BB Utrecht
+31 (0)30-2670444
KVK Utrecht 30174292
www.tmamethod.com
info@tmamethod.com
Btw NL8104.03.171.B.01
NL52 RABO 0160 6925 20

Indien de gebruiker dit verzoek toch doet aan TMA B.V. zal hij worden doorverwezen naar de organisatie die de licentie heeft voor het gebruik van het TMS.

Wie toegang heeft tot de persoonsgegevens.

De geautoriseerde medewerkers van TMA B.V. en de verwerkers welke vermeld staan in het Register van verwerkers hebben naast de organisatie die een licentie heeft op het gebruik van een eigen TMS implementatie toegang tot de persoonsgegevens. Verwerkers mogen alleen persoonsgegevens verwerken als zij passende maatregelen hebben genomen met minimaal hetzelfde beveiligingsniveau als TMA biedt en deze organisaties contractueel geheimhouding van de persoonsgegevens garanderen.

Bijlage 2: Register van verwerkers

Software ontwikkeling

Certigon B.V.
Sutton 15
7327AB Apeldoorn
Nederland

Internet: www.certigon.nl
Email: info@certigon.nl
Tel: +31 (0)55 - 8442674